Харківський національний університет радіоелектроніки

Факультет Комп'ютерних наук

Кафедра Програмної інженерії

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

другий (магістерський)
(рівень вищої освіти)

Дослідження алгоритмів цифрового підпису для пост квантового періоду. Falcon 2.

Виконав:
студент 2 курсу групи ІПЗм-21-4

Коняєв Д. К.
(прізвище, ініціали)

Спеціальність	121 – Інженерія програмного забезпечення
Тип програми	Освітньо-наукова
Керівник	проф. Качко О. Г. (посада, прізвище, ініціали)

Допускається до захисту
Зав. Кафедри З.В. Дудар

2023 р.

Харківський національний університет радіоелектроніки

Факультет Комп'ютерних наук

Кафедра Програмної інженерії

Рівень вищої освіти другий (магістерський)

Спеціальність 121 – Інженерія програмного забезпечення
(код і повна назва)

Тип програми освітньо-наукова програма

Освітня програма Інженерія програмного забезпечення

ЗАТВЕРДЖУЮ:

Зав.кафедри _____
(підпис)
«__»_____2023 р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

студента Коняєва Дмитра Костянтиновича
(прізвище, ім'я, по батькові)

1. Тема роботи «Дослідження алгоритмів цифрового підпису для постквантового періоду. Falcon 2» затверджена наказом університету від «_29_» _березня_ 2023 р. № _ 302Ст__
2. Термін подання студентом роботи до екзаменаційної комісії «_18_» __травня_ 2023__ р.
3. Вихідні дані до роботи *Технічне завдання, календарний план, методичні вказівки, алгоритми цифрового підпису.*
4. Перелік питань, що потрібно опрацювати в роботі *Аналіз предметної галузі і постановка задачі, дослідження та реалізація алгоритму цифрового підпису для постквантового періоду Falcon*

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	Аналіз предметної галузі	25.01.2023	Виконано
2	Дослідження предметної області	25.01.2023	Виконано
3	Аналітичній огляд	25.01.2023	Виконано
4	Аналіз існуючих методів або алгоритмів	01.02.2023	Виконано
5	Постановка задачі	08.02.2023	Виконано
6	Планування експериментальної частини дослідження	15.02.2023	Виконано
7	Підготовка пояснювальної записки	05.04.2023	Виконано
8	Нормконтроль, рецензування	09.05.2023	Виконано
9	Захист	18.05.2023	Виконано

Дата видачі завдання 01 лютого 2023 р.

Студент

(підпис)

Керівник роботи проф. Качко О.Г.

(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ / ABSTRACT

Пояснювальна записка магістерської атестаційної роботи: 76 с., 4 рис., 10 джерел. КРИПТОАНАЛІЗ, ПОСТКВАНТОВА КРИПТОГРАФІЯ, ЦИФРОВИЙ ПІДПИС, FALCON, АНАЛІЗ .

Об’єктом дослідження є алгоритми цифрового підпису. Метою роботи є дослідження сучасних алгоритмів цифрового підпису, та їх особливостей для пост квантового періоду.

Детальне дослідження алгоритму Falcon, криптостійкість якого базується на NTRU грат. У роботі розглянуто сучасні алгоритми ЕЦП, Falcon як алгоритм пост квантового періоду, програмна реалізація алгоритму генерації ключів для Falcon, математичні методи рішення NTRU рівняння, та їх порівняння.

Explanatory note of the master's attestation work: pp., Fig., Sources.

CRYPTOANALYSIS, POSTQUANTUM CRYPTOGRAPHY, DIGITAL SIGNATURE, FALCON, ANALYSIS.

The object of research is digital signature algorithms. The aim of the work is to study digital signature algorithms for the post-quantum period and the Falcon algorithm, to study modern electronic signature algorithms.

The paper considers modern EDS algorithms, Falcon as a post-quantum period algorithm, software implementation of key generation algorithms for Falcon, a study of existing digital signature algorithms, and analysis of the industry in general.

Умови публікації пояснювальної записки

Я,

Коняєв Дмтро Костянтинович

(прізвище, ім’я, по батькові)

студент(ка) групи ІПЗМ-21-4 здобувач вищої освіти на другому (магістерському)

рівні кафедра_____програмної інженерії_____,

(повна назва кафедри)

заявляю: моя кваліфікаційна робота на тему

Дослідження алгоритмів цифрового підпису для пост квантового періоду. Falcon 2,

(назва роботи)

що буде представлена до ЕК для публічного захисту, виконана самостійно, в ній не містяться елементи плагіату і вона може бути опублікована в електронному архіві відкритого доступу ElArKhNURE. Всі запозичення з друкованих та електронних джерел мають відповідні посилання. Я ознайомлений (а) з діючим положенням «Про протидію академічному плагіату в ХНУРЕ», згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування дисциплінарних заходів.

ПЕРЕЛІК СКОРОЧЕНЬ

NTRU – Кільце усіченого полінома N-го ступеня.

RSA – Абревіатура від призвіщ Rivest–Shamir–Adleman криптографічний алгоритм з відкритим ключем.

DSA – Алгоритм електронного підпису.

RLWE - навчання з помилками в кільці.

NIST - Національний інститут стандартів та технологій США.

ESTI - Європейський інститут стандартизації телекомунікацій.

ЗМІСТ

ВСТУП

У сучасному світі підприємства все більше використовують документи, тому електронний документообіг замінює традиційні методи розписування на папері. Електронний підпис дозволяє компаніям, приватним підприємцям та владним органам безпечно працювати та обмінюватися електронними документами.

Ефективність функціонування кожної організації залежить від швидкості обробки документації та інформації. Отже, автоматизація документообігу є важливим завданням сучасних компаній. Раніше документообіг на підприємствах був організований на паперових носіях, що затримувало обробку інформації.

Сучасні технології дозволяють значно скоротити час роботи з інформацією, зокрема за допомогою систем електронного документообігу. Для ефективного використання електронного документообігу необхідно розробити алгоритми та засоби побудови електронного підпису, що робить дослідження та порівняльний аналіз таких алгоритмів актуальною задачею.

Ця задача розглядається у дослідженні. Більшість електронних підписів, що використовуються сьогодні, такі як RSA, DSA та ECDSA, не будуть стійкими в умовах застосування потужних квантових комп'ютерів. Проте, вчені по всьому світу, включаючи Україну та вчених ХНУРЕ, працюють над розвитком криптографії, щоб знайти алгоритми, стійкі до квантових атак.

Дослідження алгоритмів цифрового підпису для постквантового періоду є однією з найважливіших тем у сучасній криптографії. З ростом потужності квантових комп'ютерів, багато з традиційних криптографічних алгоритмів можуть бути легко розкриті, що може підірвати безпеку багатьох систем.

Один з алгоритмів, який вивчається в цьому контексті - це Falcon. Цей алгоритм є несиметричним, що означає, що він використовує різні ключи для цифрового підпису та її перевірки. Він також використовує підходи, які є різними від більшості традиційних криптографічних алгоритмів.

Основна ідея Falcon полягає в тому, щоб використовувати випадкові квазі-групи які забезпечуються "вищими" конструкціями, щоб створити алгоритм, який є стійким до квантових атак. Однією з головних переваг Falcon 2 є те, що він може бути

виконаний на стандартних обчислювальних пристроях, таких як смартфони та персональні комп'ютери, що робить його практично використовуваним в різних областях.

Звичайно, немає алгоритму, який був би стійким до будь-яких можливих атак, і Falcon не є винятком. Але цей алгоритм має багато переваг, які роблять його привабливим для використання у постквантовому періоді. Дослідження в галузі цифрового підпису для постквантового періоду продовжуються, і з часом можуть з'явитися ще більш ефективні алгоритми.

Окрім алгоритму Falcon, існують інші алгоритми цифрового підпису, придатні для застосування в постквантовому періоді.

Один з таких алгоритмів - SPHINCS+. Він був розроблений у 2015 році командою дослідників з університету Штутгарт-Гутенберг та Інституту електронної пошти (E-Post) Німеччини. SPHINCS+ базується на підході "гешуй та підписуй" (hash-and-sign), але використовує сильніші хеш-функції та інший підхід до підписування, що забезпечує його стійкість до квантових обчислювачів.

Ще один алгоритм - Dilithium. Цей алгоритм був розроблений в 2017 році командою дослідників з університету Мічигану та Інституту електронної пошти Німеччини. Dilithium базується на підході "решейки з решеткою" (lattice-based), який відомий своєю стійкістю до квантових обчислювачів. Алгоритм використовує складні математичні операції над решетками для створення цифрового підпису.

Крім Falcon, SPHINCS+ та Dilithium, існує ще декілька алгоритмів цифрового підпису, придатних для застосування в постквантовому періоді. Вони розробляються дослідницькими групами з усього світу, і цей процес продовжується. Це дозволить забезпечити безпеку цифрових підписів інформації навіть в умовах розвитку квантових обчислювачів.

Метою цієї роботи є аналіз сучасних алгоритмів електронного підпису, що є стійкими до квантових атак, зокрема на основі алгоритму NTRU грат. [1]

Об'єктом дослідження є квантові обчислення, які дозволяють ефективно зменшити час, необхідний для обчислення секретних ключів та відкритих ключів. Предметом дослідження є алгоритм FALCON, який є переможцем конкурсу постквантових алгоритмів електронного підпису та генерації ключів.

Результатом роботи є порівняння часу генерації ключів цього алгоритму з

результатами інших розробників, оскільки час генерації ключів є важливою характеристикою, оскільки ключі потрібно генерувати для кожного користувача системи в умовах застосування несиметричного алгоритму електронного підпису.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1. Дослідження поняття електронного цифрового підпису

Електронний цифровий підпис (ЕЦП) є інформаційним блоком, який прикріплюється до файлу автором, щоб захистити його від несанкціонованої модифікації і позначити автора [2].

Для роботи системи ЕЦП використовуються два ключі: таємний та відкритий ключі. Таємний ключ зберігається у підписувача, а відкритий ключ публікується у загальнодоступному або спеціалізованому довіднику. Коли користувач має доступ до відкритого ключа, він не може відтворити таємний ключ або поставити цифровий підпис.

Особистий ключ підписувача є повною особистою власністю підписувача і не передається нікому іншому, навіть центру сертифікації ключів. Цифровий підпис можна перевірити будь-ким, хто має доступ до відкритого ключа. [3]

1.2. Класифікація та види електронного цифрового підпису.

У сучасних інформаційно-комунікаційних системах використовуються різні види електронного цифрового підпису (ЕЦП). Простий ЕЦП використовується для авторства та організації документообігу в межах підприємства, але не має юридичної значимості та не гарантує незмінність документа після підписання. Некваліфікований ЕЦП використовується для внутрішнього документообігу та обміну електронними документами між організаціями, але потребує угоди про визнання та використання ЕЦП між компаніями. [4]

Кваліфікований ЕЦП може бути отриманий тільки в акредитованому засвідчувальному центрі та використовується для здачі звітності в державні контролюючі органи та участі в електронних торгах. Процес верифікації підпису та пов'язаних з ним даних може значно відрізнятися залежно від призначення та життєвого циклу підпису. Існують різні типи підпису, такі як одноразові,

короткострокові та довготривалі, залежно від того, чи потрібно зберігати значення підпису після верифікації, чи потрібно проводити верифікацію протягом терміну придатності сертифіката власника ключа підпису, або чи потрібно проводити верифікацію навіть після закінчення терміну повноважень видавця сертифіката.[5]

1.3. Дослідження алгоритмів електронного підпису

Електронно-цифровий підпис є ефективним засобом для автентифікації інформації, оскільки він забезпечує захист від підробки даних, не дозволяє публікації анонімно, та дозволяє керувати цілісністю переданих даних. Для створення коректного підпису необхідно знати закритий ключ, який повинен бути відомий тільки власнику, тому власник не може відмовитися від свого підпису під даними. Якщо дані були навмисно або випадково змінені, то підпис стає недійсним, що робить підробку даних недоцільною в більшості випадків. [6]

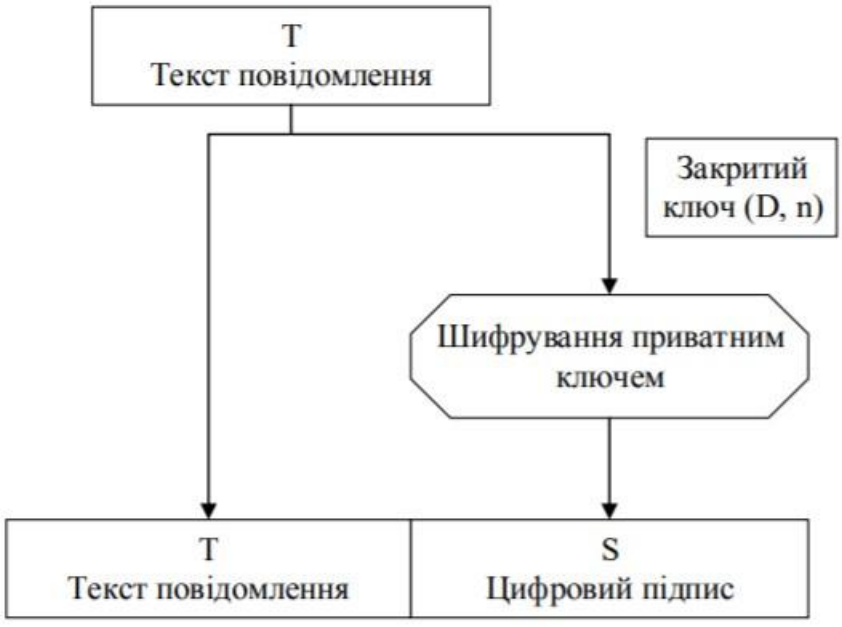

Рисунок 1.1 – Схема використання електронного підпису

Симетричні ЕЦП менш популярні, оскільки не було можливості реалізувати ефективні алгоритми підпису з використанням симетричних шифрів, що були доступні

на той момент. [7]

Для реалізації ЕЦП за допомогою симетричної схеми потрібно мати довірену особу, яка буде користуватися довірою обох сторін. Кожен користувач має обрати секретний ключ і передати його довіреній особі. [8]

Потім відправник може підписати повідомлення, зашифрувавши його своїм секретним ключем, і передати це повідомлення довіреній особі.

Довірена особа розшифрує повідомлення та надішле його отримувачу разом із своїм підписом. Отримувач може перевірити цілісність повідомлення, використовуючи отриманий підпис та довірену особу як джерело довіри. Таким чином, секретний ключ KA відправника відомий тільки йому і довіреній особі. Коли відправник хоче послати відкритим текстом отримувачу підписане повідомлення P, він формує повідомлення, зашифровує його своїм секретним ключем KA (B, RA, t, P) повідомлення з ідентифікатором B, випадковим числом RA, тимчасовим штампом t [9]

Рисунок 1.2 – Алгоритм симетричного електронного підпису

Асиметричні схеми ЕЦП мають наступні переваги:

– не потребують передачі секретного ключа для перевірки підпису, оскільки використовують відкритий ключ, який є загальнодоступним;

– забезпечують можливість перевірки автентичності даних без необхідності передачі самої інформації, оскільки підпис здійснюється окремо від даних. - Дозволяють зберігати секретний ключ в безпеці, оскільки він не передається іншим користувачам ;

– забезпечують можливість застосування цифрових підписів для масової розсилки даних, оскільки не потрібно генерувати окремий ключ для кожного одержувача.

Недоліки асиметричних схем ЕЦП:

– використання асиметричних алгоритмів є більш складним та вимагає більшої обчислювальної потужності, порівняно з симетричними алгоритмами;

– для генерації підпису використовується більш довгий ключ, що призводить до збільшення розміру підпису;

– якщо закритий ключ стане відомим стороннім особам, то це може призвести до порушення безпеки та можливості підробки підпису.

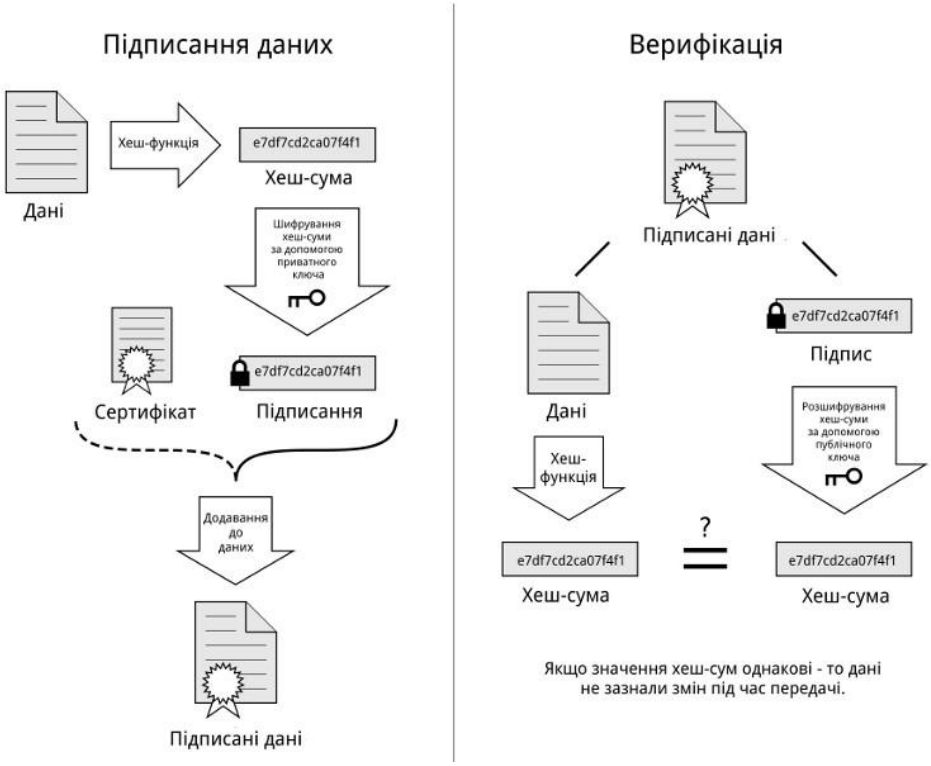

Рисунок 1.3 – Алгоритм асиметричного електронного підпису

Асиметрична схема ЕЦП має один недолік – продуктивність криптографічної схеми. Продуктивність асиметричної криптографічної схеми може виявитися недостатньою для відповідності поставленим вимогам. Рішенням для усунення даного недоліку є застосування спеціальної ефективно обчислюваної функції - функцією хешування чи хеш-функції. На вхід функції подається повідомлення, а на виході отримується слово фіксованої довжини, яка буде набагато менша, ніж початкове повідомлення.

Алгоритм ЕЦП не змінюється, але використовується не саме повідомлення, а значення хеш-функції від нього. Це прискорює процес підпису та перевірки ЕЦП.

1.4. Аналіз вимог до електронного підпису

Алгоритми, що реалізують ЕЦП повинні бути реалізовані так, щоб були дотримані наступні обов’язкові атрибути генерованого підпису:

− ЕЦП аутентичний, з допомогою програмного забезпечення одержувач документа може довести, що він належить підписнику;

− підпис не може бути помилковим. Тобто підпис мусить свідчити про те, що документ міг підписати той і тільки той користувач, чий автограф знаходиться в документі;−конкретний ЕЦП не може бути перенесений, підпис є невід’ємною складовою документу і тому не може функціонувати за його рамками, в інших документах;

− при зміні підписаного документу, програма свідчить користувачу про неактуальність перевіреного документу;

− розроблений алгоритм мусить генерувати унікальні публічні ключі з різними за довжиною факторами;

− будь-яка особа, що є власником підпису, може гарантувати, що документ, підписаний його публічним ключем свідчить про факт його підписання;− сучасні програмні засоби не повинні мати змоги відновити секретний ключ користувача, виходячи з вихідних даних програми.

Як ми знаємо криптографія має основні складові частини які зображені на рисунку 1.4. На сьогоднішній день асиметрична схема формування ЕЦП є найбільш поширена і використовується частіше, ніж симетрична схема. Це обумовлено тим фактом, що симетричні схеми для формування і розшифрування підпису використовують один і той самий ключ. Якщо зашифровану інформацію потрібно передавати, то в даному випадку потрібно і передавати ключ шифрування, саме це може створити проблему, адже якщо канал передачі не захищений, то ключ може бути перехоплений зловмисником. В асиметричних системах цей недолік відсутній, оскільки кожний учасник має пару ключів: відкритий та секретний, які зв’язані між собою.

При цьому формування ЕЦП відбувається за допомогою секретного ключа відправника, а перевірка підпису – за допомогою відкритого ключа, тому необхідність передачі секретного ключа відсутня.

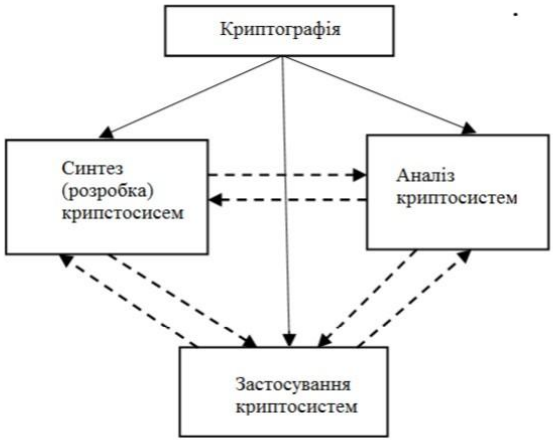

Рисунок 1.4 – Основні складові частини криптографії

У зв’язку з цим, асиметрична система має набагато більшу криптостійкість, тому саме їй надають перевагу під час створення ЕЦП. Загальновизнана схема ЕЦП, заснована на асиметричному алгоритмі охоплює три процеси: генерація відкритого та закритого ключа, формування підпису, перевірка підпису.

1.5. Аналіз сучасних алгоритмів електронного підпису

Зараз існують такі алгоритми створення цифрового підпису: Схема RSA, ЭльГамаля, DSA, ECDSA, ГОСТ Р 34.10-2001, ДСТУ 4145-2002. В даний час більшість відомих алгоритмів ЕЦП засновано на складності рішення однієї з трьох завдань: дискретного логарифмування; факторизації; дискретного логарифмування на еліптичних кривих. Першою і найбільш відомою у всьому світі системою ЕЦП стала система RSA.

Система створення ЕЦП на основі RSA ґрунтується на складності задачі факторизації великих чисел, це забезпечує дуже високу криптостійкість алгоритму. Завдяки цьому схема RSA є найбільш поширеною і використовується практично в усіх

сучасних програмах для створення ЕЦП, але все таки вона має певні недоліки. RSA є набагато повільнішим алгоритмом в порівнянні з симетричними алгоритмами.

Вважається, що для забезпечення необхідної криптостійкості даного алгоритму, потрібно використовувати відкритий ключ розміром не менше 1024 біт, та прості числа – множники розміром не менше 512 біт. Для створення електронно-цифрового підпису при заданих параметрах необхідні великі обчислювальні ресурси, тому час створення ЕЦП збільшується.

На сьогоднішній день відомі деякі способи злому алгоритму RSA, тому при практичному використанні даного алгоритму необхідно також дотримуватися певних умов підбору параметрів системи p і q. Проаналізувавши схему RSA, можна зробити висновок, що перевагами данного алгоритму є забезпечення високої криптостійкості при певній довжині ключа та простота алгоритму. Недоліки: складність обчислення ЕЦП, так як необхідні великі обчислювальні ресурси, повільність підписання документу. Більш надійний і зручний для реалізації на персональних комп'ютерах алгоритм цифрового підпису був розроблений в 1984 р. американцем арабського походження Тахер Ель Гамалем.

Схема цифрового підпису Ель Гамаля має ряд переваг у порівнянні зі схемою цифрового підпису RSA:

1) при заданому рівні стійкості алгоритму цифрового підпису цілі числа, що беруть участь в обчисленнях, мають запис на 25% коротше, що зменшує складність обчислень майже в два рази і дозволяє помітно скоротити обсяг використовуваної пам'яті;

2) при виборі модуля p достатньо перевірити, що це число є простим і що у числа (p-1) є великий простий множник;

3) процедура формування підпису за схемою Ель Гамаля не дозволяє обчислювати цифрові підписи під новими повідомленнями без знання секретного ключа.

Однак алгоритм цифрового підпису Ель Гамаля має і деякі недоліки порівняно зі схемою підпису RSA. Зокрема, довжина цифрового підпису в 1,5 рази більша, що, в свою чергу, збільшує час її обчислення. У 1991 р. в США був опублікований проект федерального стандарту цифрового підпису - DSS (Digital Signature Standard), що описує систему цифрового підпису DSA (Digital Signature Algorithm). Алгоритм DSA є

розвитком алгоритмів Ель Гамаля і Шнорра. Його надійність заснована на практичній складності розв’язання задачі обчислення дискретного логарифма. Довжина підпису в системі DSA менше, ніж в RSA, і становить 320 біт.

Функції DSA обмежені тільки цифровим підписом, система принципово не призначена для шифрування даних. По швидкодії система DSA має однакові параметри з RSA при формуванні підпису, але істотно (в 10-40 разів) поступається їй при перевірці підпису. Алгоритм ECDSA з відкритим ключем для створення цифрового підпису, аналогічний за своєю будовою DSA, але на відміну від нього використовує не цілі числа, а групи точок еліптичної кривої. Стійкість алгоритму ґрунтується на проблемі дискретного логарифмування в групі точок еліптичної кривої. Існують вагомі переваги ECDSA над DSA.

По-перше, секретний ключ в ECDSA є унікальним, а не лише випадковим, як в DSA, що покращує надійність алгоритму. Крім того, завдяки складності проблеми дискретного алгоритмування по точках еліптичної кривої систему ECDSA є більш криптостійким і надійним. При цьому довжина підпису залишається такою ж, як і в DSA, і складає 320біт .

1.6 Постановка задачі

Загальна мета дослідження алгоритмів цифрового підпису для постквантового періоду з використанням Falcon полягає в розробці ефективних та безпечних засобів забезпечення конфіденційності, цілісності та автентичності даних в умовах загроз, що виникають у зв'язку з розвитком квантових комп'ютерів.

Завдання дослідження полягає в оцінці безпеки алгоритму Falcon на різних етапах виконання, визначенні можливостей атак на цей алгоритм та розробці заходів для запобігання цим атакам. Також важливим завданням є порівняння ефективності Falcon з іншими алгоритмами цифрового підпису для постквантового періоду та виявлення його переваг та недоліків.

Отже, загальна мета дослідження полягає в розробці та вдосконаленні алгоритмів цифрового підпису для постквантового періоду з метою забезпечення безпеки та

ефективності при передачі та збереженні даних в умовах розвитку квантових технологій.

2 АНАЛІЗ АЛГОРИТМІВ ЕЛЕКТРОНОГО ПІДПИСУ ЗАХИЩЕНИХ ВІД КВАНТОВИХ АТАК

2.1. Захищеність сучасних алгоритмів електронного підпису від квантових атак

Не всі протоколи безпеки та криптографічні алгоритми вразливі до квантових атак, деякі з них вважаються безпечними, тоді як деякі, як вже відомо, вразливі. Контроль безпеки, який вважається квантово-безпечним сьогодні, з часом і при достатніх дослідженнях може бути визначений вразливим. Без доказів того, що алгоритм вразливий до квантової атаки, криптографічний примітив та протоколи, які його використовують, вважаються квантово-безпечними, якщо вони добре вивчені та протидіють атакам, з використанням усіх відомих квантових алгоритмів.

Електронний підпис дозволяє підтвердити авторство електронного документа чи то реальна особа або, наприклад, аккаунт в криптовалютній системі. Підпис пов'язаний як з автором, так і з самим документом за допомогою криптографічних методів, і не може бути підробленим за допомогою звичайного копіювання.

ЕЦП - це реквізит електронного документа, отриманий в результаті криптографічного перетворення інформації з використанням закритого ключа підпису, що дозволяє перевірити відсутність спотворення інформації в електронному документі з моменту формування підпису тобто цілісність, приналежність підпису власникові сертифіката ключа підпису тобто авторство, а в разі успішної перевірки підтвердити факт підписання електронного документа, неспростовності.

Надійність цифрового підпису визначається стійкістю до крипто аналітичних атак двох її компонент: хеш-функції і самого алгоритму ЕЦП. Стійка схема цифрового підпису повинна використовувати хеш-функцію.

2.2. Критерії по відбору для пост квантових алгоритмів

Як вже зазначалося вище, надійність цифрового підпису визначається стійкістю до криптоаналітичних атак алгоритму ЕЦП, що залежать від кожного окремого

алгоритму шифрування. Вимоги до пост квантових алгоритмів, ще точно не задані. NIST (Національний інститут стандартів та технологій США) та ESTI (Європейський інститут стандартизації телекомунікацій) у 2016 році почали роботу над стандартизацією та пошуком алгоритмів шифрування, в тому числі і для електронного цифрового підпису.

Мінімальні критерії, що визначив NIST до кандидатів пост квантових алгоритмів на першому етапі відбору до першого раунду були наступні: реалізація на мові програмування С, проходження тестів з відомими відповідями, реалізація в широкому діапазоні апаратних та програмних платформ. Далі алгоритми, що пройшли до першого раунду оцінювали за трьома показниками: безпека, вартість і продуктивність, й алгоритм та особливості реалізації.

Усвідомлюючи, що існує значна невизначеність в оцінці сильних сторін безпеки пост-квантових алгоритмів-кандидатів, NIST виділила п'ять категорій безпеки, щоб краще порівнювати рівень безпеки, наведений у поданнях. Після перевірки безпеки наступним найбільш важливим критерієм при відборі кандидатів другого туру була результативність.

При оцінці ефективності кандидатів NIST враховував як розміри ключа, шифртекста, підпису, так і обчислювальні оцінки, що були надані кандидатами-заявниками в їх документації. Крім зазначеного вище, NIST розглянув зовнішні відгуки та оцінки продуктивності, надані криптографічним співтовариством. Можна відзначити, що NIST заявив, що «параметри ефективності не будуть грати важливу роль на ранній стадії процесу оцінки», і NIST не використовував показники ефективності та швидкодії реалізації як вагомого критерії при прийнятті свого рішення.

У кількох випадках представлений алгоритм був обраний частково за його унікальність і елегантність. NIST зазвичай віддавав перевагу тим проектам, які були засновані на чітких принципах або тим чи іншим чином демонстрували інноваційну ідею. NIST вважає, що різноманітність конструкцій дасть можливість криптографам і криптоаналітикам розширити сферу ідей у своїй галузі, а також зменшить ймовірність того, що один тип атаки усуне основну частину кандидатів, обраних в процесі стандартизації.

Алгоритми, які не були обрані для переходу до наступного раунду, не розглядаються для стандартизації NIST. Серед алгоритмів для цифрового підпису у

другий раунд було обрано дев’ять кандидатів що пройшли перевірку на безпеку, ефективність та вартість. Це такі алгоритми як: Picnic, Rainbow, MQDSS, LUOV, GeMSS, SPHINCS+, qTesla, FALCON, CRYSTAL-DILITHIUM.

2.3. Умови для реалізації постквантових алгоритмів ЕЦП

Знаючи сучасні методи атак на пост квантові алгоритми можна сказати, що при реалізації пост квантових алгоритмів цифрового підпису повинні виконуватись такі умови:

− надійність математичної бази, що застосовується для цифрових підписів при криптоперетвореннях;

− практична захищеність криптографічних перетворень типу цифрових підписів від відомих атак;

− реальна захищеність цифрових підписів від усіх відомих і потенційно можлив их критпоаналітичних атак;

− стійкість цифрових підписів в умовах появи квантового комп'ютера.

2.4. Характеристика кандидатів алгоритмів цифрового підпису

Dilithium – це схема підпису на гратах, побудована з використанням евристики Фіата-Шаміра, безпека якої заснована на твердості проблеми MLWE. Dilithium входить в комплект CRYSTALS разом з механізмом обміну ключами Kyber. Основне нововведення Dilithium полягає в тому, що розмір відкритого ключа зменшується, опускаючи деякі біти низького порядку; щоб компенсувати це, кожний підпис включає в себе додаткову «підказку», яка дозволяє верифікатору перевіряти підпис.

Dilithium пропонує досить хорошу продуктивність і є відносно простим в реалізації. Найбільш відомі атаки проти Dilithium засновані на редукції грати, без істотного використання алгебраїчної структури задачі MLWE. Вибір параметрів для

Dilithium базується на консервативних оцінках вартості цих атак. Dilithium має формальний доказ безпеки в класичній моделі випадкового оракулу. Це доказ не є суттєвим і розбивається в квантовій моделі випадкового оракулу; однак поки що не відомо ніяких подібних.

qTESLA – схема підпису на основі грат, яка використовує припущення, що розподіл RLWE (Ring learning with errors – навчання з помилками в кільці) нічим не відрізняється від випадкових. Відкритий ключ в qTESLA, грубо кажучи, є зразком розподілу RLWE. Підписувач зберігає секретну інформацію про цей зразок розподілу і використовує цю інформацію разом з хеш-функцією для створення підписів.

Перевірка підпису включає в себе деяку просту арифметику всередині обраного кільця, а потім перерахунок хеш-функції. qTESLA має досить хороші параметри продуктивності в порівнянні з іншими схемами підписів на базі грати. Falcon – це також схема підпису на грат, заснована на GPV (GentryPeikertVaikuntanathan) Гауссовій вибірці з використанням грати NTRU. Основне нововведення – дуже швидкий рекурсивний алгоритм гауссової вибірки, що використовує деревовидну структуру даних («Falcon-дерево»). Найбільш відомі атаки проти Falcon засновані на зменшенні грати, без істотного використання спеціальної структури грати NTRU.

Falcon має формальний доказ безпеки в квантовій моделі випадкового оракулу. Falcon пропонує дуже хорошу 47 продуктивність. Однак це досить складно реалізувати, оскільки він значною мірою спирається на структуру «tower of fields» числового поля і вимагає обчислень з плаваючою точкою подвійної точності. Необхідно прикласти додаткові зусилля для тестування, щоб забезпечити, що підпис є стійким до побічних каналів атак. GeMSS – це «big-field» багатовимірная схема цифрового підпису у добревивченому сімействі HFEv (Hidden Field Equations). Схема перетворює базовий 48 HFEv-дизайн, імовірно має екзистенціальну непростимость, в схему захищеної підпису EUF-CMA з використанням конструкції Файстеля-Патарина. Екзистенціальна вимога непростимості для HFEv-дизайну слабо пов'язана з добре вивченими MQ (багатовимірними квадратичними) і MinRank-завданнями. GeMSS пропонує деякі з найменших довжин підпису Серед всіх уявлень. GeMSS також виграє від того, що HFEv-конструкція є одним з найбільш вивчених примітивів підпису в літературі. Крім розміру підпису та часу перевірки, деякі інші характеристики продуктивності підпису GeMSS викликають деякі побоювання. Час підпису досить великий, розмір відкритого

ключа також; ці властивості можуть бути особливостями схеми GeMSS, які були успадковані від HFEvметодології.

Тим не менш, аналіз безпеки показує, що можливі компроміси між ступенем прив'язки, мінус ранг проекції і кількість vinegar змінних, наприклад, які можуть вплинути на різні характеристики продуктивності. LUOV – «small-field» багатовимірна схема цифрового підпису, заснована на схемі незбалансованого «Масла та оцту» (UOV - nbalanced Oil and Vinegar). Основним нововведенням схеми є визначення відкритого ключа у вигляді карти на певному кінцевому поля в той час, як коефіцієнти публікуються на суб-полі.

Схема дозволяє уникнути атак, які безпосередньо використовують структуру субполя, використовуючи hash-and-sign підхід, гарантуючи, що розширення поля має бути використаним. Схема також використовує псевдовипадковий генератор для побудови частини відкритого ключа, для якої може бути вирішена відповідна частина 49 закритого ключа, аналогічна конструкцій в циклічних UOV, циклічних радугах і їх псевдовипадкових аналогах. MQDSS – це багатовимірна схема цифрового підпису, отримана з доведено безпечної схеми ідентифікації, заснованої на проблемі MQ.

Схема підпису будується з ідентифікаційної схеми шляхом застосування узагальнення перетворення Фіата-Шаміра, відповідних 5-прохідних схемам ідентифікації. Відзначимо, що запропоновані параметри не задовольняють гіпотезам зниження безпеки. MQDSS підтримує генерацію псевдовипадкових ключів з великими підписами. Характеристики продуктивності MQDSS найбільше можна порівнянняти з характеристиками схем підпису на основі хешу. Rainbow – це багатовимірна схема цифрового підпису, яка є узагальненням структури UPOV, що дозволяє параметризацію, які більш ефективна за рахунок додаткової алгебраїчної структури. Rainbow підпис в його форматі вивчається вже близько п’ятнадцяти років з різними параметрами. Picnic – це схема підпису, яка не використовує теоретико-числові або структуровані припущень складності. Зменшення безпеки відносяться до хешфункцій і симетричних блокових шифрів.

Підпис Picnic базується на неінтерактивному нульовому доказі знання секретного ключа. Підписується відкритий текст таким чином (через хешування), що тільки власник секретного ключа може вивести доказ і перевірити текст на валідність. SPHINCS+ – це схема підпису на основі хешу без стану.

Схеми підписів на основі хеш були вперше запропоновані в кінці 1970-х років, і з тих пір було розроблено багато поліпшень. SPHINCS+ використовує дві різні схеми підпису на основі хеш: Winternitz One-Time-Signature Plus (WOTS+), одноразову схему підпису і ліс випадкових підмножин (FORS), схему з декількома сигнатурами. Пара ключів підпису SPHINCS+ складається з 260 або більше пар ключів FORS.

3 ДОСЛІДЖЕННЯ АЛГОРИТМУ ЕЛЕКТРОННОГО ПІДПИСУ FALCON

3.1 Дослідження поняття електронного цифрового підпису

Falcon — це алгоритм криптографічного підпису, представлений у проекті пост квантової криптографії NIST 30 листопада 2017 року. Він був розроблений: П'єром-Аленом Фуке, Джеффрі Хоффштейном, Полом Кіршнером, Вадимом Любашевським, Томасом Порніном, Томасом Престом, Томасом Рікоссе, Грегором. Зайлер, Вільям Уайт, Чженфей Чжан.

Суть пост квантового криптографічного алгоритму у тому, щоб продовжувати забезпечувати свої характеристики безпеки навіть під час роботи з квантовими комп'ютерами . Квантові комп'ютери вважаються здійсненними, згідно з нашим нинішнім розумінням законів фізики, але ще доведеться вирішити деякі важливі технологічні проблеми, щоб побудувати повністю працюючий пристрій. Такий квантовий комп'ютер дуже ефективно зламав би звичайні алгоритми асиметричного шифрування та цифрового підпису, що базуються на теорії чисел (RSA, DSA, Діффі-Хеллмана, Ель-Гамаля та їх варіанти на основі еліптичних кривих).

Falcon заснований на теоретичній основі Джентрі, Пейкерта та Вайкунтанатана для схем підпису на основі грат. Ми реалізуємо цю структуру поверх грат

NTRU за допомогою семплера з лазівкою, званого «швидкою вибіркою Фур'є». Основна важка проблема - це завдання про коротке ціле рішення (SIS) над гратами NTRU, для якої в загальному випадку в даний час не відомий ефективний алгоритм рішення, навіть за допомогою квантових комп'ютерів.

3.2. Головний принцип алгоритму Falcon

Логічне обґрунтування конструкції FALCON випливає з простого спостереження: при переході з підписів на основі RSA або дискретного логарифма на пост-квантові підписи складність зв'язку, ймовірно, буде більшою проблемою, ніж швидкість. Дійсно, багато пост-квантових схем мають простий алгебраїчний опис, який робить їх

швидкими, але вони завжди вимагають або ключів більшого розміру, ніж до-квантові схеми, або підписів великого розміру, або обох. Очікується, що такі проблеми з продуктивністю будуть перешкоджати переходу від до-квантових до пост-квантових схем. [10]

Отже, основний принцип FALCON полягає в тому, щоб мінімізувати таке значення: | pk | | sig | (бітовий розмір відкритого ключа та бітовий розмір підпису).

Саме тому авторами використовуються грати, які дозволяють зробити як |pk| , так і |sig| досить малими, у тому ж числі структуровані грати. Коли мова йде про підписи на основі грати, існує дві парадигми: Fiat-Shamir або hash-and-sign.Обидві парадигми досягають порівнянних рівнів компактності, але hash-and-sign має цікаві властивості: структура GPV, яка описує, як отримати схеми підписів на hash-and-sign, безпечні в класичній і квантовій моделі оракула.

Для реалізації структури GPV використовуються грати NTRU: як наведено, вони дозволяють отримати досить компактну реалізацію структури GPV. Крім того, вони подаються з кільцевою структурою, яка прискорює багато операцій на два порядки. Останнім кроком був семплер з пасткою.

У алгоритмі використовується семплер з пасткою, який асимптотично такий ж швидкий, як найшвидший універсальний семплер, і забезпечує той же рівень безпеки, що і найбезпечніший семплер.

3.3. Основні функції алгоритму Falcon

Алгоритм Falcon забезпечує:

− безпека: для генерації ключів застосовується розподіл Гауса, що забезпечує неможливість визначення додаткових характеристик для секретного ключа по відкритому ключу, фактично відкритий ключ виглядає як випадковий.− Компактність: завдяки використанню грат NTRU підпис істотно коротше, ніж у будь-якій схемі підпису на основі грат з тими самими гарантіями безпеки, а відкриті ключі мають приблизно такий самий розмір;

− швидкість: використання швидкої вибірки Фур'є дозволяє дуже швидко

реалізовувати тисячі підписів на секунду на звичайному комп'ютері; перевірка проходить у п'ять-десять разів швидше; (див додаток В.)

− масштабованість: операції стоять O(n log n) для ступеня n що дозволяє використовувати дуже довготривалі параметри безпеки при помірних витратах;

− економія оперативної пам'яті: удосконалений алгоритм генерації ключів Falcon використовує менше ніж 30 кілобайт оперативної пам'яті, що в сотні разів менше в порівнянні з попередніми розробками, такими як NTRUSign. Falcon сумісний із невеликими вбудованими пристроями з обмеженим об'ємом пам'яті.

4 АЛГОРИТМ ГЕНЕРАЦІЇ КЛЮЧІВ

4.1. Основні етапи

Включає наступні етапи:

– генерація малих поліномів f, g;

– генерація полінома $h = g / f \pmod{q, \mod x^n+1}$;

– генерація малих поліномів F, G, таких що задовольняють NTRU рівнянню: $f*G – g*F = q \pmod{xn+1}$.

Генерація малих поліномів f, g.

Коефіцієнти поліномів f, g повинні задовольняти розподілу Гауса, що забезпечує властивості для полінома h, як для випадкового полінома. (див. додаток Б.)

Норма поліномів $||f|| + ||g||$ повинна бути менше ніж 1.172q.

Генерація полінома $h = g / f \pmod{q, \mod xn+1}$. Поліном f повинен мати інверсію, що забезпечує можливість обчислення поліному h. Для оптимізації операції ділення поліномів застосовують NTT формат для поліномів f, g.

Генерація малих поліномів F, G:

– для поліномів f, g виконати покроковий перехід від поля x^n+1 до полів $x^{n/2}+1$, $x^{n/4}+1$, .. x^1+1 В результаті отримаємо поліноми: f(n/2) – поліном f для поля $x^{n/2}+1$, який має n/2 коефіцієнтів g(n/2) – поліном g для поля $x^{n/2}+1$, який має n/2 коефіцієнтів f(n/4) – поліном f для поля $x^{n/4}+1$, який має n/4 коефіцієнтів g(n/4) – поліном g для поля $x^{n/4}+1$, який має n/4 коефіцієнтів … f(1) – поліном f для поля x+1, який має один коефіцієнт g(1) – поліном g для поля x+1, який має один коефіцієнт;

– вирішити діафантове рівняння $f(1)*G'(1) – g(1)*F'(1) = 1$

відносно невідомих F’(1), G’(1); (умова існування рішення в цілих числах – $GCD (f(1), g(1)) = 1$);

– обчислити $F (1) = q * F'(1)$; $G (1) = q * G'(1)$; F (1), G (1)- рішення рівняння $f(1)*G (1) – g(1)*F (1) = q$, поліноми F (1), G (1) мають по одному коефіцієнту;

– для пари поліномів F (1) G (1), виконати покроковий перехід від поля x+1 до полів x^2+1, x^4+1, .. x^n+1.

В результаті отримаємо поліноми:

– f (512, 1024) – поліном, який має 512, 1024 коефіцієнтів, які задовільняють розподілу Гауса;

– g (512, 1024) – поліном, який має 512, 1024 коефіцієнтів, , які задовільняють розподілу Гауса;

– F (512, 1024) - поліном. який має 512, 1024 коефіцієнтів, які задовільняють NTRU рівнянню;

– G (512, 1024) - поліном. який має 512, 1024 коефіцієнтів, які задовільняють NTRU рівнянню;

Функції для генерації поліномів f, g наведені в Додатку Б.

Функції для генерації відкритого ключа h для операції ділення поліномів застосовує перетворення Фурє, функції для реалізації якого наведені в Додатках В, Г.

Нижче описано алгоритм обчислення поліномів F, G.

– Перехід від поля x^t+1 до поля $x^{t/2}+1$;

– вхід: поліном a з коефіцієнтами $a_0, a_1, \ldots, a_{t-1}$;

– вихід: поліном a з коефіцієнтами $b_0, b_1, \ldots, b_{t/2-1}$.

Формування двох поліномів e, o, перший з коефіцієнтами з парними номерами, другий з непарними $e_j = a_{2j}$ (j =0, 1, t/2 - 1) ; $o_j = a_{2j+1}$ (j =0, 1, t/2 - 1).

Обчислення поліномів $e2 = e^2 \bmod x^{t/2}+1$; $o2 = o^2 \bmod x^{t/2}+1$; 3 Обчислення поліному b:

$b_0 = e2_0 + o2_{t/2 - 1}$

$b_{j+1} = e2_{j+1} – o2_j$ (j = 0, 1, … t/2 - 2)

При виконанні кроків 2 та 3 застосовують великі числа.

Перехід від поля x^t+1 до поля $x^{2t}+1$ включає:

– обчислення поліномів для поля $x^{2t}+1$;

– редукцію поліномів згідно BABAI редукції.

Для формування поліному F’(2t) для поля $x^{2t}+1$ застосовують поліном F(t) для поля x^t+1 та поліном g(2t) для поля $x^{2t}+1$.

Для формування поліному G’(2t) для поля $x^{2t}+1$ застосовують поліном G(t) для поля x^t+1 та поліном f(2t) для поля $x^{2t}+1$.

Для перетворення застосовують однакові операції:

– Вхід: поліном A(t) з коефіцієнтами A(t)0, A(t)1, …, A(t)t-1; поліном b(2t) з

коефіцієнтами $b(2t)_0$, $b(2t)_1$, …, $b(2t)_{2t-1}$;

– Вихід: поліном C(2t) з коефіцієнтами $C(t)_0$, $C(t)_1$, …, $C(t)_{2t-1}$.

1. Формування поліному u для поля $x^{2t}+1$: $u_{2j}= A(t)j$; $u_{2j+1}= 0$

(j = 0, 1, …t-1);

2. Формування поліному v для поля $x^{2t}+1$: $v_{2j}= b(2t)_{2j}$; $v_{2j+1}= b(2t)_{2j+1}$ (j = 0, 1, …t-1);

3. Обчислення поліному w для поля $x^{2t}+1$: $w = u * v \bmod x^{2t}+1$;

4. Обчислення поліному C Після виконання цього етапу отримані поліноми F’(2t), G’(2t);

5. В результаті BABAI редукції отримаємо (F(2t), G(2t)) = (F’(2t) – k* f(2t), G’(2t)- k * g(2t)).

Після обчислення поліномів для поля x^2+1, x^4+1, … x^n+1 отримані значення – поліноми F, G.

ВИСНОВКИ

В ході виконання роботи була досліджена предметна область дослідження алгоритмів цифрового підпису для постквантового періоду та дослідження роботи алгоритму Falcon. Виділено основні завдання для використання цифрового підпису та захисту цифрових даних. Розглянуто найвідоміші та найактуальніші алгоритми цифрового підпису. Було розглянуто та проаналізовано основні підходи та їх методи для аналізу алгоритмів цифрового підпису, виділено їх основні переваги та недоліки. Розглянуто основні метрики, які використовуються у якості вхідних даних для подальшого аналізу.

Виконано порівняння по цим метрикам алгоритмів, представлених на конкурс. Показано, що алгоритм Falcon має найкращі характеристики в порівнянні з іншими алгоритмами, тобто найкоротший відкритий ключ та цифровий підпис.

В практичній частині роботи виконано реалізацію алгоритму генерації ключів для Falcon, який включає в себе генерацію поліномів f, g с малими коефіцієнтами, поліномів F, G які задовольняють NTRU рівнянню, виконані усі етапи, для розробки консольної програми.

ПЕРЕЛІК ПОСИЛАНЬ

1) Falcon: Fast-Fourier Lattice-based Compact Signatures over NTRU [Електронний ресурс] – Режим доступу до ресурсу: https://falcon-sign.info.

2) Gómez Pardo J. Introduction to Cryptography with Maple / José Luis Gómez Pardo., 2012. – 736 с.

3) Вербицький О. Вступ до криптології/Вербицький О. – Львів : Видавництво науково- технічної літератури, 1998. – 247 с.

4) Bruce S. Applied Cryptography / Schneier Bruce., 2015. – 784 с. – (Wiley).

5) Горбенко І.Г., Кузнєцов О.О. Постквантова криптографія та механізми її реалізації // Радіотехніка. 2016. № 186. С.: 32-52. 5. Аитов В. Интеграция информационной системы вуза с системой e-learning. М.: Синергия, 2015. – 7с.

6) Salomon D. Data Privacy and Security / David Salomon., 2012. – 479 с.

7) Gorbenko I.D., Kachko O.G. Substantiation and proposals for the selection, improvement and standardization of the post-quantum electronic signature mechanism at the national and international levels. Radiotekhnika, 4(207), 5–26. https://doi.org/10.30837/rt.2021.4.207.01 DOI: 10.30837/rt.2021.4.207.01.

8) І.Д. Горбенко, О.Г. Качко, О.В. Потій, А.М. Олексійчук, Ю.І. Горбенко, М.В. Єсіна, .В. Стельник, В.А. Пономар Основні положення та результати порівняння властивостей електронних підписів постквантового періоду на алгебраїчних решітках / Радіотехніка No 205, 2021.

9) О.Г. Качко, Ю.І. Горбенко, В.А. Пономар, М.В. Єсіна, С.О. Кандій «Оптимізація алгоритму множення поліномів для NTRU-подібних алгоритмів» / Радіотехніка No 200, 2020.

10) Post-Quantum Cryptography | CSRC [Електронний ресурс] – Режим доступу до ресурсу: https://csrc.nist.gov/projects/post-quantum-cryptography.