Хмельницький національний університет
Факультет інформаційних технологій
Кафедра комп'ютерної інженерії та інформаційних систем

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

Галузь знань 12 – Інформаційні технології

Спеціальність 123 –Комп'ютерна інженерія

на тему «Метод криптографічного захисту протоколів в засобах комунікації інтернету речей»

КвРКІ. 2202134.22.02.37 ПЗ

Виконав: студент 2 курсу, група КІ2м-22-2 _____ Микола ЛАПТЄВ
Підпис Ім'я, прізвище

Керівник канд. техн. наук, доцент _____ Катерина БЕРЕЗЬКА
Науковий ступінь, вчене звання Підпис Ім'я, прізвище

До захисту допускаю:
Зав. кафедри КІІС, д.т.н., проф.
Тетяна ГОВОРУЩЕНКО
01 05 2024 р.

Хмельницький, 2024

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОРМАЦІЙНИХ СИСТЕМ

Освітній рівень МАГІСТР

Галузь знань 12 ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Спеціальність 123 КОМП'ЮТЕРНА ІНЖЕНЕРІЯ

Освітня програма ОСВІТНЬО-НАУКОВА ПРОГРАМА «КОМП'ЮТЕРНА ІНЖЕНЕРІЯ ТА ПРОГРАМУВАННЯ»

ЗАТВЕРДЖУЮ
Зав. кафедри КІІС
Тетяна ГОВОРУЩЕНКО
"01" 09 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Лаптєв Микола Павлович
Прізвище, ім'я, по батькові студента

1. Тема проекту (роботи) Метод криптографічного захисту протоколів в засобах комунікації інтернету речей

Керівник проекту (роботи) к.т.н., доцент Березька К.М.
Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

Затверджена наказом ректора університету від 01.01.2024р. № 1

2. Строк подання студентом проекту (роботи) на кафедру 03.05.2024 р.

3. Вихідні дані до проекту (роботи) Завдання на кваліфікаційну роботу

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити)

аналіз відомих методів криптографічного захисту протоколів;
архітектура засобів комунікації інтернету речей;
метод криптографічного захисту протоколів в засобах комунікації інтернету речей.

5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень)

6. Консультанти розділів дипломного проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Нормоконтроль	Лисенко С.М., професор кафедри КІІС		
Антиплагіат	Нічепорук А.О., доцент кафедри КІІС		

7. Дата видачі завдання «_06_»_____09_____2023 р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) дипломного проекту (роботи)	Термін виконання етапів проекту (роботи)	Примітка
1	Вибір напряму дослідження та узгодження тематики ДРМ з керівником	01.09.2022	виконано
2	Ознайомлення з предметною областю; формулювання мети та задач дослідження; визначення об'єкта та предмета дослідження	05.12.2023	виконано
3	Робота над розділом 1 – аналіз відомих моделей, методів за темою; постановка задачі	25.02.2024	виконано
4	Робота над розділом 2 – розробка архітектури для вирішення поставленої задачі	01.04.2024	виконано
5	Робота над науковою статтею та тезами	05.03.2024	виконано
6	Робота над розділом 3 – розробка методу для вирішення поставленої задачі	15.04.2024	виконано
7	Робота над розділом 4 – проектування та розробка засобів для вирішення поставленої задачі, експериментальна частина	25.04.2024	виконано
8	Оформлення пояснювальної записки згідно вимог	30.04.2024	виконано
9	Попередній захист ВКР	01.05.2024	виконано
10	Захист ВКР на засіданні ЕК	До 30.05.2024	

Студент  Микола ЛАПТЄВ
Підпис Ініціали, прізвище

Керівник роботи  Катерина БЕРЕЗЬКА
Підпис Ініціали, прізвище

РЕФЕРАТ

Тема кваліфікаційної роботи: Метод криптографічного захисту протоколів в засобах комунікації інтернету речей

Автор роботи: Лаптєв Микола Павлович

Керівник роботи: Березька К. М.

Пояснювальна записка: 70с., 84 джерела.

ПЕРЕЛІК КЛЮЧОВИХ СЛІВ: інтернет речей, протокол, криптографічний захист, ключ.

Об’єктом дослідження є процес криптографічного захисту протоколів в засобах комунікації інтернету речей.

Предметом дослідження є методи криптографічного захисту протоколів в засобах комунікації інтернету речей.

Метою кваліфікаційої роботи є розробка методу криптографічного захисту протоколів в засобах комунікації інтернету речей.

Для розв’язання поставлених задач використовувалися методи теорії комп’ютерних мереж, архітектури комп’ютерів, теорії множин.

Наукова новизна отриманих результатів:

- розроблено новий метод криптографічного захисту протоколів в засобах комунікації інтернету речей.

У вступі подано об’єкт та предмет дослідження, мету, наукову новизну та практичну цінність роботи, а також характеристику структури роботи.

У першому розділі проведено аналіз відомих рішень щодо криптографічного захисту протоколів в засобах комунікації IoT.

У другому розділі здійснено проєктування сумісних безсертифікатних та ідентифікаційних криптосистем для гетерогенного IoT та подано розроблений метод криптографічного захисту протоколів в засобах комунікації інтернету речей.

У третьому розділі розроблено подання підписів та компактних ключів в

системах з IoT та здійснено моделювання розробленої схеми з ключами в системах з IoT.

У четвертому розділі здійснено проєктування розподіленого реєстру для послідовного запису транзакцій та шифрування з можливістю пошуку за відкритим ключем на основі решітки.

У висновках підведено підсумки досягнення результатів з розв’язання завдань дослідження.

На основі проведених досліджень розроблена система для забезпечення криптографічного захисту протоколів в засобах комунікації інтернету речей.

Практична значимість отриманих результатів полягає у розробленій крипографічній системі для забезпечення захисту протоколів в засобах комунікації інтернету речей. Вона надає можливість для формування надійних з’днань між засобами інтеренту речей, щоб передавати повідомлення, без ідентифікації та без сертифікації.

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

КФС – кіберфізична система

ОС - операційна система

ПЗ - програмне забезпечення

IoT – Інтернет речей

PoW – Proof of Work

ВСТУП

Системи з використанням IoT часто покладаються на пристрої низького класу для надсилання вимірювань іншим сторонам, і в очікуванні налаштування, несанкціонованої зміни та/або порушення конфіденційності цих заходів може мати катастрофічні наслідки (наприклад, вбудовані медичні датчики). Тому забезпечення ефективної автентифікації, цілісності та конфіденційності в цих умовах є життєво важливим. Хоча звичайні криптографічні заходи можуть бути використані для задоволення цих вимог безпеки, незважаючи на їх елегантний дизайн, вони часто занадто дорогі з обчислювальної точки зору для пристроїв низького класу. Ситуація ще більше посилюється, коли до уваги береться безпека від квантових комп'ютерів.

Актуальність роботи полягає в необхідності розробити метод криптографічного захисту протоколів в засобах комунікації інтернету речей, які б не використовували сертифікатів та ідентифікації для пришвидшення обміну інформацією.

Метою кваліфікаційої роботи є розробка методу криптографічного захисту протоколів в засобах комунікації інтернету речей.

Поставлена мета досягається розв’язанням таких основних завдань:

- проаналізувати відомі методи криптографічного захисту протоколів в засобах комунікації інтернету речей;

- розробити метод криптографічного захисту протоколів в засобах комунікації інтернету речей;

- реалізувати розроблений метод криптографічного захисту протоколів в блокчейн;

- здійснити есперименталні дослідження згідно розроблених рішень.

Об’єктом дослідження є процес криптографічного захисту протоколів в засобах комунікації інтернету речей.

Предметом дослідження є методи криптографічного захисту протоколів в засобах комунікації інтернету речей.

Метою кваліфікаційої роботи є розробка методу криптографічного захисту протоколів в засобах комунікації інтернету речей.

Для розв’язання поставлених задач використовувалися методи теорії комп’ютерних мереж, архітектури комп’ютерів, теорії множин.

Наукова новизна отриманих результатів:

- розроблено новий метод криптографічного захисту протоколів в засобах комунікації інтернету речей.

На основі проведених досліджень розроблена система для забезпечення криптографічного захисту протоколів в засобах комунікації інтернету речей.

Практична значимість отриманих результатів полягає у розробленій крипографічній системі для забезпечення захисту протоколів в засобах комунікації інтернету речей. Вона надає можливість для формування надійних з’днань між засобами інтеренту речей, щоб передавати повідомлення, без ідентифікації та без сертифікації.

Для розв’язання поставлених задач використовуються основні положення теорії розподілених систем, архітектури комп’ютерів, кіберфізичних систем, інтернету речей.

За темою кваліфікаційної роботи опубліковано одну публікацію у Збірнику наукових праць за матеріалами XV Всеукраїнської науково-практичної конференції «Актуальні проблеми комп’ютерних наук АПКН-2023». (Хмельницький – 2023. – С.139-141).) [84].

1 АНАЛІЗ МЕТОДІВ І ТЕХНОЛОГІЙ КРИПТОГРАФІЧНОГО ЗАХИСТУ ПРОТОКОЛІВ В ЗАСОБАХ КОМУНІКАЦІЇ ІНТЕРНЕТУ РЕЧЕЙ

1.1 Аналіз предметної області

Інтернет речей (IoT) – це гетерогенна система, що складається з великої кількості взаємопов'язаних датчиків, розумних пристроїв, приймачів-передавачів, мікрокомп'ютерів тощо. Такі системи часто покладаються на зв'язок у реальному часі для забезпечення передбачуваної функціональності та можуть бути об'єктом зловмисних атак для аутентифікації, цілісності та/або конфіденційності даних, що передаються/зберігаються. Але, існує широкий спектр криптографічних схем, призначених для ефективного пом'якшення/запобігання цим атакам.

Ці криптографічні схеми в основному можна розділити на системи на основі симетричного ключа або системи на основі відкритого ключа. Схеми на основі симетричних ключів пропонують високоефективні та безпечні рішення, однак вони можуть бути не ідеальними для впровадження в деяких умовах IoT через наступне:

1) обчислення та розподіл спільного ключа;

2) зберігання спільних ключів;

3) недостатня публічна можливість перевірки та невідмова у схемах аутентифікації.

Схеми на основі симетричних ключів вимагають протоколу узгодження ключів для обчислення спільного секретного ключа перед ініціюванням безпечного зв'язку. Хоча в деяких програмах може бути можливим попереднє завантаження цих спільних ключів на всі пристрої, це буде досить складно для систем, де рухомі датчики/пристрої повинні зв'язуватися з безліччю нових пристроїв у режимі реального часу (наприклад, мережі повітряних дронів, автомобільна мережа тощо).

Для великих мереж Інтернету речей з тисячами або навіть мільйонами пристроїв зберігання попередньо обчислених/спільних ключів може бути неможливим на пристроях низького класу через їх обмежений обсяг пам'яті.

Хоча існує багато симетричних понять на основі ключів для забезпечення автентифікації, вони не забезпечують відмови від аутентифікації і публічна перевірюваність. Головним чином це пов'язано з тим, що такі схеми вимагають ключа підпису для перевірки автентичності токенів автентифікації.

Схеми на основі відкритих ключів призначені для усунення вищевказаних недоліків і забезпечення більш просунутих властивостей безпеки. Однак, незважаючи на свою елегантність, ці системи (наприклад, [1, 2]) часто занадто дорогі для впровадження в деяких застосунках IoT, які складаються з пристроїв низького класу (часто з живленням від батарейок) та/або мають затримки [3]. Крім того, враховуючи, що можливий дебют квантових комп'ютерів становить безпосередню загрозу класичним складним проблемам, на які покладається більшість, якщо не всі, існуючих криптосистем з відкритим ключем, плани переходу на постквантові безпечні системи вже розпочаті стандартизацією державними органами (наприклад, NIST, NSA тощо). Однак, порівняно зі своїми звичайними аналогами [4-7], ці постквантові безпечні рішення часто вимагають більше додаткових витрат на обчислення, зберігання та/або зв'язок, що робить їх впровадження у вищезгаданих налаштуваннях IoT ще складнішим.

Мета роботи полягає в тому, щоб подолати цю прогалину в дослідженнях, розробивши нові схеми на основі відкритих ключів, які можуть задовольнити масштабованість і суворі вимоги до продуктивності бюджетних інфраструктур IoT. Тому, в цій роботі представляємо серію практичних традиційних і постквантових захищених криптографічних заходів (наприклад, цифрові підписи, безсертифікатні криптосистеми, схеми шифрування з можливістю пошуку з відкритим ключем і т.д.), засновані на добре вивчених припущеннях, які будуть розгорнуті в таких застосунках, як системи розумних мереж, розумні імплантовані медичні пристрої, Інтернет дронів і безпечне хмарне сховище. Нові

схеми розроблені на основі нової/покращеної теоретичної основи або дизайну систем, які можуть допомогти подолати розрив між функціональністю, ефективністю та безпекою. Розглянемо ефективні традиційні і постквантові криптографічні схеми для задоволення жорстких вимог до систем IoT. У лінійці пропозицій ефективних схем аутентифікації розглядатимемо дві схеми підпису. Перша схема сигнатур заснована на звичайних криптографічних задачах і використовує кодування повідомлень з сімействами без покриття і особливою властивістю функцій для досягнення значного приросту продуктивності в порівнянні з аналогами [8]. Друга схема базується на постквантових примітивах [9-11] і досягається шляхом поширення одноразових сигнатур на (поліноміально обмежені) багаточасові сигнатури, використовуючи адитивно-гомоморфні властивості узагальнених компактних ранцевих функцій. Нова схема забезпечує найнижчу наскрізну затримку серед аналогів, що робить її придатною для пристроїв низького класу. Як крок до повністю постквантового блокчейну будемо використовувати протокол Proof of Work (PoW) [12], який мінімізує переваги квантового майнера. Такий протокол заснований на задачі найкоротшого вектора Ерміта в евклідовій нормі і дозволяє використовувати алгоритм швидкої перевірки. Щоб полегшити перешкоди, пов'язані з комунікацією та перевіркою сертифікатів для низького класу пристроїв, розглядатимемо і використовуватимемо засновані на ідентифікації та безсертифікатні криптосистеми, які створюються за допомогою спеціальних алгоритмів генерації ключів, які використовують адитивну гомоморфну властивість експонент, щоб дозволити користувачам включати свої приватні ключі в ключі, надані довіреною третьою стороною, не фальсифікуючи їх. Нові схеми забезпечують кращу ефективність обчислень і порівнянну ефективність зв'язку в порівнянні з аналогами на основі ідентифікації та без сертифікатів. Нарешті, з метою запропонувати ефективні та високобезпечні заходи для безпечного віддаленого зберігання даних, використаємо дві схеми шифрування з можливістю пошуку відкритим ключем на основі решітки [13] з постквантовою

безпекою. Ці схеми є першими прикладами таких схем, заснованих на ґратках, які забезпечують постквантову перевагу. Перший варіант базується на решітках і забезпечує значну перевагу в продуктивності та кращу наскрізну затримку в порівнянні з існуючими аналогами. Друга схема, заснована на стандартній моделі, що забезпечує кращу безпеку в порівнянні з аналогами з вартістю гіршої продуктивності. Усі запропоновані схеми довели свою безпеку за допомогою суворих доказів безпеки, а також впроваджені та мають відкритий вихідний код, щоб забезпечити публічне тестування та перевірку.

Високоефективна схема електронного цифрового підпису [14]. Розглянемо схему підпису [15], що розширює межі існуючих цифрових підписів, з майже 2× швидша верифікація та 33% швидший підпис у порівнянні з найшвидшим аналогом [16]. Цей приріст ефективності досягається за рахунок використання кодування повідомлень за допомогою сімейств без покриття та спеціальної односторонньої функції на основі еліптичної кривої [17]. Ці значні обчислювальні переваги пов'язані з більшими вимогами до пам'яті, що є дуже вигідним компромісом для деяких застосунків із критичною затримкою. Доведено його безпеку в умовах жорсткості задачі дискретного логарифма еліптичної кривої (в моделі випадкового числа) і надано реалізацію [17] з відкритим вихідним кодом на обладнанні та 8-розрядному мікроконтролері AVR, що підтвердило значний приріст продуктивності.

Сумісні безсертифікатні криптосистеми для IoT [18]: безсертифікатні криптосистеми, такі як ідентифікаційні [19]; безсертифікатні системи [19], що зменшують або нівелюють витрати зв'язку та верифікації сертифікатів (ланцюжків), що може бути занадто дорогим для деяких систем IoT. Перспективним для розроблення є криптосистеми на основі ідентифікації та без сертифікатів [20], які, крім того, що є більш ефективними, ніж їхні аналоги, забезпечують сумісність, щоб дозволити користувачам з різних доменів (заснованих на ідентифікації або безсертифікатних) безперешкодно спілкуватися. Ця функція корисна для деяких гетерогенних налаштувань IoT (наприклад,

повітряних дронів [21]), де різні рівні довіри/контролю передбачаються на довірену третю сторону. Ідея наших побудов полягає в тому, щоб розробити спеціальні алгоритми генерації ключів, які використовують експонентний добуток властивостей степенів та функцій без покриття (подібно до [21]), щоб дозволити користувачам включати свої приватні ключі в ключі, надані довіреною третьою стороною, не фальсифікуючи їх.

Розглянемо швидкі постквантові сигнатури з компактного набору [22]. Ппредставимо просту, але ефективну схему цифрового підпису, яка забезпечує постквантову безпеку. Схема базується на новому підході [22] до розширення одноразових сигнатур на основі хешу до (поліноміально обмежених) багаточасових сигнатур, використовуючи адитивно гомоморфні властивості узагальнених функцій компактного набору. Розглянемо дозволи на проектування для досягнення декількох ключових властивостей. По-перше, алгоритми підпису та перевірки є найшвидшими серед поточних аналогів з вищим рівнем безпеки. Це дозволяє досягти найнижчої наскрізної затримки серед своїх аналогів, а також зробити його придатним для обмежених ресурсів підписувачів. По-друге, його приватні ключі можуть бути такими ж маленькими, з бажаним рівнем безпеки. По-третє, на відміну від більшості своїх аналогів на основі ґратки, він не вимагає будь-якої гаусової вибірки під час підписання, а отже, вільний від атак на бічні канали, націлених на цей процес. Доведено безпеку його на основі односторонності сімейства функцій.

Проаналізуємо постквантовий доказ роботи для постквантового блокчейну. Протоколи Proof of Work [23], спочатку запропоновані для обходу DoS та спам-атак електронною поштою, тепер лежать в основі більшості нещодавніх криптовалют. З огляду на потенційне застосування для забезпечення ефективної автентифікації в постквантових блокчейнах, на шляху до повністю постквантово безпечного блокчейну отримуємо новий протокол PoW [24]. Поточні популярні протоколи PoW засновані на хеш-головоломках. Розглядаючи хеш як випадкову функцію і фіксуючи апріорі досить великий простір пошуку, пошуковий

алгоритм Гровера [24] дає асимптотичну квадратичну перевагу квантовим машинам над класичними. Розглядатимемо модифікований протокол PoW, для якого квантові машини мають меншу асимптотичну перевагу [25]. Зокрема, для ґратки рангу *n,* відібраної з певного класу, протокол надає як PoW екземпляр задачі найкоротшого вектора Ерміту [26]. Асимптотично найвідоміша класична задача про квантові алгоритми, які безпосередньо вирішують задачі є евристичними решітками, які виконуються в часі. Останні досягнення в області розв'язування задач, коли імпульс, наданий PoW на основі решітки, допоможуть досліджувати часто складні простори оптимізації [27].

Схеми шифрування з відкритим ключем на основі решітки з пошуком за ключовими словами [28] мають на меті пом'якшити наслідки дилеми конфіденційності даних у порівнянні з їх використанням, при цьому дозволяючи будь-якому користувачу в системі надсилання зашифрованих файлів на сервер для пошуку одержувачем, який створює закритий ключ. Існуючі схеми вводять високу наскрізну затримку, що може перешкодити їх прийняттю на практиці. У роботі [29] пропонують дві нові схеми на основі ґраток [28, 29], які задають високу обчислювальну ефективність разом із кращою безпекою порівняно з їхніми аналоги [29]. Така схема забезпечує на 18× меншу наскрізну затримку, ніж її найефективніший аналог. Це пов'язано з високоефективним алгоритмом тестування, який працює лінійно відповідно до кількості пар ключового слово-файлу. Він пропонує [30] доказову безпеку в стандартній моделі зі зменшенням до найгірших проблем з ґратками з ціною більш високої наскрізної затримки та розмірів параметрів.

Взагалі, схема цифрового підпису — це вектор з трьох аргументів, в якості яких виступають алгоритми: створення пари приватний/відкритий ключ; отримання повідомлення і закритого ключа; виведення рішення після отримання пари повідомлення-сигнатура. У наведеному визначенні визначаємо безпеку сигнатурних схем на основі методології, запропонованої в [31]. Після фази ініціалізації супротивнику надано доступ до засобу генерації підписів. А якщо

він виводить дійсну пару повідомлення-підпис, яка раніше не виводилася з знакового набору, то після відбувається виконання поліноміально обмеженої кількості запитів.

Узагальнена схема розгалуження [32] є широко використовуваною технікою для перевірки безпеки різних добре вивчених схем цифрового підпису. Якщо супротивник може успішно згенерувати підробку, то можна перемотати супротивника назад, вибрати нові випадкові відповіді набору після певного моменту, і супротивник все одно зможе згенерувати підробку з поліноміально пов'язаною ймовірністю.

Таким чином, наявні різні схеми для критпографічного захисту протоколів без сертифікатів та ідентифікації в засобах комунікації інтернету речей. Ефективність таких схем потребує дослідження.

1.2 Аутентифікація для систем IoT в реальному часі

Системи IoT [33-37] часто потребують аутентифікації для застосунків, яким потрібно перевірити великий обсяг вхідних транзакцій або команд. Хоча примітиви симетричних ключів можуть забезпечити дуже швидку автентифікацію, вони не можуть запропонувати відмову, що часто є життєво важливим для цих програм. Наприклад, Visa [38-40] щодня обробляє мільйони транзакцій [41]. Кожна транзакція відповідає багаторазовій аутентифікації запиту користувача та інформації про картку на стороні продавця, платіжного шлюзу та емітента кредитної картки [42]. Таким чином, створення більш ефективних рішень може значно зменшити загальні додаткові витрати на аутентифікацію таких систем, що призводить до значної фінансової вигоди.

Потреба в ефективній автентифікації стає ще більш нагальною для застосунків, в яких пристрої IoT повинні працювати в критично важливих для безпеки налаштуваннях та/або з обмеженнями батареї. Наприклад, повітряні дрони з батарейним живленням [43-47] можуть обмінюватися даними та передавати

потоки команд і вимірювань з оперативним центром за короткий проміжок часу. Швидка та енергоефективна аутентифікація може покращити політ та час реакції таких повітряних дронів [48]. Інші застосунки IoT, такі як системи інтелектуальних мереж та IoT, які включають датчики, що живляться від батарейок, також виграють від швидких та енергоефективних цифрових підписів, які мінімізують затримку/додаткові витрати на аутентифікацію та зменшують час роботи датчиків [49]. У транспортних мережах безпека значною мірою залежить від наскрізної затримки [50], і тому завжди бажане досягнення схеми підпису з найменшою наскрізною затримкою. Крім того, були показані ефективні схеми підпису бути корисним у цифровій криміналістиці та безпеці журналу [51-53].

Він використовує одностороннюю функцію, засновану на еліптичній кривій дискретної логарифмічної задачі і використовує гомоморфні властивості таких функцій, щоб лінійно додати елементи закритого ключа для досягнення коротшої сигнатури та замаскувати це додавання одноразовою випадковістю для досягнення (поліноміально обмеженої) схеми багаточасової сигнатури. Розглянемо основні властивості [54-58].

1. Швидка перевірка. Алгоритм забезпечує найшвидшу перевірку підпису серед своїх аналогів. Зокрема, розширює межі схем сигнатур на основі еліптичної кривої, забезпечуючи майже в два рази швидшу верифікацію порівняно зі своїм найшвидшим аналогом [59].

2. Швидке підписання. Генерація сигнатур дозволяє уникнути дорогих обчислень, таких як скалярне множення з фіксованою основою. Таким чином, алгоритм досягає на 33% швидшого підписання порівняно зі своїм найшвидшим аналогом [59].

3. Низька наскрізна затримка. Завдяки найшвидшим алгоритмам генерації та верифікації сигнатур, алгоритм досягає майже на 40% нижчої наскрізної затримки порівняно зі своїм найшвидшим аналогом [59]. Це може сприяти

потенційному впровадженню для програм, які потребують автентифікації з урахуванням затримки.

4. Енергоефективність. Уникаючи будь-яких обчислювально дорогих операцій в алгоритмах підпису та перевірки, він досягає найнижчого енергоспоживання в порівнянні з його сучасними ефективними аналогами. Зокрема, алгоритм верифікації досягає на 40% нижчого енергоспоживання порівняно з його найбільшою енергією ефективного аналогу [60-63]. Це робить його потенційно придатним для застосунків IoT, в яких пристрої, що живляться від батарейок, автентифікують телеметрію та команди (наприклад, повітряні дрони).

5. Настроювані параметри. Він використовує набір параметрів, які легко налаштовуються. Це дозволяє [64-66] створювати екземпляри з різними властивостями для різних застосувань. Наприклад, набір параметрів, який розглянуто для реалізації на мікроконтролері, має менший розмір пари відкритих ключів і закритих ключів. І якщо одна і та ж схема реалізована на такому обладнанні, то вона може отримати більш швидку генерацію сигнатур (в два рази швидше, ніж схема в [67]), витративши кілька мікросекунд на алгоритм перевірки.

Одноразові підписи [68] були запропоновані для швидкого підписання та перевірки. Слідом за ними було запропоновано багато схем з різними компромісами щодо продуктивності та безпеки, такі як одноразові підписи з терміном дії [69]. Однак ці схеми страждають від штрафів за безпеку та продуктивність, пов'язаних із необхідністю синхронізації часу і їх низька толерантність до втрати пакетів. Багаторазові підписи на основі хешу [70] використовують дерева рішень і можуть підписувати кілька повідомлень, зберігаючи стан підписувача. Останнім часом були запропоновані варіанти без стану [71], однак такі схеми страждають від великих сигнатур і повільних алгоритмів підпису.

Останнім часом запропонована поліноміально-обмежена багаточасова сигнатурна схема на основі проектування [72]. Схема використовує адитивну

гомоморфну властивість базової односторонньої функції для отримання швидких сигнатур, коли підписант агрегує лише компоненти закритого ключа під час фази онлайн. Однак, незважаючи на свою ефективність, він не може задовольнити суворі вимоги щодо затримки деяких програм IoT. Інша запропонована схема [73] використовує агреговану властивість односторонніх функцій перестановки на основі RSA і кодування повідомлень [74] для досягнення ефективного знака. Однак великі розміри параметрів не тільки призводять до дуже великих відкритих ключів, але й роблять піднесення до степеня, яке відбувається під час генерації та перевірки підпису, досить дорогим. Таким чином, будучи однією з найефективніших схем розглядувана схема не перевершує новітні реалізації сигнатур на швидких еліптичних кривих.

У ряду пропозицій швидких еліптичних кривих [75] представили ефективні екземпляри схеми на основі поверхні Куммера, яка показує значний приріст продуктивності в порівнянні до його базової схеми [76]. У 2016 році [77] запропонували нову реалізацію, засновану на іншій еліптичній кривій, яка навіть перевершує реалізацію в [75]. Алгоритм використовує гомоморфну властивість своєї базової односторонньої функції, яка обумовлена експонентним добутком степеневої властивості, для досягнення поліноміально обмежених багаторазових сигнатур зі схеми одноразової сигнатури, запропонованої в [77], з більш компактними сигнатурами. Точніше, в алгоритмі, закритий ключ складається з випадково згенерованих значень, а відповідний відкритий ключ складається з усіх значень. Продуктивність відображена на 8-бітному стабілізаторі. В якості IoT-пристрою для реалізації алгоритму використано 8-розрядний мікроконтролер. Він оснащений флеш-пам'яттю з максимальною тактовою частотою. Він широко використовується на практиці для застосунків IoT (особливо в медичних імплантатах) завдяки своїй енергоефективності [78]. Реалізований алгоритм на мікроконтролері з використанням 8-бітної реалізації кривої [79], яка забезпечує базові операції та хеш-функцію. Схему реалізовано за допомогою вбудованого мікроконтролеру і використано його симулятор точності

циклу для тестів [79].

Наявні відкриті реалізації з відкритим вихідним кодом [80-83]. Процесори з обмеженими ресурсами можуть бути непридатними для важких обчислень (наприклад, піднесення до степеня з 3072-розрядними числами в RSA [80].

В роботі [81] запропонували першу схему безпечного безсертифікатного шифрування без сполучення. Схема побудована з використанням подібних сигнатур в алгоритмі часткової генерації закритих ключів.

В роботі [82] запропонували іншу ефективну схему шифрування, яка спеціально використовується для механізмів інкапсуляції ключів. Було проведено ряд робіт, присвячених моделям безпеки безсертифікатних систем. У більшості запропонованих моделей передбачається, що зловмисник генерує ключі правдоподібно і ініціює атаки тільки після фази налаштування.

В роботі [65] запропонували нову схему, яка дозволяє уникнути гауссівської вибірки під час підписання. Безпека базується на навчанні з помилками та задачах короткого цілочисельного розв'язку в ідеальних ґратках. Ще одна схема сигнатур на основі решітки, запропонована для першого раунду стандартизації для криптографії заснована на задачі про навчання з помилками. Незважаючи на те, що вона схожа на попередню, вона уникає використання гаусової вибірки під час генерації сигнатур, але страждає від більш високої наскрізної затримки і є екземпляром модульної сигнатури ґратки. Сигнатури можуть бути згенеровані за допомогою бімодальної гаусової або однорідної вибірки. Подібно до використання відбору проб відторгнення, щоб уникнути витоку приватної компоненти ключа. Однак при поточних запропонованих параметрах схема страждає від високого часу підписання, що пов'язано з високим відсотком відмов. У той час як інші примітиви на основі ґраток, такі як протоколи обміну ключами, пройшли деякі випробування та оцінки в реальному світі.

Сьогоднішній нестабільний стан ґратчастих підходів перешкоджає розробці сигнатур, які захищені. Сигнатури на основі хешування можуть бути

доведені безпечними в стандартній моделі завдяки дуже добре вивченим властивостям хеш-функцій, такими як стійкість до попереднього зображення. Комбінація дерев Меркла [81] з ранніми одноразовими сигнатурами на основі хешу призводить до дуже ефективних схем зі збереженням стану, які є безпечними для певної кількості підписів. Традиційні схеми на основі хешування зберігають стан, щоб гарантувати, що підписувач не використовуватиме повторно деякі матеріали закритого ключа.

Останнім часом були запропоновані підписи без авторства [82]. Така схема має жорстке зниження безпеки своїх будівельних блоків, таких як хеш-функції. Ці схеми мають великі сигнатури і дуже дорога генерація сигнатур, особливо на пристроях низького класу [78].

Підписи на основі коду подано в роботі [23]. На криптографію на основі коду значною мірою вплинула проблема декодування [23]. Оскільки криптосистема заснована на двійкових кодах було для балансування безпеки та ефективності таких систем, то найбільш добре вивченим і доказово безпечним підходом до отримання схем сигнатур є застосування перетворення за схемою ідентифікації, запропонованою у [24]. Це нова схема підпису на основі коду, представлена на першій конференції з постквантової стандартизації. Її можна розглядати як високовдосконалений варіант схеми в [80], де більшість удосконалень пов'язані із заміною кодів з кодами. У той час значно поліпшено габаритні розміри параметрів в [80]. Розміри ключів як і раніше більше, ніж у його аналогів на основі решітки і хешування. Існує ряд багатовимірних підписів, представлених до стандартизації криптографії. Наприклад, в роботі [69] можна розглядати як удосконалення свого попередника [68], що базується на прихованому полі рівняння криптосистем. Він має ефективний алгоритм верифікації та дуже компактні сигнатури, однак алгоритм підпису значно повільніший, ніж його аналоги на основі хешу. Симетричні підписи на основі ключів є ще однією новою конструкцією, яка заснована на проблемах, пов'язаних з криптографією симетричних ключів.

Таким чином, проведено аналіз криптосхем, які можуть бути застосовними в системах з IoT. Особливо перспективними є схеми з безсертифікатними моделями та ідентифікаціями, оскільки пристроїв IoT багато і потрібно організовувати швидке опрацювання звернень.

1.3 Висновки до першого розділу

В результаті проведеного дослідження предметної області було встановлено недоліки відомих рішень і виділено їх з метою розробки рішень, які б покращили швидкість опрацювання повідомлень за рахунок забезпечення криптографічного захисту протоколів в засобах комунікації інтернету речей без ідентифікації вузлів та без сертифікатів.

Наявні різні схеми для критпографічного захисту протоколів без сертифікатів та ідентифікації в засобах комунікації інтернету речей. Ефективність таких схем потребує дослідження. Аналіз криптосхем, які можуть бути застосовними в системах з IoT показав, що перспективними є схеми з безсертифікатними моделями та ідентифікаціями, оскільки пристроїв IoT багато в засобах комунікації і потрібно організовувати швидке опрацювання звернень.

1.4 Постановка задачі дослідження

Поставлена мета досягається розв’язанням таких основних завдань:

- проаналізувати відомі методи криптографічного захисту протоколів в засобах комунікації інтернету речей;
- розробити метод криптографічного захисту протоколів в засобах комунікації інтернету речей;
- реалізувати розроблений метод криптографічного захисту протоколів в блокчейн;
- здійснити есперементальні дослідження згідно розроблених рішень.

2 МОДЕЛЬ КРИПТОГРАФІЧНОГО ЗАХИСТУ ПРОТОКОЛІВ В ЗАСОБАХ КОМУНІКАЦІЇ ІНТЕРНЕТУ РЕЧЕЙ

2.1 Дослідження предметної області

Системи з IoT покладаються на зв'язок у реальному часі для забезпечення передбачуваної функціональності та можуть бути об'єктом зловмисних атак для порушення механізмів аутентифікації, цілісності та/або конфіденційності даних, що передаються. Широкий спектр криптографічних схем, призначених для ефективного пом'якшення/запобігання цим атакам, має недоліки і потребує удосконалення. Щоб підписати повідомлення, підписант отримує певну кількість індексів шляхом хешування повідомлення і випадкового введення, використовує індекси для отримання відповідних елементів закритого ключа і підсумовує їх разом з одноразовою випадковістю. Сигнатура отримується шляхом застосування хеш-функції, що обчислюється як результат застосування односторонньої функції на одноразову випадковість. Верифікація відбувається шляхом обчислення підсумовування відповідних елементів відкритого ключа та їх віднімання з виходу односторонньої функції на основі застосованої до *неї* функції. Верифікатор виводить дійсні числа, якщо віднімання дає те саме значення, яке було обчислене під час генерації сигнатур. Крім того, алгоритм використовує метод для перетворення скалярного множення тільки для запропонованих наборів параметрів додавання точок з витратами на зберігання невеликої таблиці постійного розміру.

Для усунення недоліків розробимо схему, яка складається з наступних алгоритмів, що будуть використані безпосередьо в розроблюваному методі. Алгоритм є безпечним у моделі випадкового числа. Для доказу використовується лема Форкінга. Тобто, якщо супротивник порушує безпеку алгоритму після виконання випадкових запитів підпису відповідно, тоді можна побудувати інший алгоритм, який запускає підпрограму і може розв'язувати екземпляр.

При налаштуванні він зберігає три списки для відстеження виходів випадкових чисел і список для зберігання повідомлень, надісланих знаковому списку. Він встановлює випадковий список для обробки хеш-функцій і генерує публічні ключі користувачів наступним чином. Запити хеш-функції та знаковий список для багатьох разів, відповідно, будуть повторюватись. Для обробки цих запитів він працює наступним чином. Хеш-запити до хеш-функцій обробляються функціями з підпрограми. Функція запитів підпису працює наступним чином, щоб відповісти на запит підпису у повідомленні. Якщо він отримує відповідну сигнатуру, то повертає значення. Інакше, тоді це працює наступним чином. Вибирає значення і обчислює його хеш-функцію. Далі виводить підробку у повідомленні та відкритому ключі. Дотримуючись визначення користувач виграє гру, якщо алгоритм повертає дійсний результат, який ніколи не надсилався до запитів на підпис на попередньому етапі. Якщо він виводить дійсну підробку перед виконанням хеш-запитів та сигнатурних запитів, то також не може розв'язати екземпляр. Інакше, якщо він видає дійсну підробку, використовуючи схему розгалуження, то переглядає знову базу з тією ж випадковою стрічкою, щоб отримати другу підробку, де з переважною ймовірністю отримує потрібний результат. Виходячи з цього підходу задано послідовність дій, яка може вирішити випадковий екземпляр задачі, якщо виконується одна з наведених умов.

Для оцінювання ефективності алгоритм потребує реалізації на кривій, яка, є найшвидшою, що забезпечує 128-бітний захист. Реалізацію алгоритму необхідно здійснювати на комп’ютерному обладнанні, так і на 8-розрядному мікроконтролері для оцінки його продуктивності, оскільки більшість застосунків IoT складаються з них обох (наприклад, комп’ютерне обладнання як сервери або центри управління, а мікроконтролери як пристрої IoT, підключені до датчиків). Для порівняння продуктивності алгоритму із сучасними схемами цифрового підпису на обох цих платформах з точки зору обчислень, зберігання та зв'язку потрібна реалізація повинна мати відкритий вихідний код.

Алгоритм за допомогою реалізації з відкритим вихідним кодом пропонує найшвидші операції, зокрема доповнення, що має вирішальне значення для його продуктивності. При використанні потрібен процесор Intel як комп'ютерне обладнання, бо використовуються його власні можливості для оптимізації реалізації. Зокрема, реалізовувані функції за допомогою процесора Intel у режимі лічильника та хеш-функція через його ефективність.

Оскільки алгоритм розробляється на еліптичній кривій, то використовуємо її параметри, які забезпечують 128-бітну безпеку. Крім параметрів кривої, вибір параметрів алгоритму і засобів IoT, також, відіграє вирішальну роль для безпеки самого алгоритму. Зокрема, комбінації варіантів параметрів, також, повинні забезпечувати 128-бітну безпеку, щоб забезпечити такий рівень безпеки в цілому. З іншого боку, можна налаштувати ці параметри, щоб досягти бажаного рівня безпеки з різними компромісами продуктивності. Якщо збільшити їх і зменшити їх кількість, тобто варіювати ними, то це призведе до більшого сховища з швидшими обчисленнями, і навпаки. Для комп'ютерної апаратної реалізації вибираємо такі параметри, що пропонується розумний компроміс між сховищем і обчисленнями, а також пропонується бажаний 128-бітний рівень безпеки.

Алгоритм пропонує дуже швидку генерацію та перевірку підписів. Для створення підпису потрібно лише декілька мікросекунд, а для його перевірки – більше попередніх декількох мікросекунд. Це найшвидший серед аналогів алгоритмів. Крім того, якщо використовуємо ті ж параметри, що і для мікроконтролера, то можемо ще більше прискорити генерацію сигнатур до ще меншої кількості мікросекунд, з вартістю декількох мікросекунд на швидкість верифікації. В алгоритмі скалярне множення необхідне при генерації сигнатур і подвійне скалярне множення при перевірці. В алгоритмі для генерації сигнатур необхідні додавання, а перевірка здійснюється за допомогою скалярного множення та додавання. Це відповідає швидшому генеруванню сигнатур і

швидшій верифікації для нього. Тому алгоритм може стати ідеальною альтернативою для застосунків у реальному часі.

Розмір сигнатури для алгоритму такий самий, як і у його аналогів, що значно нижче, ніж у аналогів на основі RSA і хешування. З іншої сторони, алгоритм може поставлятись з більшим приватним і публічним ключем, який становить 32 КБ.

Алгоритм може бути створений з різними значеннями параметрів, що пропонує компроміс між зберіганням і обчисленнями. Оскільки мікроконтролер є пристроєм з обмеженим обсягом пам'яті, то вибираємо параметри так, щоб забезпечити ефективність зберігання. Більше того, це дозволяє зберігати приватні компоненти, замість того, щоб детерміновано генерувати їх при генерації сигнатур, і при цьому мати сховище навіть для 8-розрядного мікроконтролера. Також, встановлюємо значення параметрів в пам’яті пристроїв. Покращення швидкості алгоритму, також, можна спостерігати вибираючи модель котролерів з покращеними характеристиками.

Алгоритм швидше генерує сигнатури і швидше перевіряє підписи в порівнянні з найближчим аналогом. Це може призвести до значної практичної різниці, якщо розглядати програми в реальному часі, які потребують швидкої автентифікації.

Ці тести можуть бути отримані з більш зручним для зберігання вибором параметрів, і можуть бути додатково прискорені за допомогою різних варіантів параметрів, де мікроконтролер не обмежений пам'яттю.

У зв'язку з вибором параметрів, розміри ключів у 8-розрядній реалізації мікроконтролера менші. Це пов'язано з тим, що вибираємо інший параметр, встановлений для нього. Крім того, також зберігаємо приватні компоненти, які відповідають 8 КБ сховища підписувача. Оскільки зберігаємо ці ключі на флеш-пам'яті мікроконтролера, то вони відповідають лише невеликій частині простору від загальної пам'яті, для приватного ключа та відкритого ключа відповідно. Тому,

незважаючи на те, що є значно більші ключі, ніж у аналогів, їх все одно можливо зберігати навіть на 8-розрядних мікроконтролерах з обмеженими ресурсами.

Дуже бажано мінімізувати енергоспоживання криптографічних примітивів у програмах IoT, щоб забезпечити довший час автономної роботи. Для мікроконтролерів енергоспоживання приладу можна виміряти за парметрами: напруга; струм; час обчислення. Враховуючи, що напруга і струм мікроконтролера постійні, коли пристрій активний, споживання енергії лінійно зростає з часом обчислень. Оскільки алгоритм забезпечує найшвидшу генерацію та перевірку сигнатур, енергоспоживання алгоритму є найнижчим серед його аналогів, і тому йому буде віддано перевагу в застосунках, які вимагають більш тривалого часу автономної роботи.

Таким чином, представлено дослідження в предметній області, зокрема схему підпису, яка відповідає суворим вимогам щодо мінімальної затримки деяких систем IoT у реальному часі. Це досягається за рахунок використання гомоморфної властивості односторонньої функції, що лежить в основі, і методу попередніх обчислень. Експериментальні результати підтвердять, що запропонована схема перевершує свої сучасні аналоги за швидкістю підписання та перевірки, а також за енергоефективністю. Запропонована схема безпечна в моделі випадкового списку при жорсткості вимог до неї.

2.2 Проєктування сумісних безсертифікатних та ідентифікаційних криптосистем для гетерогенного IoT

Мобільні та гетерогенні застосунки IoT містять велику кількість обмежених ресурсів і нестаціонарних пристроїв IoT, кожен з яких має різні можливості, конфігурації та домени користувача. Наприклад, нові комерційні мережеві протоколи повітряних дронів потребують зв'язку та обробки даних майже в режимі реального часу через мережу з обмеженою пропускною здатністю. Існує безліч перешкод для використання традиційних засобів для таких систем: підтримка

засобів для таких мереж IoT вимагає значних інвестицій в інфраструктуру; засоби вимагають передачі та перевірки ланцюжків сертифікатів на стороні відправника/верифікатора. Ці додаткові витрати на зв'язок та обчислення можуть створити серйозне вузьке місце для мобільних пристроїв Інтернету речей (наприклад, повітряних дронів [83]), яким потенційно потрібно взаємодіяти з низкою пристроїв. У деяких випадках ці ланцюжки сертифікатів можуть бути більшими, ніж фактичні вимірювання/команди, що передаються, і, отже, можуть бути домінуючою вартістю для цих програм.

Криптосистеми на основі ідентифікації та безсертифікатні криптосистеми пропонують неявну сертифікацію, а отже, можуть пом'якшити вищезгадані перешкоди. В криптосистемах на основі ідентифікації публічний ключ користувача походить від його ідентифікаційної інформації, і система покладається на повністю довірену третю сторону. Він називається генератором приватних ключів, щоб видавати приватні ключі користувачів. Та зображує шифрування, при якому користувач автентифікується і отримує закритий ключ, що відповідає його ідентичності. Відправник може використовувати це як відкритий ключ для запуску шифрування. Ця криптосистема потенційно підходить для програм, де налаштування системи виконується та керується довіреною централізованою організацією. У безсертифікатних криптосистемах довіра знижується, дозволяючи приватному ключу користувача складатися з двох частин. Один обчислюється користувачем, а інший засобами. Тоді, користувач обчислює свою пару ключів, а потім працює, як у першому випадку, щоб отримати іншу частину закритого ключа. Безсертифікатні криптосистеми підходять для архітектур, які можуть не припускати повністю довірену третю сторону, де рівень довіри до ключів подібний до традиційних центрів сертифікації.

Криптосистеми на основі ідентифікації та безсертифікатні криптосистеми мають свої переваги і недоліки, тому можуть використовуватися в різних застосунках IoT. Отже, очікується, що будуть різні групи користувачів, які

покладаються на такі варіанти криптосистем, що ініційовані в різних доменах/системах. Наприклад, один з варіантів таких криптосистем вимагатиме від дронів, які перебувають під повним контролем, взаємодіяти з іншими дронами (наприклад, персональними [83]) для забезпечення безпечної роботи. Використовуючи криптографію на своїх дронах, можуf мати повний контроль над операціями своїх дронів-доставників, уникаючи додаткових витрат традиційних засобів. Однак є сильне припущення, що інші дрони, за межами мережі, приймуть подібне криптографічне налаштування для забезпечення безпечних і надійних операцій. Наприклад, персональні користувачі рідко довіряють будь-якій третій стороні повний контроль і знання про діяльність своїх дронів. Наскільки відомо, існує значна прогалина в дослідженнях щодо забезпечення безперебійного зв'язку між користувачами, які зареєстровані в різних доменах. Це потенційна перешкода для широкого розгортання ефективних безсертифікатних рішень у гетерогенних середовищах. Крім того, важливо ще більше підвищити обчислювальну ефективність методів таких криптосистем, щоб забезпечити низьку наскрізну затримку, яка необхідна застосункам IoT із затримками.

Розглянемо нову серію схем шифрування з відкритим ключем, цифрового підпису та обміну ключами, які дозволяють користувачам з різних доменів ідентифікаційних та безсертифікатних криптосистем безперешкодно спілкуватися. Наскільки відомо, це перший набір безсертифікатних криптосистем, які досягають такої сумісності та ефективності, а отже, підходяща альтернатива для систем IoT з обмеженими ресурсами, таких як комерційні повітряні дрони. Ідея цих конструкцій полягає у створенні спеціальних алгоритмів генерації ключів, які використовують адитивну гомоморфну властивість експонент та функцій без покриття, щоб дозволити користувачам включати свої приватні ключі в ключі, надані центром, без фальсифікації. Ця спеціальна конструкція застосовна до алгоритмів для ідентифікаційних та безсертифікатних криптосистем, і тому вона дозволяє безперебійний зв'язок між криптосистемами. Ця стратегія також знижує вартість

онлайн-операцій і дозволяє розроблюваним схемам досягати нижчої наскрізної затримки порівняно з аналогами.

Сумісні схеми ідентифікаційних та безсертифікатних криптосистем, колм користувачі з різних доменів і рівнів довіри можуть використовувати ідентичні алгоритми шифрування, підпису та обміну ключами для обміну даними без будь-яких додаткових витрат.

Розглянемо ефективність обчислень та зв'язку. На основі проведеного аналізу, нові схеми пропонують переваги в продуктивності порівняно зі своїми аналогами. Подібно до інших криптосистем ідентифікаційні та безсертифікатні криптосистеми схеми усувають бар'єр передачі та перевірки сертифікатів, а отже, пропонують значну ефективність комунікації в порівнянні з деякими з найефективнішими схемами на основі ключів. Ця перевага зростає пропорційно розміру ланцюжка сертифікатів. Ці схеми перевершують аналоги без сертифікатів за переважною більшістю показників ефективності. Наприклад, наскрізна затримка в розглядуваних схемах шифрування на 35% нижча, ніж у найефективніших аналог. Ці схеми підпису досягають швидшої наскрізної затримки, оскільки порівняно з аналогами досягають нижчої наскрізної затримки для ключових схем обміну.

Реалізація з відкритим вихідним кодом цих схем на апаратному забезпеченні та 8-розрядному мікропроцесорі показала порівняння їх продуктивності з безліччю їх аналогів, охопивши деякі з найбільш ефективних традиційних схем.

Розглянемо систему та модель безпеки. Введемо визначення схем шифрування та підпису на основі ідентичностей та безсертифікатів, а також моделі безпеки для безсертифікатного шифрування та схем підпису.

Схема шифрування на основі ідентичності складається з чотирьох алгоритмів: якщо вказано параметр безпеки, то вибирається головний секретний ключ; він обчислює головний відкритий ключ та параметри системи (неявне введення для всіх наведених нижче алгоритмів); отримавши ідентифікатор посвідчення та msk, він обчислює значення зобов'язання та приватний ключ;

якщо задано повідомлення, то відправник обчислює зашифрований текст. Заданий зашифрований текст та закритий ключ приймача приймач повертає або відповідний відкритий текст.

Схема підпису на основі ідентичності визначається чотирма алгоритмами.

Безсертифікатна схема шифрування визначається шістьма алгоритмами. Задають параметр безпеки. Він створить головний секретний ключ. Головний відкритий ключ і параметри системи - неявне введення для всіх наведених нижче алгоритмів. Ідентифікатор користувача обчислює її секретне значення та відповідний пароль. Задані номери обчислює частковий закритий ключ і відповідне йому відкрите зобов'язання, яке задане ідентифікатором користувача.

Відправник обчислює зашифрований текст. Задано зашифрований текст і закритий ключ приймача, то приймач повертає або відповідний відкритий текст, або вкаже, що він недійсний.

Модель безпеки схем, заснованих на ідентифікації, трохи сильніша, ніж у традиційних схем на основі без ідентифікації. Точніше, зловмисник може запитувати закритий ключ будь-якого ідентифікатора користувача, крім ідентифікатора цільового користувача. Розглянемо проєктовані схеми дотримуючись моделі безпеки систем на основі ідентифікації. У безсертифікатних системах закритий ключ користувачів складається з двох частин: секретного ключа користувача, який вибирається користувачем; часткового закритого ключа, який надається користувачеві. Тому, слідуючи цьому, природно розглядати два типи супротивників для таких систем.

Штучний інтелект зловмисника типу не має доступу до них або часткового закритого ключа користувача, але може замінити публічний ключ будь-якого користувача на публічний ключ на свій вибір. Однак, у розглядуваній моделі безпеки, оскільки використовуємо метод прив'язки, заміна відкритого ключа призведе до фальсифікації часткового закритого ключа і, очевидно, закритого ключа. Тому, дотримуючись такої гіпотези, дозволяємо запитувати секретний

ключ користувача. Ця модель також може бути розширена, щоб дозволити замінювати відкритий ключ користувача.

Передбачається, що супротивник типу є шкідливим програмним забезпеченням. Володіючи знаннями про ключ, він може запитувати частковий закритий ключ користувача через підбір пароля. За схемою дозволяємо зловмиснику витягувати закритий ключ приватних ключів користувачів. В зв’язку з цим, було запропоновано багато удосконалень моделей безпеки безсертифікатних систем. Розглянемо цю можливу подію в оригінальній моделі, але при цьому відзначаємо, що багато з цих більш жорстких вимог безпеки можуть бути застосовані при необхідності.

Запропонована криптосистема на основі ідентичності. Більшість таких схем без сполучення покладаються на класичні сигнатури при генерації ключів для забезпечення неявної сертифікації. Використання таких сигнатур для побудови схем зазвичай вимагають декількох дорогих операцій (наприклад, скалярного множення), і тому можуть спричинити незначні додаткові витрати на обчислення. Щоб зменшити ці витрати, використовуємо техніку кодування повідомлень і підмножину стійких функцій разом із експонентним добутком властивості степенів для генерації ключів. Це дозволяє підвищити ефективність як для ключів, так і для користувача, оскільки для цього потрібен лише хеш-виклик і додавання кількох точок.

Визначимо п'ять хеш-функцій. Розглядувані схеми використовують аналогічні ключі. Скалярне множення використовується як одностороння функція. Вона неявно автентифікується шляхом включення у вхідні дані. Це аналогічно методу, що використовується в інших безпарних системах на основі ідентичності та безсертифікатних системах. На кроках методу, на відміну від схеми, де відкриті секретні ключі, використовуємо адитивну гомоморфну властивість в експоненті для маскування одноразової сигнатури за допомогою простого ключа. Після цього засіб IoT надішле користувачеві сертифікат через захищений канал.

Розглянемо схему шифрування на основі ідентифікації. Індекси, отримані з функції, використовуються для отримання компонентів із загальносистемного відкритого ключа. Вхід алгоритму є хибним ключем, який задає шифротекст і може бути переобчислений приймачем. Алгоритмом обчислюються значення відповідно до перетворенням.

Схема підпису на основі ідентичності пердбачає перевірку відкритого ключа користувача, який обчислюється через індекси, отримані з виводу. Генерація ключів відбувається алгоритмом. Решта етапів підписання та перевірки схожі на стандартні підписи.

Схема обміну ключами на основі ідентичності така: для схеми обміну ключами запускаємо відповідні функції алгоритму. Відбувається первинне налаштування, а потім дозволяється обмін обом сторонам.

Розглянемо запропоновану безсертифікатну криптосистему. Для того, щоб ці схеми досягли такого ж рівня довіри до третьої сторони, як і в традиційних схемах, використовуємо метод прив'язки. Той самий захищений канал, який використовується для розпізнавання користувача може бути використаний для надсилання зобов'язання користувача. Це дозволяє неявно сертифікувати, і тому будь-які зміни фальсифікують закритий ключ. Про це повідомляє функція алгоритму. Для обчислення значень використовується зобов'язання користувача, де правильність часткового закритого ключа перевіряється спочатку, перш ніж обчислити закритий ключ.

Схема безсертифікатного шифрування та схема безсертифікатного підпису базуються на алгоритмах налаштування та генерації ключів і вони такі ж, як у стандартному алгоритмі.

Безсертифікатна схема обміну ключами з огляду на сумісність цих схем після того, як початкові алгоритми налаштування системи і генерації ключів відбудуться, то здійсниться обмін ключами і він буде ідентичний запропонованому в схемі обміну ключами на основі ідентичності.

Сумісність схем на основі ідентифікації та безсертифікатних схем у

пропонованих схемах використовує адитивну гомоморфну властивість експоненту, коли в алгоритмі включається додавання зобов'язань. Отримавши результат, користувач використовує гомоморфну властивість, щоб змінити ключ без його фальсифікації та отримати відповідь. Пропоновані схеми не пропонують сумісності, оскільки частковий закритий ключ є зобов'язанням до хешу ідентичності користувача, без гомоморфної властивості. Крім того, така схема не виводить жодних допоміжних значень для включення зобов'язань користувача до неї. Тому ці дві схеми сумісні завдяки спеціальній конструкції алгоритмів генерації ключів. Таким чином, після того, як користувачі обчислили/отримали свої ключі від третьої сторони, інтерфейс основних криптографічних функцій (наприклад, шифрування, дешифрування, підпису тощо) ідентичний в обох системах, тому користувачі можуть безперешкодно взаємодіяти з користувачами в різних сферах. Наприклад, шифротекст, що виводиться в алгоритмі може бути розшифрований користувачем в налаштуваннях, заснованих на ідентичностівід. Алгоритм стосується і схем підпису і обміну ключами, які запропоновані. Запропонована методика доведення аналогічна відомим та імітує реальне середовище. Він знає секретні значення у схемі і намагається вбудувати випадковий екземпляр задачі. Він встановлює частину відкритого ключа цільового користувача як частину зашифрованого тексту виклику та використовує чотири списки, щоб відстежувати випадкові відповіді списку і відповідно до експерименту відповідає на запити.

Штучний інтелект ініціює другий раунд запитів, аналогічних наведеним вище, з обмеженнями, визначеними у ньому, коли він виводить свій біт прийняття рішень та повертає множину вхідних запитів.

Якщо алгоритм не переривається, а результат зі штучним інтелектом виводить свій біт рішення, то відкритий ключ повинен мати і враховувати формування зашифрованого тексту виклику. Він повинен виконуватися, де відомий алгоритм. Отже, відповідь на випадковий випадок задачі може бути

отримана при вивченні вибору запитів відкритого ключа.

Спочатку розглянемо моделювання алгоритму дешифрування. Якщо вхудне значення нульове, то можна побачити, що симуляція ідеальна. Для одиничного значення помилка може виникати в тому випадку, якщо все є коректним, але ніколи не запитувалися різні ключі відповідно для трьох аргументів-функцій. Для перших двох хеш-функцій ймовірність того, що вона є дійсною, якщо запит ніколи не був зроблений, також враховує запит без урахування етапу перевірки в моделюванні. Тому ймовірність того, що це може статися, дорівнює одиниці. Тому, якщо вищевказана ймовірність має місце, то можна вирішити пробсхему, знайшовши та обчисливши значення зі списку. Оскільки розмір списку та ймовірність того, що алгоритм буде успішним у вирішенні, якщо алгоритм зловмисника може порушити безпеку через схеми шифрування після запитів до випадкових чисел. Запити до списка дешифрування та до списка з можливістю вилучення секретного ключа з певною ймовірністю, тоді існує ще один алгоритм, який запускає функцію як підпрограму і розбиває випадковий екземпляр.

Маючи доступ до випадкових чисел і зберігаючи списки, подібні до розглянутих, претендент може імітувати невідмінне середовище і відповідати на його запити, подібні до розглянутого прикладу з модельованих прикладів. Відповідно до нього може запитувати секретний ключ усіх користувачів, за винятком ідентифікатора цільового користувача. Алгоритм знає приватних значень у схемі і намагається вбудувати випадковий екземпляр задачі. У запиті відкритого ключа він визначає ймовірність вбудовування у цільове значення та встановлює частину зашифрованого тексту виклику.

Після того, як штучний інтелект виводить підробку, алгоритм може витягти розв'язок задачі, оскільки він має секретні значення.

Атака з використанням штучного інтелекту на заміну відкритого ключа не є практичною, оскільки вона фальсифікує приватний ключ.

Дійсно, якщо алгоритм з використанням штучного інтелекту замінить

значення новими значеннями, які він може знати відповідним секретним ключем, то існуючий ключ буде фальсифікований, оскільки це також сфальсифікує поточний компонент часткового закритого ключа, оскільки він обчислюється на основі індексів, отриманих шляхом обчислення. Також, якщо алгоритм з використанням штучного інтелекту може отримати оригінал за умови, що він є загальнодоступним, то він може обчислити ключ, однак є лише зобов'язанням і не розкривається жодна інформація. Атака на заміну відкритого ключа безпеки можлива, якщо штучний інтелект запитує новий частковий закритий ключ для кожного нового.

Якщо супротивник має алгоритм з використанням штучного інтелекту може порушити безпеку схеми підпису, запропонованої в алгоритмі, то можна побудувати інший алгоритм, який запускає допоміжну функцію як підпрограму і розбиває випадковий екземпляр.

Дозволяємо алгоритму з використанням штучного інтелекту бути таким, як у попердньому припущенні, тоді можемо побудувати інший алгоритм, який використовує штучний інтелект як підпрограму, і після успішної підробки вирішує випадковий екземпляр. Він знає кілька секретних значень і, подібно до поперднього випадку встановлює частину відкритого ключа цільового користувача.

Більшість кроків моделювання схожі на ті, що були в попередньому випадку. Наприкінці фази моделювання штучний інтелект виводить сигнатуру підробки, потім використовує розгалуження, щоб знову запустити супротивника, для того щоб отримати другу підробку, використовуючи ту саму випадкову стрічку.

Маючи дві підробки та знання ключів алгоритм може обчислити та розв'язати завдання. Зауважимо, що безпека схеми буде нежорсткою через розгалуження. Вибір параметрів слід вибирати так, щоб ймовірність встановлення значення була незначною. Враховуючи, що оскільки кількість індексів, довжина яких становить біт та вибираються з хеш-виходом, впливає на

продуктивність схеми, то розглянемо деякі варіанти разом з наслідками для продуктивності.

Спочатку представляємо аналітичний, а потім експериментальний аналіз продуктивності та порівняння схем з аналогами. Розглянемо онлайн-операції (наприклад, шифрування, підписання, обмін ключами), для яких ці схеми мають однакові алгоритми, а не на одноразових офлайн процесах, таких як налаштування та генерація ключів. Оскільки у випадку онлайн-операції ідентичні в цих криптосистемах, то розглядатимемо їх в наступних таблицях.

Розглянемо вартість перевірки сертифікату для схем в традиційних системах. Враховуємо лише вартість перевірки та повідомлення вартості одного сертифікату, що є дуже консервативним, оскільки на практиці у ланцюжку сертифікатів є як мінімум два сертифікати. У деяких сценаріях це число може досягати десяти сертифікатів. Аналітичний аналіз та порівняння ефективності представляємо через детальне аналітичне порівняння ефективності цих схем з їх аналогами для шифрування/дешифрування відкритих ключів, цифрового підпису та обміну ключами відповідно. Ці схеми мають значно нижчі додаткові витрати на зв'язок, ніж їхні аналоги на основі сертифікатів у всіх криптосистемах, оскільки вони не вимагають передачі сертифікатів. Це також призводить до значного збільшення пропускної здатності як обчислювальна ефективність, оскільки додаткові витрати на сертифікаційну перевірку також скасовуються. Крім того, майже у всіх випадках ці схеми також пропонують нижчі додаткові витрати на наскрізні обчислення порівняно з аналогами на основі сертифікатів. Ці схеми також пропонують нижчу наскрізну затримку обчислень, ніж у всіх їхніх аналогів у всіх криптосистемах, із загалом однаковими розмірами приватного та відкритого ключів. Однак розмір головного відкритого ключа пропонованої схеми більший, ніж у всіх їхніх аналогів.

Тепер детальніше розглянемо деталі аналізу продуктивності та порівняння з експериментальними результатами. Проводитимемо експерименти як на

комп’ютерному обладнанні, так і на бюджетних вбудованих пристроях, які зазвичай зустрічаються в системах IoT, щоб об'єктивно оцінити продуктивність цих схем, а також їх аналогів.

Реалізація з відкритим вихідним кодом у цих експериментах. Реалізовуватимемо ці схеми на еліптичній кривій, яка пропонує швидкі операції з еліптичними кривими для безпеки. Створені екземпляри цих випадкових чисел за допомогою хеш-функції, яка забезпечує високу ефективність і безпеку. Для цих параметрів вибрано сертифікати. Використовуватимемо найефективнішу альтернативу для них для схем, які потребують сполучення. Алгоритми шифрування і дешифрування цих схем більш ефективні, ніж їх аналоги в налаштуваннях на основі ідентичності та без сертифікатів. Зокрема, наскрізна затримка наших схем нижча, ніж у стандартних, що особливо підходить для повітряних дронів. Додаткові витрати на зв'язок нижчі в безсертифікатних схемах та схемах, заснованих на ідентифікації, оскільки немає необхідності в передачі сертифікатів. Ці схеми мають найшвидші алгоритми перевірки серед усіх аналогів. Це, знову ж таки, пов'язано з новим способом отримання ключів користувача, що призводить до швидшої наскрізної затримки порівняно з найефективнішим ідентифікатором та безсертифікатним аналогами відповідно.

Відомі схеми поряд з цими схемами вимагають скалярного множення при генерації сигнатур. Їх експериментальні витрати різняться. Причиною такої розбіжності є той факт, що вартість скалярного множення над генератором є швидшою, ніж скалярного множення над будь-якими точками кривої, і ці відмінності враховуються в експериментальних оцінках. Показники цих схем аналогічні аналогам в традиційних умовах з сертифікатами. Однак вони перевершують найефективніші аналоги в безсертифікатних налаштуваннях, маючи нижчу наскрізну затримку та менше навантаження на зв'язок.

Для цих схем оцінено їх вартість на основі мікробенчмарків та реалізації 8-бітного контролеру з еліптичною кривою, що реалізує криву, яка підтримує сполучення на 8-розрядних мікропроцесорах і забезпечує відповідно безпеку.

Ці схеми перевершують всі свої аналоги на основі ідентифікації та безсертифікатів і мають більш ефективний алгоритм шифрування, ніж сертифікатні. Розроблені алгоритми дешифрування, хоча і є більш ефективними, ніж всі їх аналоги, засновані на ідентифікації та без сертифікатів, дещо менш ефективні, ніж алгоритми з сертифікатною схемою. Подібно до тенденції аналітичних показників, ці фірмові схеми перевершують аналоги. Алгоритм підпису цих схем є одним з найбільш ефективних, в той час як алгоритм перевірки перевершує всі аналоги з аналогічними додатковими витратами на зв'язок. Основним обмеженням цих схем є розмір головного відкритого ключа. Якщо в різних доменах є різні ключі, то і користувачі часто спілкуються з користувачами в цих доменах. Тому, є потреба зберігати різні ключі. В іншому випадку користувачам потрібно зберігати ключ лише для власних систем. Можемо зменшити розмір ключа в обмін на невелику втрату продуктивності. Наприклад, можемо зменшити розмір ключа в чотири рази.

Основна відмінність пропонованої схеми полягає в тому, щоб зосередитися на досягненні взаємосумісності між ідентичними та безсертифікатними комбінаціми в схемі з високою ефективністю, по відношенню до існуючих альтернатив.

Ідея криптографії була запропонована для використання в схемі з використанням білінійного сполучення. Щоб отримати повні гарантії безпеки адаптивної ідентичності, обраного шифротексту без шкоди для продуктивності, використано розширену версію схеми в моделі випадкового списку. Однак доповнена версія також вимагає багаторазових обчислень сполучення в алгоритмі дешифрування. Було запропоновано кілька схем безпарного підпису із полегшеною схемою сигнатур зі зведенням до задачі дискретного логарифма.

Криптографія була запропонована для вирішення проблеми депонування приватного ключа в системах.

Таким чином, запропонована схема шифрування, а також схеми підпису та обміну ключами.

2.3 Метод криптографічного захисту протоколів в засобах комунікації інтернету речей

Для подання методу криптографічного захисту протоколів в засобах комунікації інтернету речей спочатку формалізуємо предметне поле дослідження.

Введемо для засобів IoT множину та відобразимо засоби елементами цієї множини так:

$$M = \{m_1, m_2, \dots, m_{n_M}\}, \tag{2.1}$$

де n_M- кількість засобів IoT.

Задамо абстрактну модель системи з IoT так:

$$M_{IoT} = \langle M, G \rangle, \tag{2.2}$$

де G- граф, в якому вершинами є елементи множини M.

Формула (2.2) описує зв'язки, а оскільки IoT – це концепція зв'язку, то таке задання є коректним.

Оскільки комунікації між елементами множини M потребують забезпечення, тоді розробимо метод криптографічного захисту протоколів в засобах комунікації інтернету речей.

Щоб досягти переходу до квантово-захищених обчислень, протоколи безпеки, такі як SSH, VPN, IPSec, SSLTLS тощо, також необхідно оновити. Ці протоколи потрібно поєднати з існуючими протоколами, а також необхідно ввести додатковий рівень для встановлення безпечного зв'язку для боротьби з контрзаходами. Ця зміна має наслідки для асиметричного шифрування та алгоритмів генерації ключів, вимагаючи збільшення розміру ключа симетричних криптографічних алгоритмів. У результаті це також впливає на

продуктивність і пропускну здатність. Постачальникам апаратного забезпечення також потрібно буде оновити своє обладнання, щоб узгодити його з новими алгоритмами.

Основні кроки методу криптографічного захисту протоколів в засобах комунікації інтернету речей:

1) здійснимо асиметричне шифрування для приватного обміну секретним ключем симетричного шифрування;

2) використаємо симетричний ключ шифрування для шифрування обміну.

Деталізуємо ці кроки.

Кроки генерації ключа:

1) надсилати послідовність біт з вузла m_i;

2) для кожного отриманого повідомлення випадковим чином обирати будь-яку одну основу з двох основ системи числення;

3) зберігати використані бази та отримані результати;

4) публічно повідомляти про отримання повідомлень всім вузлам з множини M;

5) зберігати лише ті події, для яких використовувалися однакові бази;

6) обчислити частоту помилок для тестових подій, і якщо вона вища за деяке попередньо визначене порогове значення, вони переривають процедуру; інакше вони переходять до наступного кроку;

7) перетворити дані в класичні біти 0 і 1, відомі як необроблений ключ; після цього застосовувати класичні процеси для виправлення помилок і посилення конфіденційності для отримання остаточного ключа.

Асиметричне шифрування вимагає занадто багато ресурсів процесора. Асиметричне шифрування повільніше, ніж симетричне шифрування. Тому комп’ютери безпечно обмінюються ключем симетричного шифрування, завдяки асиметричному шифруванню, і можуть обмінюватися даними швидше, постійно використовуючи симетричне шифрування.

Системна архітектура типової гібридної програми SSH знаходиться між

протоколами прикладного рівня та TCP. Під час передачі SSH приймає трафік даних від прикладного рівня та додає необхідний захист безпеки перед передачею його на нижчі рівні. BB84 використовується як протокол Quantum Cryptography у цій архітектурі. SSH використовує мережу для надсилання лише трафіку, що відповідає класичним публічним каналам обміну, необхідним для реалізації BB84. Останній тип трафіку передається під час рукостискання SSH і має бути автентифікованим, щоб запобігти атакам типу "людина посередині". Щоб уникнути атак типу "людина посередині" на протокол. Насправді система вразлива до нападу «людина посередині». Однак майбутні з'єднання з цим сервером залишаються безпечними, оскільки під час першого з'єднання не було підроблено. Це вірно, навіть якщо взято ключ хоста серверу.

Другим рівнем безпеки, який забезпечує цей підхід, є підвищена автентифікація та обмін даними за допомогою використання квантового ключа, оскільки метод пароля є небезпечним. З іншого боку, відкритий ключ і автентифікація на основі хоста стійкі до атак. Спостерігаючи за обміном ключами, зловмисник не зможе визначити ключ сеансу. Замість цього йому потрібно буде почати активний штурм. Він бере участь у багатьох обмінах з кожним партнером, в результаті чого отримує кілька ключів. З кожною стороною здійснюється ряд різних обмінів, щоб отримати свої ключі від клієнта та серверу. Якщо це станеться, обмін ключами з обох сторін обміну ключами призначений для видалення ідентифікаційних номерів сеансу з обох сторін обміну ключами. Це вірно як для SSH-1, так і для SSH-2. На кожній стороні є два окремих ідентифікатори сеансу. Коли клієнт надає цифровий підпис для відкритого ключа або автентифікації на основі хосту, цифровий підпис містить ідентифікацію даних, підписаних клієнтом. Отже, зловмисник не може просто передати автентифікатор, наданий клієнтом, на сервер і не має способу змусити клієнта підписати будь-який інший ідентифікатор сеансу.

Оскільки SSH побудовано на основі TCP, він сприйнятливий до атак, які використовують слабкі місця TCP та IP. Гарантії конфіденційності, цілісності та

автентифікації, що надаються технікою, значно зменшують цю вразливість до атак типу «відмова в обслуговуванні». Оскільки TCP/IP стійкий до проблем мережі, таких як перевантаження та втрата з’єднання, TCP/IP використовується для передачі даних. Якщо хакеру вдасться зламати маршрутизатор, IP може його обійти. Очікувалося, що зловмисник, який вводить фальшиві мережеві пакети, не зможе його перемогти. Неможливо визначити джерело керуючих повідомлень TCP або IP. Отже, протокол TCP/IP має різноманітні слабкі сторони, якими можна скористатися, наприклад SYN-лавину, яка є різновидом лавинної передачі пакетів. Через частоту, з якою цей пакет отримується, отримувач повинен регулярно споживати ресурси, щоб підготуватися до наступного з’єднання. Якщо зловмисник передає велику кількість цих пакетів, стек TCP одержувача може бути перевантажений і не зможе встановити з’єднання. У випадку TCP-з'єднання будь-яка сторона може надіслати RST-пакет у будь-який момент, і в результаті з'єднання буде миттєво розірвано. Пакети RST можуть бути миттєво введені в мережу, в результаті чого будь-яке цільове TCP-з’єднання буде миттєво припинено та відключено.

Хакер, який не може прочитати мережевий трафік, може отримати цінну інформацію, просто спостерігаючи за нею та записуючи обсяг надісланих даних, а також адреси джерела та призначення, а також дату та час передачі. У випадку іншої організації несподіваний сплеск трафіку може свідчити про початок комерційних відносин. Шаблони трафіку також можна використовувати для прогнозування того, коли найімовірніше відбудеться резервне копіювання або коли найімовірніше станеться напад на відмову в обслуговуванні. Можливо, тривалий період спокою під час з’єднання SSH із робочого столу системного адміністратора вказує на те, що він вжив певних дій. Кожного разу, коли системний адміністратор повідомляє, що він або вона залишив об’єкт, це чудовий час, щоб проникнути електронно чи фізично та скористатися ситуацією. Атаки на SSH, засновані на аналізі трафіку, не допускаються. Оскільки з’єднання SSH часто адресуються на добре відомий порт, наш підхід є дуже швидким для

визначення з’єднань SSH. Приховати результати аналізу трафіку. Щоб уникнути кореляції активності, реалізація SSH може транслювати випадковий трафік через неактивне з’єднання, щоб запобігти кореляції активності.

У порівнянні між стандартним протоколом SSH і розробленим, встановлено, що більш стійкіший розроблений до різноманітних нападів. Звичайний протокол SSH не забезпечує захисту від атак, які переривають або перешкоджають формуванню TCP-з’єднань, які починаються з IP- і TCP-атаки. З іншого боку, шифрування SSH і автентифікація хоста ефективні проти атак, які використовують маршрутизацію для читання конфіденційної інформації або перенаправлення з’єднання на скомпрометований сервер. Атаки, які перенаправляють або змінюють дані TCP, з іншого боку, зазнають невдачі, оскільки SSH ідентифікує їх, але вони також не вдаються, оскільки SSH їх не виявляє, що призводить до розриву з’єднання SSH. Через те, що під час використання Quantum SSH весь зв’язок перевіряється на етапі формування з’єднання, протокол захищений від цієї вразливості. Злом паролів є ще одним потенційно смертельним нападом. SSH значно підвищує безпеку паролів, шифруючи паролі, які надсилаються через мережеве з’єднання.

Пароль, з іншого боку, є слабким типом автентифікації, який слід використовувати з особливою обережністю. Важко вгадати пароль, який би запам’ятовувався і не був очевидним для інших, якщо його не надати. Протокол є успішним з точки зору шифрування, оскільки він пропонує ряд різних методів шифрування даних, які надходять через мережу. Наслідком цього є те, що можна побудувати криптографічний рівень, стійкий до такого роду нападів.

Квантова технологія не повністю розгорнута на ринку, але це не заважає використовувати її надійність для вдосконалення класичних рішень, доступних у цій галузі. У зв’язку з цим об’єднано квантову технологію, щоб підвищити ефективність і безпеку класичного криптографічного підходу. Багато перевірених концепцій класичної криптографії, такі як одноразовий буфер, багатостороння криптографія, делеговані обчислення та

гомографічне шифрування, можна використовувати для реалізації квантових основ.

Таким чином, розроблено метод криптографічного захисту протоколів в засобах комунікації інтернету речей, кроки якого деталізовано з врахуванням номерів вузлів.

2.4 Висновки до другого розділу

Розроблено схему підпису, яка відповідає вимогам щодо мінімальної затримки деяких систем IoT у реальному часі. Це досягається за рахунок використання гомоморфної властивості односторонньої функції, що лежить в основі, і методу попередніх обчислень. Запропонована схема безпечна в моделі випадкового списку при жорсткості вимог до неї.

Ідея криптографії була запропонована для використання в схемі з використанням білінійного сполучення. Щоб отримати повні гарантії безпеки адаптивної ідентичності, обраного шифротексту без шкоди для продуктивності, використано розширену версію схеми в моделі випадкового списку. Однак доповнена версія також вимагає багаторазових обчислень сполучення в алгоритмі дешифрування. Було запропоновано кілька схем безпарного підпису із полегшеною схемою сигнатур зі зведенням до задачі дискретного логарифма.

Розроблено метод криптографічного захисту протоколів в засобах комунікації інтернету речей, кроки якого деталізовано з врахуванням номерів вузлів.

3 МЕТОД ШВИДКИХ ПІДПИСІВ З КОМПАКТНИМ КЛЮЧЕМ В СИСТЕМАХ З IoT

3.1 Подання підписів та компактних ключів в системах з IoT

Квантові алгоритми поліноміального часу для розкладання на множники і дискретного логарифму забезпечили загрозу квантових обчислень над криптографією з відкритим ключем. Оскільки традиційна криптографія з відкритим ключем зламана квантовими атаками, альтернативні схеми з постквантовою безпекою повинні бути визначені до того, як квантові комп'ютери стануть практичними. Нещодавно було оголошено про можливість переходу на криптографію безпеки в найближчому майбутньому.

Щоб уникнути поспішного переходу від поточних традиційних криптосистем до систем постквантової безпеки, вже ініціювали перший раунд стандартизації криптографії. Було запропонувано першу схему одноразового підпису постквантової безпеки, яку засновано на ідеї фіксації секретних ключів за допомогою односторонніх функцій. Пізніше запропонували різні варіанти підпису Лемпорта з метою мінімізації відкритого ключа та розміру підпису відповідно.

Сьогодні цифрові підписи на основі решіток, хеш-функцій, кодів, багатовимірних і симетричних примітивів є провідними практичними кандидатами з постквантової безпеки. Сигнатура на основі решітки передбачає, що існує дві основні категорії схем підпису на основі решітки. Одна з них полягає в тому, щоб зосередитися на твердості задач від найгіршого до середнього випадку зі стандартними ґратками. Незважаючи на те, що вони забезпечують надійний захист, вони страждають від дуже великих розмірів параметрів порядку кількох мегабайт.

Інший напрямок, з більшою увагою до ефективності, базується на кільцевих аналогах стандартних задач на ґратку. Більшість з цих ефективних схем, однак, страждають від дорогих операцій вибірки з високою точністю над

деяким нормальним розподілом під час підписання. Послаблення цієї вимоги, шляхом вибірки тільки над цілими числами, дозволило отримати більш ефективні конструкції, що базуються на перетворенні безсертифікатних схем.

Схему підпису хеш-функцією можна підписувати меншою сигнатурою та розміром ключа, але з повільнішим підписанням через дорогу дискретну гаусову дискретизацію через ґратку. Гаусова вибірка не тільки тягне за собою зниження продуктивності, але і схильна до атак по сторонньому каналу. На даний момент уникнення таких побічних каналів при реалізації вважається дуже складним і схильним до помилок. Результат виходить шляхом застосування перетворення на ефективний доказ з нульовим розголошенням, що призводить до дуже коротких розмірів відкритого ключа і приватного ключа. Однак схема страждає від великих розмірів сигнатур з відносно повільними (в порівнянні зі схемами на основі решітки) алгоритмами підпису і перевірки.

Тому, пропонуємо просту та ефективну схему підпису постаквантової безпеки в системах з IoT. Вона заснована на примітивах.

Новий алгоритмічний дизайн можна розглядати як нову модифікацію конструкції, яка базується на односторонніх функціях. Використовуємо підхід з узагальненим компактним набором. Адитивно гомоморфна властивість дає дві переваги: вона дозволяє стискати розмір сигнатури в порівнянні з одноразовими сигнатурами; це призводить до абсолютно нової парадигми розширення.

Розглянемо нечисленні підписи на основі хешу в схемах без стану, що підтримують поліноміально обмежену кількість підписів.

Безпека розробленої схеми базується на односторонності сімейства функцій. Ці властивості зводять до найгіршого випадку задач у циклічних ґратках.

Покращена стійкість бічних каналів показана через гаусову вибірку і схильна до атак на сторонньому каналі. Оскільки бічні канали є властивістю алгоритму реалізації, то їх можна дещо пом'якшити за допомогою відповідних методів реалізації. Однак відомо, що процес усунення бічних каналів в

алгоритмах вибірки Гаусса є важким і схильним до помилок. Розроблена схема не вимагає будь-яких варіантів відбору проб за Гауссом. Натомість, вона використовує рівномірну вибірку над обмеженим доменом та вибірку відхилення, щоб перевірити, чи вихідна сигнатура знаходиться в безпечному діапазоні.

Алгоритм перевірки розробленої схеми дуже ефективний. Він включає лише два виклики хеш-функції, односторонній виклик функції та додавання векторів. Це робить розроблену схему найбільш перевіреною обчислювально ефективною альтернативою серед своїх аналогів. Наприклад, за допомогою ключа з захистом дозволяє перевіряти багато повідомлень в секунду на комп'ютерному обладнанні, що становить швидше, ніж одна з його найшвидших альтернатив.

Розглянемо швидке підписання. Генерація сигнатур розробленої схеми не вимагає будь-яких дорогих операцій (наприклад, гаусової вибірки), а лише виклику функції, який, як було продемонстровано, є швидким, поряд з невеликою постійною кількістю викликів псевдовипадкової функції та невеликою кількістю векторних доданків. Це робить покоління розробленої схеми найшвидшим у порівнянні з аналогами.

Приватні ключі в розробленої схеми такі ж малі, як є найменшими серед існуючих схем постквантової безпеки. Крім того, на відміну від деяких інших схем є ефективнішими,

Підписувачу не потрібно зберігати попередньо обчислену таблицю для використання в процесі вибірки. Поряд з обчислювальною ефективністю підпису, ця властивість робить розроблену схему реальною альтернативою для пристроїв низького класу.

Параметри, що налаштовуються базуються на новій алгоритмічній архітектурі і дозволяє пропонувати різні компроміси щодо швидкості та сховища на основі вибору параметрів. Наприклад, можна попередньо обчислити та зберегти деякі проміжні значення на стороні підписувача в обмін на швидший

підпис. Також, можна зменшити відкритий ключ та/або розмір підпису, але зі збільшенням наскрізної затримки, або збільшити розмір підпису, щоб забезпечити нижчу частоту дискретизації відхилень для швидшого підписання. Деякі з цих варіантів переюувають на межі можливих компромісів.

Всі ці бажані властивості досягаються за рахунок більшого відкритого ключа. Тим не менш, існує багато випадків, коли зберігання більшого відкритого ключа є допустимим. Наприклад, винахідливий командний центр, який перевіряє велику кількість сигнатур від датчиків, може зберігати такий публічний ключ. Однак, якщо верифікатор строго обмежений пам'яттю і не може дозволити собі зберігати великі публічні ключі, то слід розглянути схеми з меншим відкритим ключем. Оскільки розроблена схема побудована на основі сигнатурної схеми, яка використовує бієктивну функцію та односторонню функцію, то її просте узагальнення для побудови теж надає ефект.

Схема сигнатур складається з трьох алгоритмів. Концептуальною відправною точкою є конструкція, яка сама по собі є варіантом схеми. Закритий ключ складається з безлічі випадкових значень, а відкритий ключ складається з відповідних зображень - одностороння функція. Звичайно ж, ці значення можуть бути отримані з маленької множини за допомогою відповідної функції і призводить до мінімального ключа підпису. Щоб підписати повідомлення, підписувач спочатку обчислює і інтерпретує його як послідовність індексів. Тоді підпис складається з мінімальної кількості символів. Щоб перевірити, можна просто порівняти його зі значенням відкритого ключа для кожного відповідного індексу.

В цій парадигмі застосовано підхід, що полягає у використанні адитивно гомоморфного ключа. Зокрема, вибираємо узагальнене сімейство функцій компактного ранця. Це дозволяє стискати підпис наступним чином. Замість цього підпис може містити тільки вказівки. Потім верифікатор може перевірити, що такий підхід призводить до витоку лінійної комбінації секретного ключа. Після помірної кількості сигнатур можна було б розв'язати для всього секретного

ключа за допомогою системи лінійних рівнянь. Щоб цьому завадити, додаємо трохи «шуму». Зокрема, сигнатура складається для відповідним чином розподіленого ключа. При додаванні цього шуму є дві проблеми. По-перше, повинні переконатися, що верифікатор все ще може перевірити такий підпис. Цього можна домогтися, видавши частину ключа. Оскільки вихід довгий, то замість цього видаємо короткий хеш. По-друге, він визначається над деяким кільцем, але може приймати лише короткі входи, тобто входи надходять з підмножини кільця, які не замкнуті при гомоморфній операції. Це ускладнює маскування чутливої суми. Використовуємо наступний підхід відбраково-вибіркового підходу. Беремо зразки шуму з відповідного рівномірного розподілу і перезапускаємо весь алгоритм підписання, якщо результат є «занадто великим» або «занадто маленьким». Нарешті, замість того, щоб вибирати індекси, як у основному алгоитмі вибираємо їх так, що це гарантує, що значення буде зафіксовано перед початком процесу і решту підпису буде згенеровано.

Цей аспект схеми використовується в доказі безпеки, зокрема в узагальненій схемі про розгалуження. Аргумент про розгалуження передбачає, що будь-який супротивник, який генерує підробку в проєктованій схемі, може бути переглянутий так, щоб отримати дві підробки з однаковим ключем. З цих двох підробок можемо порушити односторонність.

Формальний опис розробленої схеми відноситься до односторонньої функції. Його вхід є вектором, а його виходом є відповідне кільце. Функція параметризована відкритим значенням, яке вибирається випадковим чином. Випадковий вибір забезпечує односторонність. Таким чином, він може бути глобальним параметром тобто спільним для всіх користувачів. Вибірка забезпечує рівномірний розподіл по векторах з усіма записами в певному діапазоні допустимих значень. Ця функція може бути реалізована аналогічно іншим ґратковим конструкціям, які використовують рівномірну вибірку. Алгоритм відноситься до псевдовипадкової функції, вихід якої інтерпретується як двійковий вектор і має параметри, пов'язані як з безпекою контролюючи вагу

його входів, так і з імовірностями, пов'язаними з відбором дискретизації.

Випадковий список з вихідною довжиною, який використовується для фіксації підпису перед вибором індексів використовується для вибору індексів. Алгоритм є правильним у тому сенсі, що сигнатура, згенерована за допомогою розробленої схеми завжди буде перевірятися. Це можна показати так. Дано пару повідомлення-сигнатура, що обумовлено детермінованою властивістю хеш-списку. Індекси, створені шляхом обчислення, ідентичні створеним.

Таким чином, для дійсної пари повідомлення-підпис завжди повертатиме одиницю.

Ідея відбраковування вибірки в ґратках вперше була запропонована при побудові ідентифікаційних схем. У розробленої схеми потрібно замаскувати підсумовування секретних ключів випадковим числом. Якщо розподіл рівномірний по всьому кільцю на якому визначено підсумовування, то очевидно, що вся інформація про підсумовування прихована. Однак верифікатор повинен використовувати як вхідні дані для, що можливо лише в тому випадку, якщо число є малим. Отже, індекс повинен бути обраний з деякого обмеженого розподілу.

Розглянемо, як визначається цей розподіл.

Алгоритм редукції не знає всього ключа підпису, тому він використовує свою здатність програмувати випадковий список для генерації імітованих підписів. Зокрема, він вибирає сигнатуру рівномірно випадковим чином, а потім програмує так, щоб сигнатура перевірялася. Припустимо, що алгоритм успішно конструює підробку. Розглянемо перемотування супротивника до точки, де він зробив запит, а потім продовження з незалежною випадковістю. Об'єкт розгалуження стверджує, що з великою ймовірністю супротивник видасть підробку і в цьому випадку. Важливо, що нова підробка міститиме ту саму літеру. Зауважимо, що два підсумовування знаходяться над різними мультимножинами індексів. За умови відсутності зіткнення отримаємо сумісні індекси, якщо є деякий індекс, який з'являється з кратністю рівно один раз. Наші

умови редукції на тому, що індкси завжди сумісні. З незалежною ймовірністю маємо, що вони насправді сумісні відносно спеціального індексу. Сумісність має на увазі, що можемо вирішити з ними завдання пошуку ключа.

Алгоритм редукції знає початкові образи до всіх доданків у правій частині. Таким чином, можна застосувати гомоморфну властивість і записати праву частину, застосовану до значення, відомого алгоритму редукції. Іншими словами, редукція може обчислити передобраз.

Розглянемо детальніше сумісні набори індексів.

Перш ніж більш детально описати редукцію, уточнимо властивості сумісного індексу. Нехай рядки, які кодують мультимножини природним чином, тоді індекси сумісні щодо певного індексу, якщо він з'являється з певною кратністю. Якщо є один фіксований рядок, то інші рівномірно вибрані рядки.

Розглянемо алгоритм скорочення. Маючи супротивника визначаємо алгоритм редукції в алгоритмі. Алгоритм приймає на вхід значення індексів, а також список випадкових відповідей списку, які він буде використовувати для програмування. Цей інтерфейс необхідний для використання схеми з розгалуженням. Він переходить до моделювання гри проти супротивника, імплантуючи певне значення у відкритий ключ і генеруючи симульовані сигнатури. Якщо він успішно генерує підробку, то супротивник виводить її, а також індекс хеш-виклику, що відповідає реальному значенню. Це вказує на схему про розгалуження, що хочемо повернутися до цього запиту і продовжити з новою випадковістю.

Таким чином, отримано подання підписів та компактних ключів в системах з IoT. Отримана схема дає змогу отримати компактні ключі.

3.2 Моделювання розробленої схеми з ключами в системах з IoT

Порівнюємо погляд розробленої схеми в редукції з його поглядом у стандартній грі. Єдиними відмінностями є значення, що вибираються рівномірно,

а не псевдовипадково. Це змінює думку супротивника на незначну величину. Підпис формується у зворотному порядку. Тому, справжні підписи розподіляються рівномірно, отже, ця різниця не впливає на думку супротивника.

Єдина інша відмінність між скороченням і грою полягає в тому, що скорочення може перерватися в разі коли виникає помилка, коли редукція потребує програмування випадкових ключів, але вони вже запитані в потрібній точці. Значення є однорідними, кожне з яких має принаймні декілька біт ентропії. Звідси випливає, що ймовірність того, що такий апріорний запит був зроблений, становить не більше певного числа. Беручи об'єднання, пов'язане з усіма викликами, то загальна ймовірність помилки обмежена.

Тепер можемо розглянути можливість виклику схеми розгалуження за допомогою цього алгоритму. Результатом є алгоритм, який має ймовірність як мінімум виготовлення двох підробок. Ці підробки повинні бути по відношенню до одних і тих же значень через спосіб, у який алгоритм обчислює індекс спеціального запиту ключа, і той факт, що лема про розгалуження гарантує, що цей індекс однаковий в обох схемах. Кожна підробка перевіряється на різне значення.

Нехай є дві підробки, які виведені для повідомлення. Нехай значення у першому випадку менше значення з другого випадку. Коли вони сумісні відносно преобразу, то може бути обчислений ефективно ключ.

З точки зору симетрії, припустимо, що з'являється ключ в першому випадку, але він не збігається за довжиною, яку передбачає другий випадок. З рівняння верифікації для цих сигнатур маємо наступне. Оскільки алгоритм перериваєтся, якщо зіткнення було виявлено, тоді маємо виділення, яке з'являється в лівому підсумовуванні, але не в правому і використання гомоморфної властивості.

Останнім аргументом є значення, яке можна обчислити з відомих значень, і воно є прообразом.

З огляду на те, що супротивник порушує безпеку, як зазначено, то

спочатку будуємо алгоритм редукції/гру. В результаті гра створює підробку з певною ймовірністю, ігноруючи незначні часові терміни.

Потім застосовуємо схему розгалуження. Результатом є алгоритм, який генерує дві підробки з певною ймовірністю.

У випадку, якщо він виводить дві підробки, визначаємо як значення у першій схемі, а значення, що повторилось, як його значення у другій схемі. Обмежимо ймовірність того, що вони сумісні. Однак, оскільки друге значення не розповсюджується незалежно від успіху, то інтуїтивно супротивник може вибрати, чи буде друга схема успішною після того, як побачить результат.

З іншої сторони, нехай значення множини відповідей ключа рівномірно повторюються під час другого запуску схеми. Важливо, що вони розподіляється незалежно від другого ключового значення, тому можна зв'язати ймовірність того, що перше значення сумісне з усіма елементами. Так як друге значення, якщо воно існує, гарантовано є елементом, то це дозволяє припустити про їх сумісність.

Час виконання алгоритму дорівнює часу виконання для виведення двох сигнатур підробки з переважною ймовірністю та час, необхідний для процесів моделювання. Процес налаштування займає для генерації приватних ключів та відповідних відкритих ключів певний час, який ігноруємо. Кожен процес підписання для генерації потребує один відведений та один додатковий момент часу. Кожен хеш-запит вимагатиме тех виокремлення певного часу. Таким чином, загальний час роботи є верхньою межею всього часу.

Відсутність зіткнень функції для розробленої схеми дорівнюють відповідно двом значенням часу як для першого так і для другого випадків з розробленої схеми. Для того, щоб сімейство функцій допустило значне зниження безпеки, то необхідно забезпечити, щоб для деякого значення було досягнення найбільшого часу.

Специфічно з цими часовими параметрами знайти зіткнення в середньому з будь-якою незначною ймовірністю не менш важко, ніж вирішити основну

задачу, тобто на певних видах точкових ґраток, у гіршому випадку. Вибір конкретних параметрів відповідає вимогам, щоб забезпечити сильне зниження безпеки.

Задавши рівномірно випадковий вектор, задача над кільцем просить знайти ненульовий вектор такий, що забезпечує отримання результату з високою ймовірністю.

Підхід до оцінки цієї задачі полягає у вимірюванні часу виконання алгоритмів редукції базису ґратки. Ці алгоритми редукції мають на меті знайти гарні базиси, які складаються з досить коротких і майже ортогональних векторів. Дійсно, дослідження показують, що таке скорочення виконання алгоритму для ґратки з малою розмірністю дозволяє знаходити вектори потрібної довжини.

Використаємо алгоритм, який є найбільш відомим алгоритмом знаходження коротких ненульових векторів в ґратках. Алгоритм починається зі зменшення базису ґратки за допомогою ключа задачі найкоротших векторів у меншій розмірності. Число викликів ключа залишається поліноміальним, однак точне обчислення числа викликів є важким завданням і тому підлягає евристичним підходам. Алгоритм вимагає розв'язання задачі у ґратках з розмірністю не більше розміру блоку. Тому він запускається протягом декількох раундів, щоб знайти остаточний результат. З огляду на зв'язану нормою екземпляру, відповідне значення може бути обчислене, тоді оцінка часу виконання для досягнення обчислюється сумарно. Також, для цього використовуємо співвідношення для визначення найменшого розміру блоку для досягнення належної точності результату. Найновіший класичний розв'язувач працює в часі повільніше, ніж найвідоміший квантовий розв'язувач працює в часі. Розглянемо два типи супротивника, а саме: класичну та постквантову. Для розробленої схеми пропонується три набори параметрів (для трьох рівнів безпеки) і аналізується рівень безпеки кожного з них для згаданих вище типів змагальності. У класичній моделі для створення екземпляра середньої безпеки встановлюємо такі початкові значення, щоб досягти оптимального результату.

Для рекомендованої інстанціації, яка досягає оптимального результату встановлюємо такі значення для створення екземпляра з високим рівнем безпеки. Таким чином, виходячи з аналізу, досягли класичної бітової безпеки для середньої, рекомендованої та високої захищеності в розробленій схемі, на відміну від гратчастих атак відповідно. Для постквантового захисту від ґратчастих атак досягаємо безпеки для середньої, рекомендованої та високої захищеності екземплярів відповідно. Вибір параметрів для розробленої схеми є консервативним.

Комбінаторна задача елемента як зазначено в доказі безпеки передбачає, що параметри повинні бути обрані таким чином, щоб ймовірність була незначним числом. Враховуючи, що оскільки багато індексів, які вибираються з хеш-виведенням випадковим чином, то це дає розмитий результат. Далі потребують подаьшого вибору деякі варіанти разом з їх наслідками для забезпечення та досягнення безпеки/продуктивності.

Квантова випадкова модель ключа розглядає сценарій, коли супротивник має класичний доступ до ключа підпису та квантовий доступ до ключа хеш-функції. Доведено, що для розробленої схеми безпечний стан у моделі випадкового ключа, і тому не надаємо доказів безпеки розробленої схеми. Ця тенденція справедлива для широкого спектру ефективних схем, які в основному засновані на фреймворку, оскільки їхній пристрій пам’яті не є вільним від історії через схему про розгалуження на етапі скорочення. Початкові підходи до отримання безпеки для схем, заснованих на перетворенні, призвели до значно менш ефективних сигнатур, оскільки вони вимагали багаторазового виконання базової схеми ідентифікації. Однак нещодавно, в напрямку забезпечення безпеки забезпечили жорстке зниження рівня, що тягне за собою менший штраф за продуктивність/зберігання порівняно з безпосереднім застосуванням методу. Цей загальний фреймворк може бути застосований до схем ідентифікації, які допускають відкриті ключі з втратами. Можна довести безпеку розробленої схеми, і тому в лінійці будемо досліджувати безпеку ключів.

Представляємо аналіз продуктивності та деякі потенційні компроміси між продуктивністю та швидкістю для розробленої схеми. Потім надаємо оціночні показники та експериментальну установку, а потім детальне експериментальне порівняння розробленої схеми із сучасними схемами цифрового підпису, захищеної постквантової безпеки.

Розглянемо аналітичну ефективність розробленої схеми на основі параметрів. В обчислювальному аналізі додаткових витрат представляємо досліджуване середовище виконання в термінах загальної кількості викликів, функцій хешування і векторного додавання. Не враховуватимемо додаткові витрати на невелику постійну кількість хеш-викликів.

Додаткові витрати на обчислення та зберігання підписів розробленої схеми вимагає лише зберігання бітового випадкового початкового числа як приватного ключа, який використовується для детермінованої генерації необхідної компоненти. На вартість генерації сигнатур істотно впливає виведення і підсумовування та кількість. Для цього потрібно здійснити виклик функції, витягуючи двійкові вектори з виходів алгоритму і векторні додавання, де обчислювальні додаткові витрати незначні. Для кожного випадку бітові вхідні дані розширено до бітів. Крім того, функція обов'язково враховується. Вона породжує вектор довжини з компонентами байтової довжини. Тому вона може бути реалізована за допомогою методу, що розширює бітове введення в об'єкт і виведення бітів. У сумі вони відповідають генерації псевдовипадкових бітів через об'єкти програми. Ще однією значною вартістю генерації сигнатур є виклик функції, який використовується для обчислення образу випадковості. Виклик функції в основному складається з двох операцій: обчислення теоретико-числового перетворення і лінійної комбінації. Для того, щоб обчислити виклик функції, необхідна певна кількість викликів і одна лінійна комбінація, де обидві ці операції засновані на простих множеннях і додаваннях за модулем. Таким чином, загалом генерація сигнатури розробленої схеми вимагає зберігання певної кількості біт закритого ключа, певної кількості

викликів функції, такої ж кількості векторних доданків, одного виклику основної функції і виклик функції для обчислення сигнатури. Розмір сигнатури включає сигнатури вектора і хеш-виводу. Розглядувана вибірка задовільняє вимогам, бо складається з достатньої кількості бітів компонентів. Цей вектор можна представити за допомогою будь-якої кількості бітів. Загальний розмір сигнатури визначаємо в бітах. Додаткові витрати на обчислення та зберігання верифікатора можна визначити здійснивши перевірку сигнатури, яка вимагає лише одного виклику функції та певної кількості векторних додваань, що робить її найбільш ефективною схемою перевірки серед її поточних аналогів. З іншої сторони, розмір відкритого ключа становить все-таки певну кількість бітів, тобто певну кількість векторів сталої довжини, що відносно більше, ніж його аналоги. Покращена відмовостійкість бічних каналів розробленої схеми вимагає лише рівномірної вибірки у своєму поколінні. Оскільки він не вимагає гауссової вибірки, то він має покращену стійкість бічних каналів у порівнянні з деякими аналогами на основі решітки. Крім того, вибірка відмов ґрунтується на повторюваних випробуваннях Бернуллі, які схильні до деяких атак. Ця ефективна техніка вибірки відхилення піддавалася деяким атакам по побічних каналах. Незважаючи на те, що розроблена схема вимагає вибірки відхилень, щоб переконатися, що статистичний розподіл сигнатур не призводить до витоку інформації про компоненти приватного ключа, подібно до прототипу оскільки вибірка відхилень не вимагає жодних випробувань Бернуллі, а атака не стосується етапу вибірки відхилень.

Розроблена конструкція допускає кілька компромісів між продуктивністю та сховищем, які можуть підійти для різних сценаріїв використання. Попереднє обчислення підписів за допомогою базового ключа реалізації можна зберігати замість того, щоб детерміновано генерувати його під час генерації сигнатур. Це дозволяє підписувачу уникнути витрат на генерацію цих значень і витяг двійкових векторів під час генерації сигнатур. Оскільки підписант повинен зберігати ці вектори, то це в сумі дає приватний ключ не менше бітів, що більше,

ніж у розробленої схеми. Однак ця стратегія кешування забезпечує швидшу генерацію сигнатур, і тому їй можна віддати перевагу, коли підписувач може зберігати такі вектори. Переваги у швидкості генерації сигнатур та необхідний розмір закритого ключа додатково може бути використаний повторно. Зокрема, підписувач повинен зберігати три типи векторів розміром всього декілька біт,

Підбір параметрів лінійно впливає на розмір відкритого ключа розробленої схеми. Параметр визначає кількість викликів, двійкові вектори, які потрібно витягти, і додавання векторів у розробленій схемі підпису, а також кількість векторних доданків у розробленої схеми перевірка підпису. За зменшенням одного параметру йде вимога збільшення другого або навпаки для збереження потрібного рівня безпеки для забезпечення бітової безпеки відповідно. Однак можливі й різні параметри для одних і тих самих рівнів безпеки. Може бути, наприклад, 128-бітовий рівень безпеки і він може бути кращим для розробленої схеми Забезпечення безпеки середнього рівня забезпечило б менший відкритий ключ, де час генерації підпису було б збільшено.

Розглянемо параметри вибірки відхилення. Частота дискретизації відхилення передбачає, як і скільки разів в середньому має бути виконано генерацію сигнатури, щоб вивести прийнятну сигнатуру. Таким чином, приріст ймовірності прийняття має лінійний вплив на генерацію сигнатури. Ці два параметри можна налаштувати, щоб збільшити ймовірність прийняття з вихідних сигнатур збільшуючи і зменшуючи їх окремо та разом. Хоча налаштування цих параметрів може призвести до значного скорочення середнього часу підписання, існують компроміси, які слід враховувати. Збільшення першого параметру спричиняє збільшення розміру сигнатури. Крім того, це збільшення тягне за собою втрату безпеки, оскільки безпосередньо впливає на стійкість та вимагає відбору проб при генерації сигнатур. Кількість необхідних повторень генерації сигнатур через дискретизацію відхилення становить для середнього, рекомендованого та високого рівнів безпеки

прийнятні значення з допустимих діапазонів.

Вимога до вибірки Гаусса однакова для всіх рівнів безпеки, і тому вона представлена єдиним значенням.

Схема вимагає гауссової вибірки, яку можна вважати несприятливою через атаки на бічному каналі. Вона позначає рівень безпеки, відмінний від стандартних біт. З іншої сторони, гратчасті атаки зменшують число стандартних біт і вимагатимуть збільшення часу для компенсації втрати безпеки, що збільшує розмір відкритого ключа.

Розглянемо показники оцінки розробленої схеми для експериментів. Розроблену схему порівнюємо з її аналогами з точки зору часу генерації та перевірки підпису, приватного ключа, відкритого ключа та розмірів підпису, а також наскрізної криптографічної затримки, тобто суми часу генерації та перевірки підпису, без урахування часу передачі підпису, оскільки це залежить від мережі.

Вибір параметрів, який базується на степені двох чисел за модулем два дозволяє використовувати засоби для прискорення обчислень відповідної функції. Аналогічний підхід був зроблений в розробленій схемі. Потім, щоб завершити роботу функції, обчислили лінійну комбінацію вхідних даних з випадковою та загальнодоступною матрицею. Оскільки найвищий рівень захисту не використовували, то жодних бібліотек для цих обчислень не використовувалось. Ця операція може бути виконана дуже швидко з деякими оптимізаціями рівня збірки. Однак будемо використовувати консервативну реалізацію.

Таким чином, створено екземпляри випадкових ключів за допомогою заданої для цього функції через оптимізацію обладнання з точки зору швидкості та безпеки. Використовуємо для цього внутрішні властивості процесора для реалізації функції у режимі лічильника.

Для контрагентів використовуємо оптимізовані коди, якщо вони є, в іншому випадку довідкові коди, які подаються на підпис, запускаючи їх на

процесорі. Для цієї схеми використовуємо реалізацію з відкритим вихідним кодом.

Розглянемо аналіз та порівняння продуктивності.

Для проведення експериментальних досліджень відібрано різні схеми, які були представлені зі стандартизації постквантової криптографії крім схеми, яка була обрана, оскільки вона є однією з найшвидших сигнатур на основі ґратки. Ці схеми включають конструкції на основі ґратки, конструкцію на основі хешу, конструкцію на основі коду, конструкцію на основі криптографії симетричного ключа і багатовимірну схему. Очевидно, що розроблена схема має найнижчу наскрізну затримку, а генерація та верифікація його сигнатур є найшвидшими серед аналогів для кожного рівня безпеки. Наприклад, для розробленої схеми має найшвидшу генерацію сигнатур і найнижчу наскрізну затримку серед усіх схем з будь-яким рівнем безпеки. Крім того, розроблена схема пропонує найнижчий можливий розмір закритого ключа, що те ж саме, що і на основі симетричного ключа. Розроблена схема має сигнатуру трохи більше аналогів, що можна порівняти з аналогами на основі решітки, але більше, ніж багатоваріантні та кодові конструкції. Публічний ключ розробленої схеми значно більший, ніж більшість їхніх аналогів з високим рівнем безпеки. Беручи до уваги загальну ефективність розробленої схеми, можна вважати, що йому можна віддати перевагу, коли верифікатор може допустити таке зберігання.

Можна розглядати кешування векторів як приватний ключ замість того, щоб детерміновано виводити їх за допомогою бітового початку. Якщо врахувати цю оптимізацію, то вона забезпечує генерацію сигнатур, яка є значно швидшою, ніж у розробленої схеми. Оскільки перевірка залишається незмінною, то цей варіант може ще більше покращити наскрізну затримку, яка наразі є найшвидшою. З іншої сторони, коли ці вектори кешуються, то розмір закритого ключа значно збільшується, що лише менше, ніж основна частина ключа, для певних рівнів безпеки. Це може призвести до кешування недоцільного для деяких застосувань, де підписувач обмежений у пам'яті. У цих випадках

розробленої схеми слід віддавати перевагу будь-якому кешуванню.

Розглянемо вартість розробленої схеми для майбутніх оптимізацій з точки зору витрат. Обчислення функції відповідає частині від загальної вартості генерації сигнатур розробленої схеми, що трохи знижується на вищих рівнях безпеки. Найвищі витрати визначаються як виклики фугкції і вилучення двійкових векторів з цього виходу функції зробленого для детермінованого генерування векторів збільшує додаткові витрати. Це може бути додатково підтверджено покращеннями, що спостерігаються за допомогою кешування векторів, де ця вартість усувається та замінюється лише додаванням векторів. За перевірку підпису понад загальної вартості припадає на функцію.

Обчислення функції можуть бути додатково прискорені за допомогою інструкцій по збірці функції. Подані результати з еталонною реалізацією без будь-яких інструкцій на рівні збірки. Тому для розробленої схеми все ще є значний простір для підвищення продуктивності, особливо в алгоритмі перевірки, де домінуючою вартістю є функція. З іншої сторони, оскільки реалізувано функції для розробленої схеми за допомогою внутрішніх функцій процесора, то розроблена схема може зіткнутися з додатковими витратами за продуктивність на інших платформах. Тому, для реалізації викликів в розробленій схемі на інших платформах слід віддавати перевагу легким симетричним шифрам або хеш-функціям.

Таким чином, запропоновано нову схему цифрового підпису з постквантовим безпекою, яку називаємо розроблена схема. Її алгоритмічна будова використовує відому структуру та адитивно гомоморфні функції для розширення одноразових сигнатур до поліноміально обмежених багаточасових сигнатур. Розроблена схема пропонує кілька властивостей. Вона дає змогу досягти найнижчої наскрізної затримки з найшвидшою генерацією та перевіркою сигнатур серед своїх аналогів на кожному рівні безпеки. Розроблена схема має найменший розмір закритого ключа, тобто декілька біт серед своїх аналогів.

Розроблена схема має параметри, що легко налаштовуються, які пропонують різні компроміси між швидкістю та зберіганням. Розроблена схеми не вимагає будь-якої гаусової вибірки, і тому вона несприйнятлива до атак зі сторони каналу, спрямованих на цю функцію. Всі ці властивості мають більший відкритий ключ, ніж більшість її аналогів.

3.3 Висновки до третього розділу

В результаті запропоновано нову схему цифрового підпису з постквантовим безпекою, яку називаємо розроблена схема. Вона дає змогу досягти найнижчої наскрізної затримки з найшвидшою генерацією та перевіркою сигнатур серед своїх аналогів на кожному рівні безпеки. Розроблена схема має найменший розмір закритого ключа, тобто декілька біт серед своїх аналогів. Розроблена схема має параметри, що легко налаштовуються, які пропонують різні компроміси між швидкістю та зберіганням. Розроблена схеми не вимагає будь-якої гаусової вибірки, і тому вона несприйнятлива до атак зі сторони каналу, спрямованих на цю функцію. Результатом є подання підписів та компактних ключів в системах з IoT.

4 СХЕМА СЕРТИФІКАТІВ НА ОСНОВІ РЕШІТКИ ДЛЯ ПОСТКВАНТОВИХ БЛОКЧЕЙНІВ

4.1 Проєктування розподіленого реєстру для послідовного запису транзакцій

Механізми консенсусу лежать в основі децентралізованої природи блокчейнів. Поширені криптовалюти, такі як Bitcoin, використовують блокчейн як розподілений реєстр для послідовного запису транзакцій. Цей розподілений реєстр підтримується одноранговою мережею майнерів, які зацікавлені в пошуку рішення криптографічної головоломки під назвою Proof of Work (PoW). Майнер, який першим знайде рішення, може додати блок транзакцій до блокчейну. Чим більше обчислювальної потужності вкладає майнер, тим вищі його шанси спочатку вирішити головоломку.

У відкритих системах, таких як Bitcoin, будь-якому користувачеві, який готовий виділити певну кількість обчислювальних ресурсів, дозволяється приєднатися до мережі та зробити свій внесок у підтримку блокчейну. Ця відкритість, поряд зі стратегією стимулювання, привернула велику кількість обчислювальних ресурсів у вигляді окремих майнерів і майнінгових пулів. В даний час існує невелика кількість майнінгових пулів, які додають більшість блоків транзакцій в мережі Bitcoin.

Було проведено великий масив робіт, присвячених безпеці протоколу консенсусу Bitcoin. Деякі недавні роботи доводять, що якщо більшість обчислювальних ресурсів контролюється чесними майнерами, то ці протоколи досягають ряду корисних властивостей безпеки. З іншої сторони, ці роботи показують, що якщо зловмисники контролюють більшість обчислювальних ресурсів у мережі, то ці властивості безпеки більше не гарантуються. З недавніх пір він було показано, що цей сценарій, коли майнінг-пул перевищує 50% обчислювальних ресурсів у зловмисників, то виникає проблема захисту. Тому, з'явилася однорангова мережа Bitcoin. Наприклад, у 2014 році майнінг-пул

GHash.io володів більшістю обчислювальних ресурсів мережі Bitcoin.

PoW є найбільш поширеними алгоритмами консенсусу і були прийняті в більше, ніж 90% блокчейнів включаючи Bitcoin. У цих блокчейнах майнери повинні довести, що вони виконали певну обчислювальну роботу, в основному у формі оцінки криптографічних хеш-функцій. Наприклад, кожен майнер шукає такий набір, де хеш попереднього блоку і складність задані мережею. Хеш-функція багаторазово викликається на різних етапах, щоб знайти ту, яка задовольняє вищевказаній умові. Майнер, який задовольняє цій умові, потім транслює блок включаючи блок попереднього етапу, а інші вузли в одноранговій мережі перевіряють, чи дійсно цей блок задовольняє умові, і якщо так, то додають блок до своїх блокчейнів. Таким чином, забезпечується консенсус щодо розподіленого реєстру та децентралізованої довіри за рахунок витрат енергії.

Протоколи PoW в більшості блокчейн-застосунків, наприклад Bitcoin, покладаються на криптографічні хеш-функції. Хеш-функції, що використовуються в таких системах, досягають бажаних властивостей захисту від квантових супротивників при моделюванні у вигляді випадкового ключа. Незважаючи на це, пошуковий алгоритм дає асимптотичну квадратичну перевагу квантовим комп'ютерам при вирішенні PoW на основі хешування. З огляду на цю квадратичну перевагу, дебют квантових комп'ютерів збільшить ризик атаки на PoW на основі хешування. Тому, хоча деякі переваги перед класичними комп'ютерами можуть узгоджуватися з природою протоколів PoW, бо дорожчі або потужніші машини повинні працювати краще, щоб зменшити цю перевагу, наприклад, тому, що квантові комп'ютери можуть існувати протягом деякого часу, перш ніж стати доступними для більшості.

Розглянемо процес стандартизації, який спрямований на забезпечення плавного переходу до постквантових безпечних асиметричних криптосистем і застосуємо ідеї кандидатів на основі решітки до блокчейнів на основі PoW.

Основна мета полягає в тому, щоб усунути прогалину в дослідженнях у сучасному світі шляхом створення нового протоколу консенсусу, зокрема,

алгоритму PoW, який зменшує перевагу квантових комп'ютерів над класичними, має швидку перевірку та регульовану складність. Для досягнення цієї мети пропонуємо новий протокол PoW під назвою TPoW. Новий протокол PoW заснований на проблемі. З огляду на сучасне розуміння задач такого типу, TPoW задовольняє базовим основним властивостям та дає незначну квантову перевагу. Асимптотична квантова перевага менша, ніж квадратична швидкість алгоритму. TPoW важко вирішити, але легко перевірити. Розв'язок еквівалентний розв'язанню задач з малим коефіцієнтом наближення. Перевірка еквівалентна обчисленню норми, n-го кореня і деяких множень.

Параметри TPoW легко точно налаштувати, щоб відрегулювати його складність. Зокрема, збільшення розмірності ґратки має добре вивчений вплив на необхідні обчислювальні ресурси для розв'язання проблеми PoW. Другорядною метою цього процесу є створення протоколу PoW, який заохочує подальші експерименти та розуміння практичних алгоритмічних удосконалень для вирішення проблем типу майнінгу.

Тому, пропонується використовувати як енергію, витрачену на хеш-головоломки, так і попит на майнінг криптовалют, щоб покращити сучасний рівень дискретного криптоаналізу журналів. Відповідно враховуючи, що складність майнінгу є фундаментальною для безпеки подання на основі решітки до процесу постквантової стандартизації, PoW на основі розробленої схеми може аналогічно використовувати цю енергію та попит для допомоги в криптоаналізі проблеми довіри до вузла.

Якщо припустити, що дана хеш-функція виконує випадковий підпис, то алгоритм дає оптимальне прискорення проти PoW на основі цієї хеш-функції і не може бути розпаралелений інакше, як тривіальним способом. Фактично це означає, що параметри PoW, наприклад, кількість початкових нулів, необхідних у хеш-виході, повинні будуть збільшуватися лише для того, щоб врахувати підвищену обчислювальну потужність, а не принципово нові алгоритмічні методи. Це не обов'язково стосується конкретної проблеми решітки, яку

розглядаємо. Відсутні жодні докази оптимальності для алгоритмів, які зараз використовуються для її розв'язання. По суті, це означає, що параметри PoW, тобто ранг решітки, можливо, доведеться збільшити, щоб врахувати алгоритмічні покращення, а також для збільшення обчислювальної потужності.

Найвідомішою часовою складністю для вирішення головоломок цієї задачі, які ми розглядаємо, є для ґраток певного рангу, і що будь-яка зміна хоча б трохи субекспоненціальної функції буде являти собою розвиток теорії ґраток. Тому, не очікуємо, що доведеться занадто сильно підвищувати ранг, навіть для того, щоб врахувати будь-які алгоритмічні покращення.

Запропонований протокол TPoW для виконання робіт в блокчейні дає можливість верифікатору довести, що він виконав певний обсяг роботи. Перед тим, як представити протокол PoW, представимо формальне визначення цих протоколів наступним чином. Визначення таких протоколів, яке складається з алгоритмів, які генерують цю проблему, вирішують таку задачу, тим самим виробляючи доведення розв'язку, і, нарешті, перевіряють правильність цього доведення. Ця трійка алгоритмів повинна задовольняти наступним вимогам. Ефективність гарантує, що верифікація виконується в близькому лінійному часі. Ефективність і повнота разом гарантують, що виконавець, який виконує приблизно певну невелику кількість операцій, може довести верифікатору, що він це зробив. Стійкість вимагає, щоб верифікатор мав, наприклад, незначний шанс для деякої незначної функції переконати адміністратора, не виконуючи додатково операцій. Це залишається вірним, навіть якщо дослідник може обчислювати задачі разом.

Перед тим, як запропонуємо новий протокол PoW, розглянемо про те, як вирішуються випадки проблем. Розв'язати їх можна за допомогою різних сімейств алгоритмів. Сімейство, яке розглядаємо, - це евристичні решітчасті алгоритми, які мають найвідомішу класичну та квантову часову складність.

Однак для розв'язання задач такого типу не обов'язково викликати ґратчасті сімейства алгоритмів в повній розмірності ґратки. Так, просіювання у

розмірності є достатнім при певних евристичних припущеннях.

Існує також багато інших евристичних методів, які забезпечують значне практичне прискорення. Нарешті, структура, яка зіставляє, розширює та реалізує ці методи, є найвищим виміром розв'язаної проблеми. Розглянуті методи нетривіально залежать від якості ґратчастої основи, що використовується неформально. Наскільки короткими і близькими до ортогоналів є його базисні вектори, то решітка використовується в алгоритмах редукції, які самі вимагають ключів для проектованих підґраток нижчої розмірності. Константа буде залежати від методів, що використовуються для поліпшення якості базису.

Високорівнева архітектура PoW відповідає визначенню. Встановлюємо n ній як розмірність решітки так і параметри. Нехай TPoW визначається наступним чином. Використовуємо розширювану вихідну функцію, щоб витягти достатню випадковість з попереднього блоку для вибірки необхідних величин. Далі для неї невідомо, як згенерувати певну кількість бітових простих чисел, ймовірно або доказово. Дійсно, теорема про прості числа говорить, що певна кількість біт непарних чисел є простим числом з ймовірністю приблизно, і жоден відомий тест простоти не виконується. Тоді, використовуючи тест з випадковими базисами на однорідних непарних бітових цілих числах, можемо згенерувати ймовірне бітове просте число за очікуваний час. Оскільки перевірка вимагає множення матриці та вектора, то вона витрачає час. Нехай ця витрата є незначною функцією, тоді, згідно з сучасними методами розв'язування існує PoW проти класичних комп'ютерів і проти квантових комп'ютерів. Можемо згенерувати ймовірне просте число з певною кількістю бітів за очікуваний час вибірки, а отже, результат досяжний.

Найефективніші з відомих алгоритмів розв'язують на вході задачу з викликом хоча б одного, а максимум і більше ключів у розмірності. Тому в класичному випадку результат відмінний від випадку в квантовому випадку, використовуючи найбільш ефективні відомі класичні та квантові підходи. Для будь-якої константи алгоритм з розробленої схеми повинен бути викликаний

у розмірності. Термін будь-який означатиме алгоритм субекспоненціального часу для цієї задачі.

Розв'язки для задачі при великих числах отримуються, і тому PoW є повним, крім незначної ймовірності. Щоб зробити його абсолютно повним, замість нього можна взяти і встановити число варіантів більшого розміру, якщо це доречно, щоб підтримувати бажану вартість для розв'язання.

Невідомо, як використовувати інформацію з незалежних випадкових ґраток в інших випадкових ґратках. Якщо задано певну кількість ґраток, породжених алгоритмом, то ймовірність того, що будь-яка з них має достатньо коротку сигнатуру та знаходиться у векторі є високою. Не знаючи, як інакше використовувати інформацію з інших ґраток, обчислюємо значення, яке, як очікуємо, дуже приблизно відповідає поточній вартості майнінгу біткойна.

Якщо припустити, що алгоритм на вхідних байтах займає приблизно невелику кількість циклів, це дає приблизно таку ж кількість циклів. Кілька верхніх точок даних, в яких використовуються однаково згенеровані випадкові ґратки, мають розміри і приблизну кількість циклів відповідно. Тому пропонуємо подвоїти їх кількість принаймні з огляду на сучасні методи. Для опрацювання може бути використано графічний процесор з потрібною або адлишковою кількістю ядер до тих же завдань. Тоді він дає інший набір експериментальних значень, за допомогою яких можна параметризувати необхідну складність.

Евристичні методи розв'язання СВП, наприклад, величина досяжних вільних розмірностей, залежать від якості основи ґратки. При цьому прихована константа важлива. Також, при цьому вплинути на ці методи економії розмірів можливо. Недоліком просіювання є експоненціальна вартість пам'яті, що може призвести до затримок доступу до пам'яті, які стають вузьким місцем. Було висловлено припущення, що це може бути частково пом'якшено апаратними реалізаціями сит. З огляду на великі ресурси, вкладені в розробку для PoW на основі хешування, можна очікувати, що аналогічні досягнення будуть здійсненні

у випадку TPoW, а також просунутися за межі паралелізму, запропонованого як альтернативу. Зокрема, можна сподіватися на прогрес у порівнянні з попередньою роботою з розподіленого просіювання до більших або більш загальних контекстів.

При розгляді конкретних квантових схем і застосуванню корекції помилок, оцінюються прискорення, досяжні на практиці від квантового пошуку при використанні в контексті хеш-функцій і решітчастих сит. Згідно з сьогоднішнім розумінням квантових комп'ютерів, використання квантового комп'ютера при вирішенні PoW сьогодні практично не буде давати жодної переваги. Тому розглядаємо випадок, коли, наприклад, удосконалення класичної обчислювальної потужності забезпечує необхідну стійкість PoW до діапазонів, де квантовий комп'ютер забезпечив би значну перевагу, або там, де доступна більш ефективна корекція помилок квантових схем. У гіршому випадку вказано новий PoW на основі добре вивчених складних задач. Ця робота в кінцевому підсумку випливає про створення PoW, який у майбутньому захистить блокчейни від надання великої переваги квантовим комп'ютерам.

Технологія блокчейн досягається за рахунок використання набору симетричних і асиметричних криптографічних примітивів, які є життєво важливими для забезпечення розподіленої довіри, аутентифікації транзакцій, конфіденційності тощо. Хеш-функції, зокрема, необхідні для встановлення безперервності між блоками в блокчейні. Однак всім цим примітивам, в тій чи іншій мірі, загрожує можлива поява квантових комп'ютерів.

Було зроблено багато спроб розробити та стандартизувати постквантові безпечні криптографічні примітиви. Наприклад, очікується, що випуститься перший проект постквантового стандарту. Так само деякі дослідження були зосереджені на постквантових блокчейн-системах. Bitcoin Post-Quantum був запропонований як експериментальна гілка Bitcoin. Bitcoin Post-Quantum використовує підписи для заміни сигнатур, які в даний час розгорнуті в блокчейні Bitcoin. Ця схема підпису на основі хешування, яка, хоча й забезпечує

надійну постквантову обіцяну безпеку страждає від великих параметрів. Тому є використання більш ефективних схем постквантового підпису, таких як схеми на основі решітки, щоб замінити традиційні схеми підпису, які зараз використовуються в блокчейнах. Ethereum має плани на майбутнє щодо розгортання постквантових захищених протоколів, які користуються постквантовою безпекою.

Існують також деякі протоколи PoW, які прагнуть досягти кращої постквантової безпеки в порівнянні зі звичайними протоколами PoW. Ці підходи в основному спрямовані на вирішення проблем, що вимагають інтенсивної пам'яті. Перший екземпляр цих протоколів називається Proof-of-Space, в якому програматор генерує жорстку функцію пам'яті, а верифікатор запитує підмножину ділянок пам'яті, щоб перевірити, чи заповнені вони належною функцією. У той час як протокол користується ефективною верифікацією, жорстке ядро схеми, засноване на суперконцентраторах, працює досить повільно. По суті завданням виступає вимага від організатора знайти цикл певної довжини в орієнтованому дводольному графі, що складається з вершин і ребер. Початкова схема була зламана шляхом зменшення потреби в пам'яті при збільшенні обчислювальної вартості. Інша схема, шукає колізії на виходах хеш-функції з входом, хоча детального компромісу між часом і простором не передбачено.

Мінімізація потреби в пам'яті в коефіцієнті тягне за собою лише збільшення додаткового часу роботи через коефіцієнт. Нарешті, є реалізація, яка базується на узагальненій проблемі дня народження. Щоб зробити алгоритм стійким до амортизації, пропонується метод, який називають зв'язуванням алгоритму, використовуючи властивості алгоритму.

Таким чином, TPoW є першим обчислювальним протоколом PoW, який прагне мінімізувати розрив між класичним і квантовим майнером.

4.2 Шифрування з можливістю пошуку за відкритим ключем на основі решітки

Хмарні обчислення суттєво вплинули на обчислювальну інфраструктуру та уможливили створення великої множини застосунків. Наприклад, аутсорсинг даних дозволяє малому/середньому бізнесу підвищити доступність даних за рахунок мінімізації витрат на управління та обслуговування. Аутсорсинг даних, незважаючи на свої переваги, викликає у клієнтів значні занепокоєння щодо конфіденційності даних. Традиційні методи шифрування можуть бути використані для подолання таких проблем конфіденційності. Однак стандартне шифрування не дозволяє здійснювати пошук зашифрованих даних. Тому значна кількість досліджень зосереджена на технологіях пошукового шифрування, які можуть бути використані для ефективного вирішення цієї проблеми. Існує дві основні гілки, кожна з яких адаптована для окремого набору застосунків.

Динамічне симетричне шифрування з можливістю пошуку забезпечує пошук зашифрованих даних для застосунків аутсорсингу приватних даних, наприклад, зберігання даних у хмарі, в яких клієнт використовує свій власний приватний ключ для шифрування, а потім пошуку власних даних у хмарі. Серед інших методів, заснованих на симетричних ключах, для приховування шаблонів доступу користувача використовується альтернативна схема. Схеми шифрування за відкритим ключем з пошуком за ключовими словами дозволяють будь-якому клієнту шифрувати дані за допомогою заданих ключових слів під відкритим ключем призначеного одержувача. Потім призначена одержувачка чи одержувач можуть використовувати свій приватний ключ, щоб генерувати та надсилати пастки для потрібних ключових слів, а також дозволити серверу шукати зашифровані дані, щоб отримати файли, пов'язані з ключовим словом. Цей метод добре підходить для розподілених застосунків. Наприклад, електронна пошта, журнали аудиту для Інтернету речей тощо, де велика кількість користувачів/сутностей генерують зашифровані дані, які отримує

одержувач. Основна увага приділена схемам. Для початкової пропозиції схем вона має кілька пристроїв. Наприклад, мобільний телефон, комп'ютер тощо. Вона хоче, щоб її електронні листи спрямовувалися на її пристрої на основі ключових слів, пов'язаних із ними. Наприклад, коли відправник, надсилає їй електронного листа з ключовим словом, то терміново лист має бути спрямований на її мобільний телефон. Для досягнення цієї мети, після шифрування вмісту електронної пошти звичайним шифруванням з відкритим ключем, відправник використовує схему для шифрування ключового слова терміново і відправляє його разом із зашифрованим електронним листом на поштовий сервер. Потім отримувач може використати свій приватний ключ, щоб згенерувати пастку, що відповідає ключовому слову терміново і попросити сервер отримати всі електронні листи, пов'язані з цим ключовим параметром. Іншим важливим застосуванням схем є зберігання та пошук у приватних файлах журналів. Схеми можуть дозволити гетерогенному набору пристроїв надсилати зашифровані файли журналів, об'єднані з шифротекстом із можливістю пошуку з різними ключовими словами, на ненадійний сервер зберігання. Для аналізу файлів журналу аудитор може використовувати свій приватний ключ для створення пасток і дозволити серверу шукати та повертати файли, пов'язані з цільовим ключовим словом.

З моменту їх введення було запропоновано кілька схем з різноманітними особливостями. Однак широкому впровадженню схем на практиці перешкоджає ряд перешкод.

Висока наскрізна затримка є найбільш витратною з обчислювальної точки зору частиною схеми. Як правило, є фаза пошуку, яка вимагає виконання тесту алгоритму для кожної пари з ключовим слово-файлпм у базі даних. Існуючі схеми запровадили значну наскрізну затримку обчислень через принаймні одну операцію сполучення, яка потрібна в тесті алгоритму, який слід назвати лінійним до загальної кількості пар ключ-файл у базі даних для кожного пошукового запиту. Таким чином, забезпечення обчислювальної ефективності тесту

алгоритму є критично важливою вимогою для мінімізації наскрізної затримки.

Відсутність довгострокової безпеки є дуже бажаною властивістю для застосунків зберігання даних, щоб запропонувати довгострокові заходи безпеки даних. Однак досягнення високого рівня безпеки протягом тривалого періоду часу вимагає безперервного збільшення розмірів ключів, що призводить до значного збільшення додаткових витрат на обчислення для звичайних криптографічних примітивів. Крім того, поява квантових комп'ютерів зробить більшість звичайних примітивів асиметричної криптографії небезпечними, і тому є велика заслуга в розробці схем, які можуть забезпечити постквантові належні рівні безпеки.

Незважаючи на те, що ряд схем були повністю реалізовані на реальних даних і є загальнодоступними до теперішнього часу у відкритому доступі немає повноцінної реалізації з реальним набором даних. Звідси виникає потреба в забезпеченні повноцінної реалізації схем та порівняльному аналізі їх розгортання на реальних хмарних платформах для вимірювання важливих факторів продуктивності, наприклад, затримки зв'язку, часу доступу до диску, які не можуть бути точно зафіксовані за допомогою простих «оцінок вартості».

Тому, розроблено дві схеми на основі решітки з забезпеченням постквантової безпеки та реалізацію розробленої схеми на основі решітки та її аналога на основі сполучення.

Перші схеми на основі решітки у початковій пропозиції показали, як вивести схему з шифрування на основі ідентифікації. Розглядувані для експериментів дві схеми засновані на інструментах на основі решіток. Перша схема відповідає всім вимогам, передбаченим для забезпечення доказової безпеки в моделі випадкового ключа. Друга схема використовує конструкції, щоб запропонувати перший доказовий безпечний підпис на основі ґратки в стандартній моделі. Розглянемо розміри параметрів, щоб уникнути потенційних помилок узгодженості з великою ймовірністю.

Висока обчислювальна ефективність в розробленій схемі пропонує значні

переваги обчислювальної ефективності в порівнянні з існуючими схемами. Це досягається за рахунок використання останніх зусиль по підвищенню ефективності схем на основі ґратки, кільцевих і швидких арифметичних операцій над поліноміальними кільцями. Ця схема має значно більш ефективні алгоритми, які в даний час розглядаються як найбільш ефективні альтернативи. Ефективність алгоритму має життєво важливе значення, оскільки він виконується сервером один раз на кожну пару ключове слово-файл у базі даних, що призводить до додаткових витрат на обчислення. Ефективність алгоритму полегшує реалізацію схем на обмежених батареях пристроїв. Завдяки обчислювальній ефективності, незважаючи на наявність більших параметрів, показано, що розгортання схеми на реальній хмарі забезпечує кращий наскрізний час відгуку в порівнянні з аналогами.

Результати експерименту з отримання ключів подано в табл. 4.1.

Таблиця 4.1 - Результати експерименту для засобів IoT

№ засобу	Ключ
5	hjfklsnf bch56kmdjjfnwenf!nnw%nlkn;rkbvbvjbjvbljbljl;knk;bnbjlnhv
11	besebnbknknk;n;kgmn;gm;n;nvk;snb;kd’mlgnl’gjbk;nbmlmbgl’nlg’nlg
34	vjbvln;knb;kfnb;kfnb;fmb;mlmnldmb;db;dnb;dml;mnl;mtcjzlnklnbknk
51	vjdlsb.vljbjlbvljnv/lrnvbnirbnkz/snvk;nfbkninv;bvkhbvjbjvbjlsbvlsbvls
78	bjbaljvba/lvbljw/ablrnbls/lrnigbnkfnbkfnbznadgrrhvjlnfkb;nf;;;nbkfndb
98	bjblavbbrlebvjlfdnjbnjlninbknb;knnkfnbkdlbnknbkdnvksrijribnkfdnbkd
103	vnknenbinbineibieaaaanknnb4840gnrni9bknbkdnpjse;bn;kdnbibn;kdbb

Отримані ключі, які подано в табл. 4.1 є такими, що надійно забезпечують подання вузла в засобах комунікації інтернету речей.

Таким чином, проведені експериментальні дослідження підтверджують ефективність розробленої схеми. Отримані ключі не потребують сертифікатів та

ідентифікації. Так розроблена схема може бути використана в засобах комунікації інтернету речей, зокрема в різних системах блокчейну та автоматизованих системах з дронами, для яких було проведено дослідження щодо її використання.

4.3 Висновки до четвертого розділу

Розроблений метод криптографічного захисту було застосовано до створення протоколу TPoW, який є обчислювальним протоколом стандартного PoW. Його завданням є мінімізація розрив між класичним і квантовим майнером.

З розробленими системами, в яких використано метод криптографічного захисту проведені експериментальні дослідження, які підтверджують ефективність розробленої схеми. Отримані ключі не потребують сертифікатів та ідентифікації. Розроблена схема може бути використана в засобах комунікації інтернету речей, зокрема в різних системах блокчейну та автоматизованих системах з дронами, для яких було проведено дослідження щодо її використання.

ВИСНОВКИ

У роботі за результатами виконаних теоретичних та практичних досліджень розроблено новий метод криптографічного захисту протоколів в засобах комунікації інтернету речей та отримано такі результати:

1. Здійснено аналіз відомих методів криптографічного захисту протоколів в засобах комунікації інтернету речей.

2. Розроблено метод криптографічного захисту протоколів в засобах комунікації інтернету речей. Розроблено схему підпису, яка відповідає вимогам щодо мінімальної затримки деяких систем IoT у реальному часі. Це досягається за рахунок використання гомоморфної властивості односторонньої функції, що лежить в основі, і методу попередніх обчислень. Запропонована схема безпечна в моделі випадкового списку при жорсткості вимог до неї.

3. Реалізовано розроблений метод криптографічного захисту протоколів в блокчейн та автоматизованій системі з дронами. Розроблений метод криптографічного захисту було застосовано до створення протоколу TPoW, який є обчислювальним протоколом стандартного PoW. Його завданням є мінімізація розрив між класичним і квантовим майнером.

4. Здійснено есперементальні дослідження згідно розроблених рішень. З розробленими системами, в яких використано метод криптографічного захисту проведені експериментальні дослідження, які підтверджують ефективність розробленої схеми. Отримані ключі не потребують сертифікатів та ідентифікації. Розроблена схема може бути використана в засобах комунікації інтернету речей, зокрема в різних системах блокчейну та автоматизованих системах з дронами, для яких було проведено дослідження щодо її використання.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Alwen J., Peikert C. Generating shorter bases for hard random lattices. *Theory of Computing Systems*, 2011, 48(3), Pp. 535–553.

2. American Bankers Association. *ANSI X9.6P-1998: Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)*, 1999.

3. Attila A. Yavuz and Jorge Guajardo. Dynamic searchable symmetric encryption with minimal leakage and efficient updates on commodity hardware. In Orr Dunkelman and Liam Keliher, editors, *Selected Areas in Cryptography – SAC P015*, pages 241–259. Springer Berlin Heidelberg, 2016.

4. Zhang R., Imai H. Generic combination of public key encryption with keyword search and public key encryption. In Feng Bao, San Ling, Tatsuaki Okamoto, Huaxiong Wang, and Chaoping Xing, editors, *Cryptology and Network Security Proceedings*, Springer Berlin Heidelberg. 2007. P. 159–174.

5. Amy M., Matteo O., Gheorghiu V., Mosca M., Parent A., Schanck J. Estimating the cost of generic quantum pre-image attacks on sha-2 and sha-3. In Roberto Avanzi and Howard Heys, editors, *Selected Areas in Cryptography – SAC P016*, Springer International Publishing Cham. 2017. P. 317–337.

6. Andersen D. Exploiting time-memory tradeoffs in cuckoo cycle. https://arstechnica.com/information-technology/2014/06/ bitcoin-security-guarantee-shattered-by-anonymous-miner-with-51-network-power/, 2014.

7. Armbrust M., Fox A., Griffith R., Joseph A., Katz R., Konwinski A., Lee G., . Patterson D., Rabkin A., Stoica I., et al. Above the clouds: A berkeley view of cloud computing. 2009.

8. Ateniese G., Bianchi G., Capossele A., Petrioli C. Low-cost Standard Signatures in Wireless Sensor Networks: A Case for Reviving Pre-computation Techniques? In *Proceedings of the P0th Annual Network & Distributed System Security Symposium, NDSS P013*, NDSS2013, San Diego, CA, February 24-27 2013.

9. Ho Au M., Mu Y., Chen J., Wong D., K. Liu J., Yang G. Malicious kgc attacks in certificateless cryptography. In *Pnd ACM Symposium on Information, Computer and Communications Security*, ASIACCS, pages 302–311, 2007.

10. Aumasson J., Henzen L., Meier W., Phan R. Sha-3 proposal blake. *Submission to NIST (Round 3)*, 2010.

11. Baek J., R., Susilo W. Certificateless public key encryption without pairing. In Jianying Zhou, Javier Lopez, Robert H. Deng, and Feng Bao, editors, *Information Security*, Springer Berlin Heidelberg, 2005. P. 134–148.

12. Baek J., Safavi-Naini R., Susilo W. Public key encryption with keyword search revisited. In Osvaldo Gervasi, Beniamino Murgante, Antonio Laganà, David Taniar, Youngsong Mun, and Marina L. Gavrilova, editors, *Computational Science and Its Applications*, Springer Berlin Heidelberg, 2008. P. 1249–1259.

13. IEEE standard for wireless access in vehicular environments security services for applications and management messages. *IEEE Std 1609.P-P013 (Revision of IEEE Std 1609.P-P006)*, pages 1–289, April 2013.

14. Abdalla M., Bellare M., Catalano D., Kiltz E., Kohno T., Lange T., Malone-Lee J., Neven G., Paillier P., Shi H. Searchable encryption revisited: Consistency properties, relation to anonymous ibe, and extensions. In Victor Shoup, editor, *Advances in Cryptology – CRYPTO P005: P5th Annual International Cryptology Conference*, Springer Berlin Heidelberg, 2005. P. 205–222.

15. Aggarwal D., Brennen G., Lee T., Santha M., and Tomamichel M. Quantum attacks on bitcoin, and how to protect against them. *arXiv preprint arXiv:1710.10377*, 2017.

16. Agrawal S., Boneh D., Boyen X. Efficient lattice (h)ibe in the standard model. In Henri Gilbert, editor, *Advances in Cryptology – EUROCRYPT P010: P9th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Springer Berlin Heidelberg, 2010. P. 553–572.

17. Ajtai M. Generating hard instances of lattice problems. In *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, ACM, 1996. P. 99–

108.

18. Akleylek S., Bindel N., Buchmann J., Krämer J., Marson G. An efficient lattice-based signature scheme with provably secure instantiation. In David Pointcheval, Abderrahmane Nitaj, and Tajjeeddine Rachidi, editors, *Progress in Cryptology – AFRICACRYPT P016*, Springer International Publishing, 2016. P. 44–60.

19. Al-Riyami S., Paterson K. Certificateless public key cryptography. In Chi-Sung Laih, editor, *Advances in Cryptology - ASIACRYPT P003*, Springer Berlin Heidelberg, 2003. P. 452–473.

20. Albrecht M., Bai S., Ducas L. A subfield lattice attack on overstretched NTRU assumptions. In Matthew Robshaw and Jonathan Katz, editors, *Advances in Cryptology – CRYPTO P016*, pages 153–178. Springer Berlin Heidelberg, 2016.

21. Albrecht M., Ducas L., Herold G., Kirshanova E., Postlethwaite E., Stevens M. The general sieve kernel and new records in lattice reduction. In Yuval Ishai and Vincent Rijmen, editors, *Advances in Cryptology – EUROCRYPT P019*, Springer International Publishing. Cham, 2019. P. 717–746.

22. Albrecht M., Gheorghiu V., Postlethwaite E., Schanck J. Estimating quantum speedups for lattice sieves. In Shiho Moriai and Huaxiong Wang, ed- itors, *Advances in Cryptology – ASIACRYPT P0P0*, Springer International Publishing. Cham, 2020. P. 583–613.

23. Alkadri N., Buchmann J., Bansarkhani R., Krämer J. A framework to select parameters for lattice-based cryptography. Cryptology ePrint Archive, Report 2017/615, 2017. https://eprint.iacr.org/2017/615.

24. Alkim E., Ducas L., Pöppelmann T., Schwabe P. Post-quantum key exchange-a new hope. In *USENIX Security Symposium*, 2016. P. 327–343.

25. Ball M., Rosen A., Sabin M., Vasudevan P. Proofs of work from worst-case assumptions. In *Advances in Cryptology - CRYPTO P018 - 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, P018, Proceedings, Part I*, pages 789–819, 2018.

26. Laarhoven T. Sieving for shortest vectors in lattices using angular locality-

sensitive hashing. In CRYPTO, 2015. P. 3–22.

27. Becker A., Ducas L., Gama N., Laarhoven T. New directions in nearest neighbor searching with applications to lattice sieving. In *Proceedings of the Twenty-seventh Annual ACM-SIAM Symposium on Discrete Algorithms*, SODA ’16, Society for Industrial and Applied Mathematics. Philadelphia, PA, USA, 2016. P. 10–24.

28. Behnia R., Ozmen M., Yavuz A. Authentication for real-time iot systems. In *ICC P019 - P019 IEEE International Conference on Communications (ICC)*, pages 1–6, 2019.

29. Behnia R., Ozmen M., Yavuz A. Lattice-based public key searchable encryption from experimental perspectives. *IEEE Transactions on Dependable and Secure Computing*, 17(6):1269–1282, 2020.

30. Behnia R. NTRUPEKS. https://github.com/Rbehnia/NTRUPEKS, 2016.

31. Behnia R., Ozmen M., Yavuz A. Authentication for real-time IoT systems. In *IEEE International Conference on Communications (ICC)*, ICC, pages 1855–1867, New York, NY, USA, 2019. ACM.

32. Behnia R., Ozmen M., Yavuz A., Rosulek M. Tachyon: Fast signatures from compact knapsack. In *Proceedings of the P018 ACM SIGSAC Conference on Computer and Communications Security*, CCS ’18, pages 1855–1867, New York, NY, USA, 2018. ACM.

33. Rouzbeh Behnia, Attila Altay Yavuz, and Muslum Ozgur Ozmen. High-speed high-security public key encryption with keyword search. In Giovanni Livraga and Sencun Zhu, editors, *Data and Applications Security and Privacy XXXI: 31st Annual IFIP WG 11.3 Conference*, Cham, Springer International Publishing. 2017. P. 365–385,

34. Behnia R., Yavuz A., Ozmen M., Yuen T. Compatible certificateless and identity-based cryptosystems for heterogeneous iot. In Willy Susilo, Robert H. Deng, Fuchun Guo, Yannan Li, and Rolly Intan, editors, *Information Security*, Springer International Publishing. Cham, 2020. P. 39–58.

35. Bellare M., Rogaway P. Random oracles are practical: A paradigm for

designing efficient protocols. In *Proceedings of the 1st ACM conference on Computer and Communications Security (CCS '93)*, pages 62–73, NY, USA, 1993. ACM.

36. Bellare M., Boldyreva A., Desai A., Pointcheval D. Key-privacy in public-key encryption. In Colin Boyd, editor, *Advances in Cryptology — ASIACRYPT P001 Proceedings*, Springer Berlin Heidelberg, 2001. P. 566–582.

37. Bellare M., Boldyreva A., O'Neill A. Deterministic and efficiently searchable encryption. In Alfred Menezes, editor, *Advances in Cryptology - CRYPTO P007: P7th Annual International Cryptology Conference*, pages 535–552. Springer Berlin Heidelberg, 2007.

38. Bellare M., Namprempre C., Neven G. Security proofs for identity-based identification andăsignature schemes. *Journal of Cryptology*, 22(1):1–61, Jan 2009.

39. Bellare M., Neven G. Multi-signatures in the plain public-key model and a general forking lemma. In *Proceedings of the 13th ACM Conference on Computer and Communications Security*, CCS '06, pages 390–399, New York, NY, USA, 2006. ACM.

40. Bellare M., Rogaway P. Random oracles are practical: A paradigm for designing efficient protocols. In *Proceedings of the 1st ACM Conference on Computer and Communications Security*, CCS '93, pages 62–73, New York, NY, USA, 1993. ACM.

41. Bellare M., Rogaway P. The security of triple encryption and a framework for code- based game-playing proofs. In Serge Vaudenay, editor, *Advances in Cryptology - EUROCRYPT P006*, pages 409–426. Springer Berlin Heidelberg, 2006.

42. Bendlin R., Krehbiel S., Peikert C. How to share a lattice trapdoor: Threshold protocols for signatures and (h)ibe. In Michael Jacobson, Michael Locasto, Payman Mohassel, and Reihaneh Safavi-Naini, editors, *Applied Cryptography and Network Security*, Springer Berlin Heidelberg. Berlin, Heidelberg, 2013. P. 218–236.

43. Bernstein D. A subfield-logarithm attack against ideal lattices. http://blog.cr.yp.to/20140213-ideal.html, 2014.

44. Bernstein D., Chuengsatiansup C, Lange T., Schwabe P. Kummer strikes back: New dh speed records. In Palash Sarkar and Tetsu Iwata, editors, *Advances in*

Cryptology – ASIACRYPT P014, pages 317–337. Springer Berlin Heidelberg, 2014.

45. Bernstein D., Duif N., Lange T., Schwabe P., Yang B. High-speed high-security signatures. *Journal of Cryptographic Engineering*, 2(2):77–89, Sep 2012.

46. Bernstein D., Hopwood D., Hülsing A., Lange T., Niederhagen R., Papachristodoulou L., Schneider M., Schwabe P., Wilcox-O'Hearn Z. Sphincs: Practical stateless hash-based signatures. In Elisabeth Oswald and Marc Fischlin, edi- tors, *Advances in Cryptology – EUROCRYPT P015*, pages 368–397. Springer Berlin Heidelberg, 2015.

47. Aumasson, J.-P., Neves, S., Wilcox-O'Hearn, Z., Winnerlein, C.: BLAKE2: Simpler, Smaller, Fast as MD5. In: Jacobson, M., Locasto, M., Mohassel, P., Safavi-Naini, R. (eds.) ACNS 2013. LNCS, Springer, Heidelberg 2013. Vol. 7954. P. 119–135.

48. Bindel N., Akeylek S., Alkim E., Barreto P., Buchmann J., Eaton E., Gutoski G., Kramer J., Longa P., Polat H., Ricardini J., Zanon G. Submission to the NIST's post-quantum cryptography standardiza- tion process, 2018. https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/round-1/submissions/qTESLA.zip.

49. Biryukov A., Khovratovich D. Equihash: Asymmetric proof-of-work based on the generalized birthday problem. *Ledger*, 2:1–30, Apr. 2017.

50. Blichfeldt H. A new principle in the geometry of numbers, with some applications. *Transactions of the American Mathematical Society*, 15(3):227–235, 1914.

51. Boneh D., Boyen X. Efficient Selective-ID secure identity-based encryption without random oracles. In *Proc. of the P3th International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT '04)*, 2004. P. 223–238.

52. Boneh D., Crescenzo G., Ostrovsky R., Persiano G. Public Key Encryption with Keyword Search. In Christian Cachin and Jan L. Camenisch, editors, *Advances in Cryptology - EUROCRYPT P004: International Conference on the Theory and Applications of Cryptographic Techniques*, Springer Berlin Heidelberg, 2004. P. 506–522.

53. Boneh D., Franklin M. Identity-based encryption from the weil pairing. In *Advances in Cryptology - CRYPTO P001*, 2001. P. 213–229.

54. Boneh D., Waters B. Conjunctive, subset, and range queries on encrypted data. In Salil P. Vadhan, editor, *Theory of Cryptography Proceedings*, pages 535–554. Springer Berlin Heidelberg, 2007.

55. Bos J., Costello C., Naehrig M., Stebila D. Post-quantum key exchange for the tls protocol from the ring learning with errors problem. In *P015 IEEE Symposium on Security and Privacy*, pages 553–570, 2015.

56. Bos J., Naehrig M., Pol J. Sieving for shortest vectors in ideal lattices: a practical perspective. Cryptology ePrint Archive, Report 2014/880, 2014.

57. Bösch C., Hartel P., Jonker W., Peter A. A survey of provably secure searchable encryption. *ACM Comput. Surv.*, 47(2):18:1–18:51, 2014.

58. Bost R. Sophos - forward secure searchable encryption. Cryptology ePrint Archive, Report 2016/728, 2016. https://eprint.iacr.org/2016/728.

59. Bost R., Minaud B., Ohrimenko O. Forward and backward private searchable encryption from constrained cryptographic primitives. Cryptology ePrint Archive, Report 2017/805, 2017. https://eprint.iacr.org/2017/805.

60. Boyen X. A tapestry of identity-based encryption: practical frameworks compared. *IJACT*, 1(1):3–21, 2008.

61. Boyen X. Lattice mixing and vanishing trapdoors: A framework for fully secure short signatures and more. In Phong Q. Nguyen and David Pointcheval, editors, *Public Key Cryptography – PKC P010: 13th International Conference on Practice and Theory in Public Key Cryptography*, Springer Berlin Heidelberg, 2010. P. 499–517.

62. Braithwaite M. Experimenting with post-quantum cryptography, 2016.

63. Bringer J., Chabanne H., Kindarji B.. Error-tolerant searchable encryption. In *IEEE International Conference on Communications*. 2009.P. 1–6.

64. Buchmann J., Dahmen E., Hülsing A. Xmss - a practical forward secure signature scheme based on minimal security assumptions. In *Proceedings of the 4th International Conference on Post-Quantum Cryptography*, PQCrypto’11, Berlin,

Heidelberg, Springer-Verlag. 2011. P. 117–129.

65. Byun J., Rhee H., Park H., Lee D. Off-line keyword guessing attacks on recent keyword search schemes over encrypted data. In Willem Jonker and Milan Petković, editors, *Secure Data Management: Third VLDB Workshop Proceedings*, pages 75–83. Springer Berlin Heidelberg, 2006.

66. Camara C., Peris-Lopez P., Tapiador J. Security and privacy issues in implantable medical devices: A comprehensive survey. *Journal of Biomedical Informatics*, 55. 2015. P. 272 – 289.

67. Casanova A., Faugere J.-C., Macario-Rat G., Patarin J., Perret L., Ryckeghem J. Submission to the NIST's post-quantum cryptography standardization process, 2018. https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/ round-1/submissions/GeMSS.zip.

68. Cash D., Hofheinz D., Kiltz E. How to delegate a lattice basis. Cryptology ePrint Archive, Report 2009/351, 2009. http://eprint.iacr.org/2009/351.

69. Chase M., Derler D., Goldfeder S., Orlandi C., Ramacher S., Rechberger C., Slamanig D., Zaverucha G. Post-quantum zero-knowledge and signatures from symmetric-key primitives. In *Proceedings of the P017 ACM SIGSAC Conference on Computer and Communications Security*, CCS '17, pages 1825–1842, New York, NY, USA, 2017. ACM.

70. Chen Y. *Reduction de reseau et securite concrete du chiffrement completement homo- morphe*. PhD thesis, Université Paлгоритм Diderot, 2013.

71. Genise N., Micciancio D. Faster gaussian sampling for trapdoor lattices with arbitrary modulus. Cryptology ePrint Archive, Report 2017/308, 2017. https://eprint.iacr. org/2017/308.

72. Gervais A., Karame G., Wüst K., Glykantzis V., Ritzdorf H., Capkun S. On the security and performance of proof of work blockchains. In *Proceedings of the P016 ACM SIGSAC Conference on Computer and Communications Security*, CCS '16, pages 3–16, New York, NY, USA, 2016. Association for Computing Machinery.

73. Göpfert F., Vredendaal C., Wunderer T. A hybrid lattice basis reduction and

quantum search attack on lwe. In Tanja Lange and Tsuyoshi Takagi, editors, *Post-Quantum Cryptography*, pages 184–202, Cham, 2017. Springer International Publishing.

74. Bruinderink L., Hülsing A., Lange T., Yarom Y. Flush, gauss, and reload – a cache attack on the bliss lattice-based signature scheme. In Benedikt Gierlichs and Axel Y. Poschmann, editors, *Cryptographic Hardware and Embedded Systems – CHES P016: 18th International Conference, Santa Barbara, CA, USA, August 17-19, P016, Proceedings*, Springer Berlin Heidelberg. Berlin, Heidelberg, 2016. P. 323–345.

75. Hastings M., Heninger N., Wustrow E. Short paper: The proof is in the pudding. In Ian Goldberg and Tyler Moore, editors, *Financial Cryptography and Data Security*, Springer International Publishing, 2019. P. 396–404.

76. Hoang T., Behnia R., Jang Y., Yavuz A. Mose: Practical multi- user oblivious storage via secure enclaves. In *Proceedings of the Tenth ACM Conference on Data and Application Security and Privacy*, CODASPY '20, page 17âĂŞ28, New York, NY, USA, 2020. Association for Computing Machinery.

77. Hoffstein J., Pipher J., Whyte W., Zhang Z. A signature scheme from learning with truncation. Cryptology ePrint Archive, Report 2017/995, 2017. https://eprint.iacr.org/2017/995.

78. Hulsing A., Bernstein D., Dobraunig C., Eichlseder M., Fluhrer S., Gazdag S., Kampanakis P., Kolbl S., Lange T., Lauridsen M., Mendel F., Niederhagen R., Rechberger C., Rijneveld J., Schwabe P. Sphincs+. Submission to the NIST's post-quantum cryptography standardization process, 2018. https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/round-1/submissions/SPHINCS_Plus.zip.

79. Hülsing A., Rijneveld J., Schwabe P. Armed SPHINCS - computing a 41 KB signature in 16 KB of RAM. In *Public-Key Cryptography - PKC P016 - 19th IACR International Conference on Practice and Theory in Public-Key Cryptography*, pages 446–470, March 2016.

80. Costello C., Longa P. Schnorrq: Schnorr signatures on fourq. Technical report, MSR Tech Report, 2016. Available at: https://www. microsoft. com/en-

us/research/wp- content/uploads/2016/07/SchnorrQ. pdf.

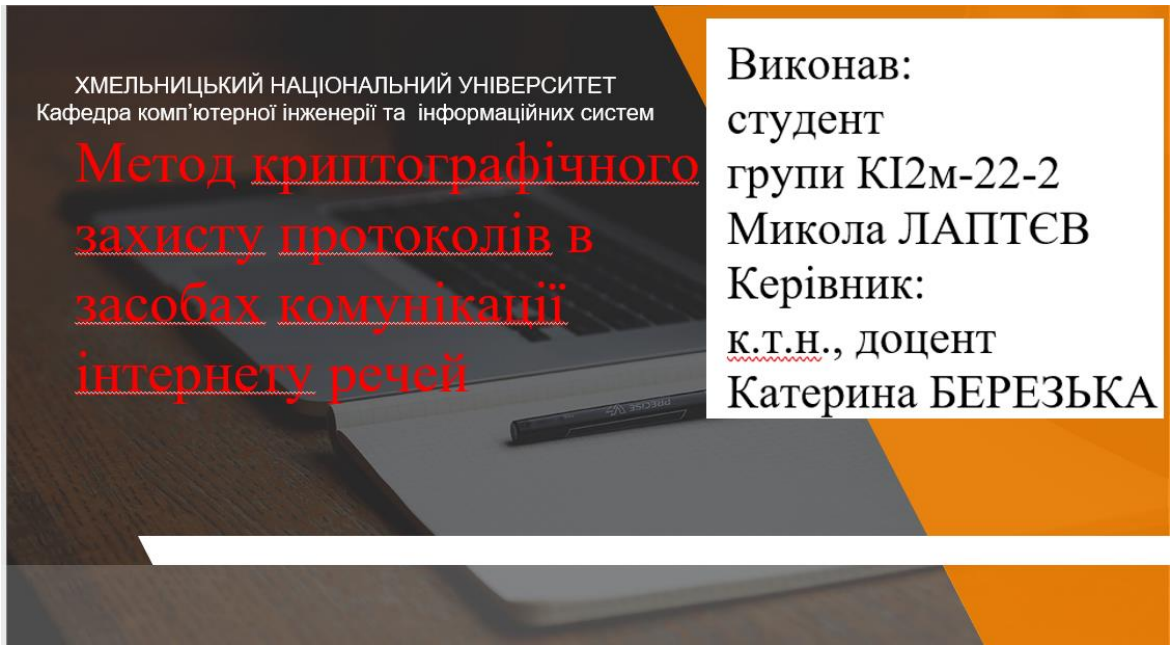
81. Ducas L. Shortest vector from lattice sieving: A few dimensions for free. In Jesper Buus Nielsen and Vincent Rijmen, editors, *Advances in Cryptology – EUROCRYPT P018*, Springer International Publishing, Cham. 2018.P. 125–145.

82. Pass R., Seeman L., Shelat A.. Analysis of the blockchain protocol in asynchronous networks. In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *Advances in Cryptology – EUROCRYPT P017*, pages 643–673, Cham, 2017. Springer International Publishing.

83. Melnychenko O, Scislo L, Savenko O, Sachenko A, Radiuk P. Intelligent Integrated System for Fruit Detection Using Multi-UAV Imaging and Deep Learning. *Sensors*. 2024; 24(6):1913. https://doi.org/10.3390/s24061913

84. Лаптєв М.П., Лисий А.М., Сєргєєв Є.В., Віжевський П.В. Метод криптографічного захисту протоколів в засобах комунікації інтернету речей / Збірник наукових праць за матеріалами XV Всеукраїнської науково-практичної конференції «Актуальні проблеми комп'ютерних наук АПКН-2023». Хмельницький, 2023, С.161-162.
https://kn.khmnu.edu.ua/wp-content/uploads/sites/18/apkn2023_corpuspaper.pdf

ДОДАТОК А Презентація роботи



2

Зв'язок роботи з науковими програмами, планами, темами.

Актуальність роботи полягає в необхідності розробити метод криптографічного захисту протоколів в засобах комунікації інтернету речей, які б не використовували сертифікатів та ідентифікації для пришвидшення обміну інформацією.

Дослідження, представлені у кваліфікаційній роботі, проводились в рамках студентської наукової роботи кафедри комп'ютерної інженерії та інформаційних систем Хмельницького національного університету.

3

Перелік публікацій

За темою кваліфікаційної роботи опубліковано одну публікацію у Збірнику наукових праць за матеріалами XV Всеукраїнської науково-практичної конференції «Актуальні проблеми комп'ютерних наук АПКН-2023». (Хмельницький – 2023. – С.139-141).) [84].

Метою кваліфікаційої роботи є розробка методу криптографічного захисту протоколів в засобах комунікації інтернету речей.

Поставлена мета досягається розв'язанням таких основних завдань:
- проаналізувати відомі методи криптографічного захисту протоколів в засобах комунікації інтернету речей;
- розробити метод криптографічного захисту протоколів в засобах комунікації інтернету речей;
- реалізувати розроблений метод криптографічного захисту протоколів в блокчейн;
- здійснити есперементальні дослідження згідно розроблених рішень.

- *Об'єктом дослідження є процес криптографічного захисту протоколів в засобах комунікації інтернету речей.*
- *Предметом дослідження є методи криптографічного захисту протоколів в засобах комунікації інтернету речей.*

Наукова новизна отриманих результатів:
розроблено новий метод криптографічного захисту протоколів в засобах комунікації інтернету речей.

На основі проведених досліджень розроблена система для забезпечення криптографічного захисту протоколів в засобах комунікації інтернету речей.
Практична значимість *отриманих результатів полягає у розробленій крипографічній системі для забезпечення захисту протоколів в засобах комунікації інтернету речей. Вона надає можливість для формування надійних з'днань між засобами інтеренту речей, щоб передавати повідомлення, без ідентифікації та без сертифікації.*

Інтернет речей (IoT) – це гетерогенна система, що складається з великої кількості взаємопов'язаних датчиків, розумних пристроїв, приймачів-передавачів, мікрокомп'ютерів тощо. Такі системи часто покладаються на зв'язок у реальному часі для забезпечення передбачуваної функціональності та можуть бути об'єктом зловмисних атак для аутентифікації, цілісності та/або конфіденційності даних, що передаються/зберігаються. Але, існує широкий спектр криптографічних схем, призначених для ефективного пом'якшення/запобігання цим атакам.

Ці криптографічні схеми в основному можна розділити на системи на основі симетричного ключа або системи на основі відкритого ключа. Схеми на основі симетричних ключів пропонують високоефективні та безпечні рішення, однак вони можуть бути не ідеальними для впровадження в деяких умовах IoT через наступне:
1) обчислення та розподіл спільного ключа;
2) зберігання спільних ключів;
3) недостатня публічна можливість перевірки та невідмова у схемах аутентифікації.

Схеми на основі симетричних ключів вимагають протоколу узгодження ключів для обчислення спільного секретного ключа перед ініціюванням безпечного зв'язку. Хоча в деяких програмах може бути можливим попереднє завантаження цих спільних ключів на всі пристрої, це буде досить складно для систем, де рухомі датчики/пристрої повинні зв'язуватися з безліччю нових пристроїв у режимі реального часу (наприклад, мережі повітряних дронів, автомобільна мережа тощо).

Для подання методу криптографічного захисту протоколів в засобах комунікації інтернету речей спочатку формалізуємо предметне поле дослідження.

Введемо для засобів IoT множину та відобразимо засоби елементами цієї множини так:

$$M = \{m_1, m_2, \dots, m_{n_M}\}, \tag{2.1}$$

де n_M- кількість засобів IoT.

Задамо абстрактну модель системи з IoT так:

$$M_{IoT} = \langle M, G \rangle, \tag{2.2}$$

де G- граф, в якому вершинами є елементи множини M.

Формула (2.2) описує зв'язки, а оскільки IoT – це концепція зв'язку, то таке задання є коректним.

- *Основні кроки методу криптографічного захисту протоколів в засобах комунікації інтернету речей:*

1) здійснимо асиметричне шифрування для приватного обміну секретним ключем симетричного шифрування;

2) використаємо симетричний ключ шифрування для шифрування обміну.

- *Кроки генерації ключа.*

1. Надсилати послідовність біт з вузла m_i.
2. Для кожного отриманого повідомлення випадковим чином обирати будь-яку одну основу з двох основ системи числення.
3. Зберігати використані бази та отримані результати.
4. Публічно повідомляти про отримання повідомлень всім вузлам з множини M.
5. Зберігати лише ті події, для яких використовувалися однакові бази.
6. Обчислити частоту помилок для тестових подій, і якщо вона вища за деяке попередньо визначене порогове значення, вони переривають процедуру. Інакше вони переходять до наступного кроку
7. Перетворити дані в класичні біти 0 і 1, відомі як необроблений ключ. Після цього застосовувати класичні процеси для виправлення помилок і посилення конфіденційності для отримання остаточного ключа.

Результати експерименту для засобів IoT

№ засобу	Ключ
5	hjfklsnf bch56kmdjjfnwenf!nnw%nlkn;rkbvbvjbjvbljbljl;knk;bnbjlnhv
11	besebnbknknk;n;kgmn;gm;n;nvk;snb;kd'mlgnl'gjbk;nbmlmbgl'nlg'nlg
34	vjbvln;knb;kfnb;kfnb;fmb;mlmnldmb;db;dnb;dml;mnl;mtcjzlnklnbknk
51	vjdlsb.vljbjlbvljnv/lrnvbnirbnkz/snvk;nfbkninv;bvkhbvjbjvbjlsbvlsbvls
78	bjbaljvba/lvbljw/ablrnbls/lrnigbnkfnbkfnbznadgrrhvjlnfkb;nf;;;nbkfndb
98	bjblavbbrlebvjlfdnjbnjlninbknb;knnkfnbkdlbnknbkdnvksrijribnkfdnbkd
103	vnknenbinbineibieaaaanknnb4840gnrni9bknbkdnpjse;bn;kdnbibn;kdbb

ВИСНОВКИ

У роботі за результатами виконаних теоретичних та практичних досліджень розроблено новий метод криптографічного захисту протоколів в засобах комунікації інтернету речей та отримано такі результати:

1. Здійснено аналіз відомих методів криптографічного захисту протоколів в засобах комунікації інтернету речей.

2. Розроблено метод криптографічного захисту протоколів в засобах комунікації інтернету речей. Розроблено схему підпису, яка відповідає вимогам щодо мінімальної затримки деяких систем IoT у реальному часі. Це досягається за рахунок використання гомоморфної властивості односторонньої функції, що лежить в основі, і методу попередніх обчислень. Запропонована схема безпечна в моделі випадкового списку при жорсткості вимог до неї.

3. Реалізовано розроблений метод криптографічного захисту протоколів в блокчейн та автоматизованій системі з дронами. Розроблений метод криптографічного захисту було застосовано до створення протоколу TPoW, який є обчислювальним протоколом стандартного PoW. Його завданням є мінімізація розрив між класичним і квантовим майнером.

11

*4. Здійснено есперименталь*ні *дослідження згідно розроблених рішень. З розробленими системами, в яких використано метод криптографічного захисту проведені експериментальні дослідження, які підтверджують ефективність розробленої схеми. Отримані ключі не потребують сертифікатів та ідентифікації. Розроблена схема може бути використана в засобах комунікації інтернету речей, зокрема в різних системах блокчейну та автоматизованих системах з дронами, для яких було проведено дослідження щодо її використання.*

ДОДАТОК Б Наукова праця здобувача

Міністерство освіти і науки України
Хмельницький національний університет

ЗБІРНИК НАУКОВИХ ПРАЦЬ
за матеріалами XV Всеукраїнської науково-практичної конференції
«Актуальні проблеми комп'ютерних наук АПКН-2023»

17-18 листопада 2023

Хмельницький 2023

УДК 004.5

Лаптєв М.П., Лисий А.М., Сєргєєв Є.В., Віжевський П.В.

Хмельницький національний університет

МЕТОД КРИПТОГРАФІЧНОГО ЗАХИСТУ ПРОТОКОЛІВ В ЗАСОБАХ КОМУНІКАЦІЇ ІНТЕРНЕТУ РЕЧЕЙ

Розроблено метод, що здійснює криптографічний захист і досягає найнижчої наскрізної затримки серед аналогів. Це робить його придатним для пристроїв нижчого класу. Як крок до повністю постквантового блокчейну пропонується протокол Proof of Work (PoW), який мінімізує переваги квантового майнера. Новий протокол базується на проблемі найкоротшого вектора у евклідовій нормі та забезпечує швидкий алгоритм перевірки. Щоб зменшити перешкоду передачі сертифікатів і перевірки для низького рівня пристроїв, представлено криптосистеми на основі ідентифікації та без сертифікатів, створені за допомогою спеціальних алгоритмів генерації ключів.

A method has been developed that provides cryptographic protection and achieves the lowest end-to-end latency among peers. This makes it suitable for lower end devices. As a step towards a full post-quantum blockchain, a Proof of Work (PoW) protocol is proposed, which minimizes the benefits of a quantum miner. The new protocol is based on the shortest vector problem in the Euclidean norm and provides a fast verification algorithm. To reduce the barrier of certificate transmission and verification for lower-level devices, identity-based and certificate-less cryptosystems created using special key generation algorithms are introduced.

Інтернет речей (IoT) – це гетерогенна система, що складається з великої кількості підключених датчиків, розумних пристроїв, трансиверів, мікрокомп'ютерів тощо. Такі системи часто спираються на спілкування в режимі реального часу, щоб забезпечити заплановану функціональність. Вони можуть бути піддані спрямованій з боку зловмисника атаці, яка може бути направлена на автентифікацію, цілісність та/або конфіденційність даних, що передаються/зберігаються. Наявний широкий спектр криптографічних схем, призначених для ефективного пом'якшення/попередження на такі напади.

Ці криптографічні схеми можна в основному розділити на системи з симетричними або відкритими ключами. Проте схеми на основі симетричних ключів пропонують [1, 2] високоефективні та безпечні рішення, але вони можуть бути не ідеальними для впровадження в деяких налаштуваннях IoT через спільний ключ обчислення та розповсюдження. Для схем на основі симетричних ключів потрібен протокол узгодження ключів. Потрібно обчислити спільний секретний ключ перед ініціюванням безпечного зв'язку. Хоча це може бути здійсненним попередньо завантаживши ці спільні ключі на всі пристрої в деяких програмах, але це може бути досить складно для систем, у яких рухомі датчики/пристрої потребують зв'язку з безліччю нових пристроїв у режимі реального часу Зберігання спільного доступу до ключів для великих мереж IoT з тисячами або навіть мільйонами пристроїв створює теж проблеми. Зберігання попередньо обчислених

спільних ключів може бути неможливими на пристроях нижчого класу через їх обмежене сховище. Відсутність публічної перевірки та неспростовності в схемах автентифікації. Хоча існує багато понять на основі симетричних ключів для забезпечення автентифікації, вони не можуть забезпечити неспростування.

Системи IoT часто покладаються на пристрої низького рівня для надсилання вимірювань іншим сторонам, і залежно від налаштувань несанкціонована зміна та/або порушення конфіденційності цих заходів може мати катастрофічні наслідки. Тому, забезпечення ефективної автентифікації, цілісності та конфіденційності в цих параметрах є життєво важливим. Хоча звичайні криптографічні засоби можуть бути використані для задоволення цих вимог безпеки, незважаючи на їх дизайн, вони часто занадто дорогі з обчислювальної точки зору для пристроїв низького класу. Ситуація ще більше посилюється, коли береться до уваги захист від квантових комп'ютерів.

Розроблено серію нових ефективних звичайних і постквантових криптографічні схеми, щоб відповідати суворим вимогам таких систем IoT. У рядку пропозицій ефективних схем автентифікації пропонується дві схеми підпису. Перша схема підпису заснована на звичайних криптографічних проблемах і використовує кодування повідомлень із сімействами без покриття та особливі властивості функцій для досягнення значного приросту продуктивності порівняно з аналогами. Друга схема заснована на постквантових примітивах і досягається шляхом розширення одноразових підписів до (поліноміально обмежених) багаторазових підписів, використовуючи адитивні гомоморфні властивості узагальнених компактних функцій.

Схема досягає найнижчої наскрізної затримки серед аналогів, що робить її придатною для пристроїв нижчого класу. Як крок до повністю постквантового блокчейну пропонується протокол Proof of Work (PoW), який мінімізує переваги квантового майнера. Новий протокол базується на проблемі найкоротшого вектора Ерміта (Hermite-SVP) у евклідовій нормі та забезпечує швидкий алгоритм перевірки. Щоб зменшити перешкоду передачі сертифікатів і перевірки для низького рівня пристроїв, представляємо криптосистеми на основі ідентифікації та без сертифікатів, створені за допомогою спеціальних алгоритмів генерації ключів, які використовують властивість адитивної гомоморфності експонент, щоб дозволити користувачам включати свої приватні ключі в ключ, наданий довіреною третьою стороною, не підробляючи його. Нові схеми досягають кращої ефективності обчислень і порівнянної ефективності зв'язку порівняно з аналогами на основі ідентифікації та без сертифікатів.

Перелік посилань

1. Melissa Chase, David Derler, Steven Goldfeder, Claudio Orlandi, Sebastian Ramacher, Chris1tian Rechberger, Daniel Slamanig, and Greg Zaverucha. Post-quantum zero-knowledge and signatures from symmetric-key primitives. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS '17, pages 1825–1842, New York, NY, USA, 2017. ACM.

2. Léo Ducas. Shortest Vector from Lattice Sieving: a Few Dimensions for Free (talk). https: //eurocrypt.iacr.org/2018/Slides/Monday/TrackB/01-01.pdf, April 2018.

ДОДАТОК В Результати перевірки на антиплагіат

UNICHECK
by Turnitin

Ім'я користувача:
Кафедра КІ

ID перевірки:
1016200930

Дата перевірки:
19.04.2024 21:06:33 EEST

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
19.04.2024 21:07:13 EEST

ID користувача:
100005591

Назва документа: **Лаптєв_Метод криптографічного захисту протоколів в засобах комунікації інтернету речей**

Кількість сторінок: **84** Кількість слів: **20544** Кількість символів: **158669** Розмір файлу: **248.37 KB** ID файлу: **1015968366**

2.34%
Схожість

Найбільша схожість: **1.23%** з Інтернет-джерелом (https://kn.khmnu.edu.ua/wp-content/uploads/sites/18/apkn-2023-cor...

2.07% Джерела з Інтернету	39	Сторінка 86
1.09% Джерела з Бібліотеки	83	Сторінка 86

0% Цитат

Цитати	1	Сторінка 87
Посилання	1	Сторінка 87

0%
Вилучень

Немає вилучених джерел

Модифікації

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

Замінені символи	7

Anti-Plagiarism v-15.257

Максимальне співпадіння з одним документом 0.0%

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 12%**

ID: 125393 Назва: МКР Метод криптографічного захисту протоколів в засобах комунікації інтернету речей Додано в БД: 2024-04-19 Автора: Лаптєв М. Керівники: Березька К. Консультанти: Опоненти:	Документ		Сумарний збіг по Базі Даних	
	Символи	Лексеми	Символи	Лексеми
	147644	937	1250 (1%)	7 (1%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми

ДОДАТОК Г Заява та висновок про аналіз результатів на антиплагіат

Завідувачу кафедри КІІС
д-р.техн.наук, проф. Тетяні ГОВОРУЩЕНКО

Миколи ЛАПТЄВА
ПІБ здобувача вищої освіти

ФІТ, 2 курсу, групи КІ2м-22-2

ЗАЯВА

З правилами чинного Положення «Про систему забезпечення академічної доброчесності у Хмельницькому національному університеті» від 01.07.2022, згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений (а). Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщений(а) та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Unicheck та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

31 березня 2024 року

РІШЕННЯ ЕКСПЕРТНОЇ КОМІСІЇ

КАФЕДРИ КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОРМАЦІЙНИХ СИСТЕМ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Метод криптографічного захисту протоколів в засобах комунікації інтернету речей

Автор: Лаптєв Микола

Спеціальність: 123 – Компютерна інженерія

Освітня програма: освітньо-наукова

Науковий керівник: Березька Катерина Миколаївна, к.т.н, доцент

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом. Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	

Підтвердження:

Запозичення, виявлені в роботі, є законними і не є плагіатом, оскільки:

1) окремі виявлені збіги є загальновживаними фразами або виразами, про що свідчить посилання системи на збіг з 10-30 джерелами на один фрагмент речення;
2) всі зафіксовані системою ознаки модифікації тексту відносяться до комбінування латинських символів зі україномовними скороченнями індексів в формулах, що не є модифікацією тексту.

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості, складає 1% і адресується до двох основних першоджерел (по 2% і 1%), що, з урахуванням наведених обґрунтувань, відповідає характеру завдання і свідчить на користь кваліфікаційної роботи.

Керівник роботи _____ Катерина БЕРЕЗЬКА

Гарант ОП _____ Олег САВЕНКО

Завідувач кафедри КІІС _____ Тетяна ГОВОРУЩЕНКО

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА ДИПЛОМНУ РОБОТУ

Дипломник: Микола ЛАПТЄВ

Тема: Метод криптографічного захисту протоколів в засобах комунікації інтернету речей

Спеціальність: 123 «Комп'ютерна інженерія»

Обсяг кваліфікаційної роботи:

Кількість листів креслень - ; кількість сторінок записки 99

1. Короткий зміст роботи та прийнятих рішень У роботі розроблено метод криптографічного захисту протоколів в засобах комунікації інтернету речей

2. Висновок про відповідність роботи дипломному завданню Кваліфікаційна робота відповідає виданому завданню

3. Характеристика виконання кожного розділу, ступінь використання останніх досягнень науки і техніки і передових методів роботи: у вступі подано об'єкт та предмет дослідження, мету, наукову новизну та практичну цінність роботи, а також характеристику структури роботи. У першому розділі проведено аналіз відомих рішень щодо криптографічного захисту протоколів в засобах комунікації IoT. У другому розділі подано розроблений метод криптографічного захисту протоколів в засобах комунікації інтернету речей. У третьому розділі розроблено подання підписів та компактних ключів в системах з IoT. У четвертому розділі здійснено проєктування розподіленого реєстру для послідовного запису транзакцій та шифрування. У висновках підведено підсумки досягнення результатів з розв'язання завдань дослідження.

4. Позитивні сторони роботи: ___

5. Негативні сторони роботи: немає.

6. Оцінка графічного оформлення та пояснювальної записки роботи: __=____

7. Відгук про роботу в цілому: __Робота виконана на належному рівні.

8. Інші зауваження: ___=

9. Оцінка дипломної роботи:

Розглянувши позитивні та негативні сторони представленої кваліфікаційної роботи вважаю, що робота заслуговує оцінки «добре» 4,00 (С)

Рецензент (прізвище, ім'я, по батькові, посада, місце роботи) __Мартинюк Валерій Володимирович, д.т.н., професор, завідувач кафедри АКІТР ХНУ

"_2_" __травня__2024р.