Міністерство освіти і науки України
Харківський національний університет імені В.Н. Каразіна
Навчально-науковий інститут комп'ютерних наук та штучного інтелекту
Спеціальність 125 «Кібербезпека»
Освітня програма «Кібербезпека»

В.о. зав. кафедрою КІСМТ
Марина ЄСІНА
"Допущено до захисту"
« »_____2025 р.

Пояснювальна записка

до кваліфікаційної роботи бакалавра

на тему: «Методи та засоби електронного підпису на основі одноразових ключів для постквантового періоду»

оцінка « _____ »

Голова ЕК

Мичуда Л. З.

Керівник: к.т.н. Шеханін К. Ю.

Рецензент: к.т.н., доцент Лещишин Ю. З.

Виконавець: студент групи КБ-41

Старченко Є. К.

Харків – 2025

РЕФЕРАТ

Пояснювальна записка до дипломної роботи бакалавра складається з 53 сторінок основного тексту, містить 12 ілюстрацій, 1 таблицю, 5 додатків і 34 бібліографічні джерела.

Метою роботи є всебічне вивчення інноваційних методологій створення систем цифрового підпису, що здатні протистояти викликам епохи квантових технологій. Центральним фокусом роботи є детальний розгляд криптографічних механізмів на базі одноразових криптографічних ключів та оцінка їх практичної придатності у майбутньому постквантовому світі.

Об’єкт дослідження — криптографічні системи електронного підпису нового покоління, спроможні забезпечувати надійний захист інформації навіть в умовах функціонування потужних квантових обчислювальних систем.

Предметом дослідження виступають технології квантового розподілу криптографічних ключів (QKD), сучасні постквантові криптографічні алгоритми та концептуальні підходи до створення систем одноразового цифрового підпису. Досліджуються особливості їх програмно-технічної імплементації, функціональні переваги та обмеження з точки зору забезпечення тривалої інформаційної безпеки.

Під час виконання дослідження здійснено компаративний аналіз класичних криптографічних підходів та перспективних рішень, орієнтованих на протидію майбутнім квантовим загрозам. Окрему увагу приділено вивченню практичних аспектів інтеграції досліджуваних технологій у сучасну інфраструктуру захисту цифрових операцій.

Отримані в роботі наукові результати мають практичне значення для формування майбутніх регламентів безпечного електронного підпису та можуть бути використані установами, що розглядають можливість міграції до постквантових криптографічних систем.

Ключові слова**:** КВАНТОВІ КРИПТОГРАФІЧНІ ТЕХНОЛОГІЇ, КВАНТОВИЙ РОЗПОДІЛ КЛЮЧІВ, ОДНОРАЗОВЕ ШИФРУВАННЯ, ЕЛЕКТРОННИЙ ПІДПИС, КВАНТОВО-СТІЙКІ АЛГОРИТМИ, КРИПТОГРАФІЯ МАЙБУТНЬОГО, ОБЧИСЛЮВАЛЬНІ МЕТОДИ.

ABSTRACT

The explanatory note to the bachelor's thesis consists of 50 pages of the main text, contains 12 illustrations, 1 table, 5 appendices and 34 bibliographical sources.

The objective of this work is a comprehensive study of innovative methodologies for creating digital signature systems capable of withstanding the challenges of the quantum technology era. The central focus of the work is a detailed examination of cryptographic mechanisms based on one-time cryptographic keys and an assessment of their practical applicability in the future post-quantum world.

The research object consists of next-generation electronic signature cryptographic systems capable of ensuring reliable information protection even under the operation of powerful quantum computing systems.

The research subject encompasses quantum key distribution (QKD) technologies, modern post-quantum cryptographic algorithms, and conceptual approaches to creating one-time digital signature systems. The study examines the characteristics of their software and technical implementation, functional advantages and limitations from the perspective of ensuring long-term information security.

During the research execution, a comparative analysis was conducted between classical cryptographic approaches and promising solutions oriented toward countering future quantum threats. Special attention was given to studying the practical aspects of integrating the investigated technologies into the modern infrastructure for protecting digital operations.

The scientific results obtained in this work have practical significance for the formation of future regulations for secure electronic signatures and can be utilized by institutions considering migration to post-quantum cryptographic systems.

Keywords: QUANTUM CRYPTOGRAPHIC TECHNOLOGIES, QUANTUM KEY DISTRIBUTION, ONE-TIME ENCRYPTION, ELECTRONIC SIGNATURE,

QUANTUM-RESISTANT ALGORITHMS, FUTURE CRYPTOGRAPHY, COMPUTATIONAL METHODS.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ПК	портативний комп’ютер;
ЕП	електронний підпис;
ОК	одноразовий ключ;
КО	квантовий обчислювальний;
КВ	квантовий;
Крипто	криптографічний;
КП	криптографічний протокол;
КЕ	криптографічна ефективність;
СЗЗ	система захисту з відкритим ключем;
СКЗ	система криптозахисту;
ПО	програмне забезпечення;
ПК	персональний комп'ютер;
ШФР	шифрування;
ДЗЗ	довірена третя сторона;
ПКЗ	публічний ключовий засіб;
КР	криптографічний розклад;
ЗВ	захист від квантових атак.

ВСТУП

У контексті стрімкого розвитку інформаційних технологій та глобальної цифровізації, постає критична необхідність у створенні надійних та захищених механізмів передачі даних, що забезпечують збереження конфіденційності та автентичності інформації. Процеси створення, передачі та обробки цифрових документів, зокрема у сфері електронних довірчих сервісів, потребують впровадження специфічних технологічних рішень, які гарантують їх неспотвореність та підтверджують походження.

Прийнятий 1 січня 2023 року Закон України "Про електронні довірчі послуги" (№ 2155-VIII) формує нормативно-правову базу та встановлює регуляторні принципи функціонування електронних довірчих сервісів на території України. Основна мета даного нормативного акту полягає у стимулюванні поширення та практичного застосування електронних довірчих технологій з одночасним забезпеченням їх юридичної валідності та технічної надійності.

Означений законодавчий документ легітимізує електронний підпис як інструмент верифікації достовірності цифрових документів та підтримання їх структурної цілісності. Документ формулює технічні специфікації для електронних підписів та закріплює їх правову силу в українському правовому полі.

Крім того, законодавство деталізує кваліфікаційні вимоги до постачальників електронних довірчих сервісів та встановлює рамки їх професійної діяльності. Нормативний акт фіксує критерії безпеки та приватності для електронних довірчих послуг, одночасно гарантуючи правовий захист інтересів споживачів таких сервісів.

Значення цього законодавства є критичним для прогресу електронної торгівлі, цифрового врядування та інших галузей, що активно використовують цифрову документацію та електронні довірчі технології. З огляду на зростаючу актуальність питань кібербезпеки та інформаційного захисту, цей нормативний акт формує правову

платформу для імплементації захисних технологій та підтримує суспільну довіру до електронних довірчих сервісів.

Відповідно, представлена дипломна робота концентрується на науковому вивченні та практичному впровадженні алгоритмічних рішень для передачі криптографічних ключів електронного підпису відповідно до положень Закону України "Про електронні довірчі послуги". Цей законодавчий акт становить фундаментальну правову основу, що визначає параметри безпеки та довіри до електронних довірчих технологій в Україні, забезпечуючи їх стабільне функціонування та захист кінцевих користувачів.

Варто також зазначити, що наукові результати даного дослідження були успішно презентовані на «IX Міжнародній науково-технічній конференції у м. Львів» та отримали схвальну оцінку наукової спільноти [34].

1 ДОСЛІДЖЕННЯ ФУНДАМЕНТАЛЬНИХ АСПЕКТІВ ЦИФРОВОГО ПІДПИСУ ТА КВАНТОВО-ОБЧИСЛЮВАЛЬНИХ ТЕХНОЛОГІЙ

1.1 Концептуальні основи електронного підпису та його значення у сфері кібербезпеки

Електронний підпис являє собою технологічний механізм, який забезпечує цифрову автентифікацію та гарантує правову силу електронних документів у сучасному інформаційному суспільстві. За своєю суттю електронний підпис є математичним алгоритмом, що базується на криптографічних методах і дозволяє однозначно ідентифікувати автора документа, підтвердити цілісність переданої інформації та забезпечити юридичну відповідальність за підписані дані [1].

Сучасні системи електронного підпису інтегровані у широкий спектр інформаційних платформ – від банківських систем та електронного документообігу до державних порталів надання послуг. Наприклад, в Україні електронний підпис активно використовується у системі "Дія", що демонструє практичну реалізацію концептуальних основ цифрової автентифікації у повсякденному житті громадян, як показано на рисунку 1.1.

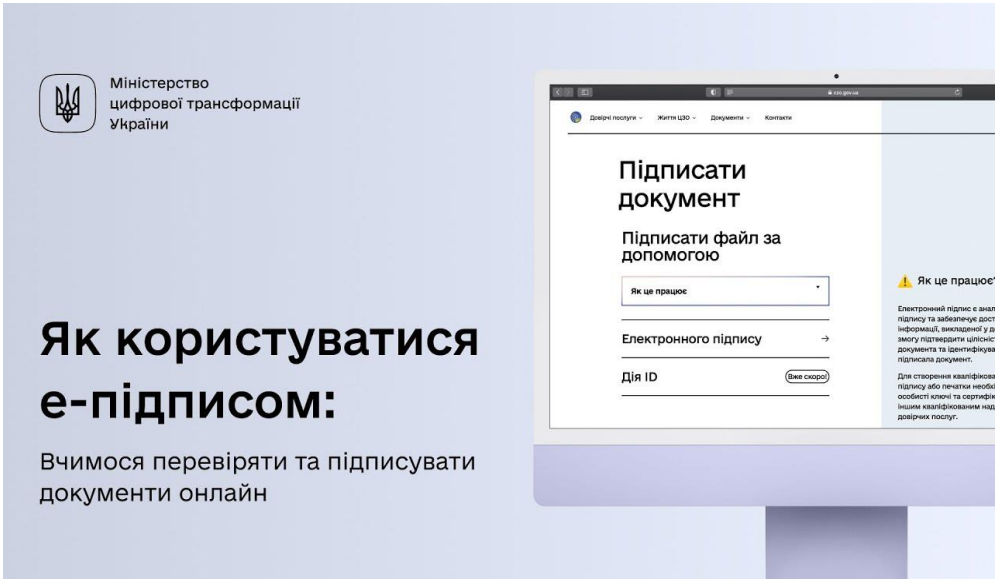


Рисунок 1.1 – Використання електронного підпису в системі "Дія"

1.1.1 Сутність цифрового підпису і його функції в інформаційній безпеці

Цифровий підпис представляє собою криптографічний механізм, що генерує унікальний математичний код для кожного документа на основі його змісту та приватного ключа підписувача. Основними функціями цифрового підпису в системі інформаційної безпеки є автентифікація відправника, забезпечення цілісності даних, гарантія незаперечності авторства та захист від несанкціонованих змін. Цифровий підпис працює як односторонній математичний алгоритм, який дозволяє будь-якому користувачу з відкритим ключем перевірити автентичність підпису, але унеможливлює його підробку без доступу до приватного ключа, що робить його надійним інструментом забезпечення довіри у цифрових комунікаціях.

1.1.2 Механізми ідентифікації особи

Електронний підпис функціонує як цифровий відбиток особи, використовуючи унікальну комбінацію криптографічних ключів для встановлення особи підписувача. Процес ідентифікації базується на математичному зв'язку між приватним ключем власника та його цифровим сертифікатом, що дозволяє з високою точністю підтвердити автентичність відправника без можливості підміни або фальсифікації.

1.1.3 Забезпечення незмінності даних

Криптографічний хеш-алгоритм електронного підпису створює унікальний цифровий відбиток документа, який змінюється навіть при найменших модифікаціях тексту. Ця властивість забезпечує миттєве виявлення будь-яких спроб несанкціонованого редагування або пошкодження інформації, гарантуючи повну цілісність даних протягом усього життєвого циклу документа.

1.1.4 Гарантії авторства та відповідальності

Принцип незаперечності електронного підпису створює юридично обов'язковий зв'язок між підписувачем та підписаним документом. Математична природа

криптографічного підпису унеможливлює відмову від авторства, оскільки створити дійсний підпис можливо лише за наявності приватного ключа, що знаходиться виключно у володільця, забезпечуючи таким чином правову відповідальність за цифрові дії.

1.1.5 Захист інформації від несанкціонованого доступу

Електронний підпис у поєднанні з технологіями шифрування створює багаторівневу систему захисту інформації. Хоча сам підпис первинно забезпечує автентифікацію та цілісність, його інтеграція з криптографічними протоколами дозволяє контролювати доступ до конфіденційних даних, створюючи комплексний бар'єр проти несанкціонованого втручання та кіберзагроз [3].

1.1.6 Сфери практичного застосування цифрових підписів

Електронний підпис знайшов широке застосування у ключових секторах цифрової економіки, де критично важливими є безпека та довіра між учасниками взаємодії. У сфері електронної комерції цифрові підписи забезпечують автентифікацію онлайн-угод, підтвердження електронних платежів та юридичну силу віртуальних контрактів між покупцями та продавцями. Системи електронного документообігу використовують цифрові підписи для верифікації службових документів, захищеної електронної кореспонденції та автентифікації звітної документації в корпоративному середовищі.

Особливо критичну роль електронний підпис відіграє у фінансовому секторі, де він забезпечує безпеку інтернет-банкінгу, автентифікацію електронних переказів та підтвердження фінансових транзакцій, як демонструє рисунок 1.2. У сфері державного управління цифрові підписи стали основою електронного урядування, забезпечуючи безпеку подання електронних декларацій, верифікацію державних документів та автентифікацію електронних дозволів і ліцензій, що значно підвищує ефективність взаємодії громадян з державними органами.

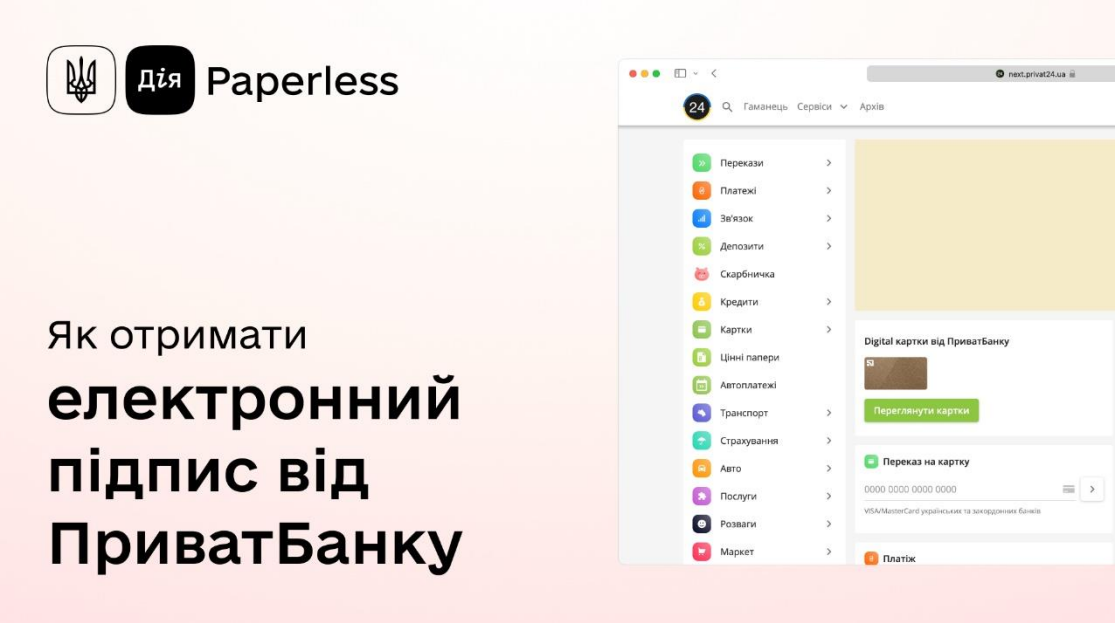


Рисунок 1.2 – Застосування електронного підпису в інтернет банкінгу

1.1.7 Проблемні аспекти функціонування електронного підпису в умовах квантових загроз

Розвиток квантових обчислювальних технологій створює фундаментальну загрозу для існуючих систем електронного підпису, оскільки квантові алгоритми, зокрема алгоритм Шора, здатні ефективно розкладати великі числа на прості множники, що лежить в основі безпеки сучасних криптографічних систем RSA та ECC. Ця квантова перевага робить традиційні методи асиметричної криптографії вразливими до компрометації, що вимагає термінової розробки постквантових криптографічних рішень для збереження довіри до електронних підписів у майбутньому [4].

1.2 Дослідження сучасних технологій електронного підпису та їх слабкі місця у контексті квантових обчислень

У контексті постквантових обчислень традиційні методи електронного підпису, що ґрунтуються на симетричних або асиметричних криптографічних алгоритмах, стають уразливими до квантових атак. Найпоширеніші методи електронного підпису та їхні обмеження в умовах постквантового періоду описано нижче.

1.2.1 Вивчення криптосистеми RSA та її характеристик

Криптосистема RSA, розроблена Рівестом, Шаміром та Адлеманом у 1977 році, залишається одним із найфундаментальніших та найширше застосовуваних алгоритмів асиметричної криптографії у сфері електронного підпису. Безпека RSA базується на математичній складності факторизації добутку двох великих простих чисел, що при використанні ключів достатньої довжини робить практично неможливим розкриття приватного ключа класичними обчислювальними методами навіть при використанні найпотужніших сучасних комп'ютерів. Приклад роботи даного алгоритму зображено на рисунку 1.3 [4].

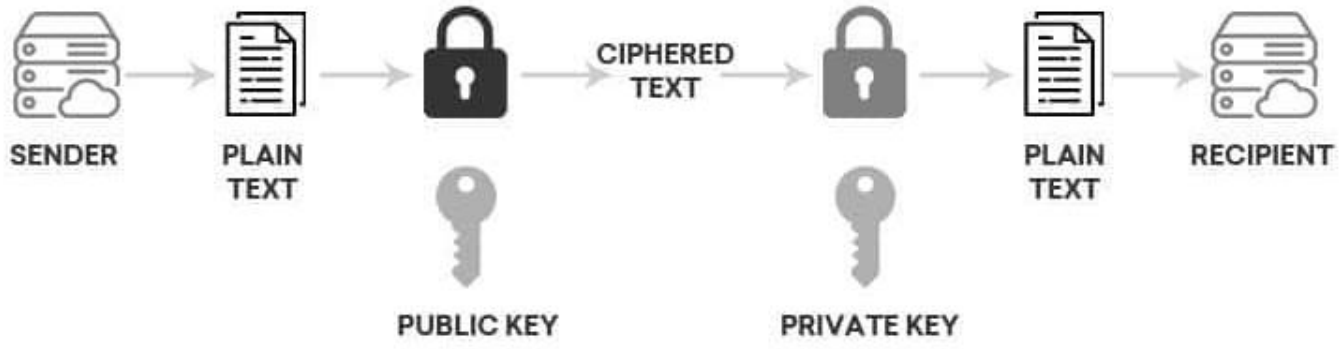


Рисунок 1.3 – Робота алгоритму RSA

Однак поява квантових обчислювальних технологій кардинально змінює рівень безпеки RSA-криптосистем. Алгоритм Шора, розроблений для квантових комп'ютерів, демонструє експоненційне прискорення процесу факторизації великих цілих чисел, скорочуючи час розкриття RSA-ключів з експоненційного до поліноміального. Це означає, що навіть RSA-ключі довжиною 4096 біт, які вважаються безпечними для класичних комп'ютерів протягом десятиліть, можуть бути скомпрометовані квантовими системами за лічені години або дні.

1.2.2 Дослідження алгоритму цифрового підпису DSA

Алгоритм DSA представляє собою асиметричний метод створення електронних підписів, який широко застосовується у різноманітних криптографічних системах та стандартах безпеки. Уязвимість цього алгоритму до атак з використанням квантових обчислень пов'язана з його фундаментальною основою - задачею дискретного логарифмування, яка може бути ефективно розв'язана за допомогою алгоритму Шора. Принцип функціонування алгоритму DSA детально проілюстровано на рисунку 1.4.

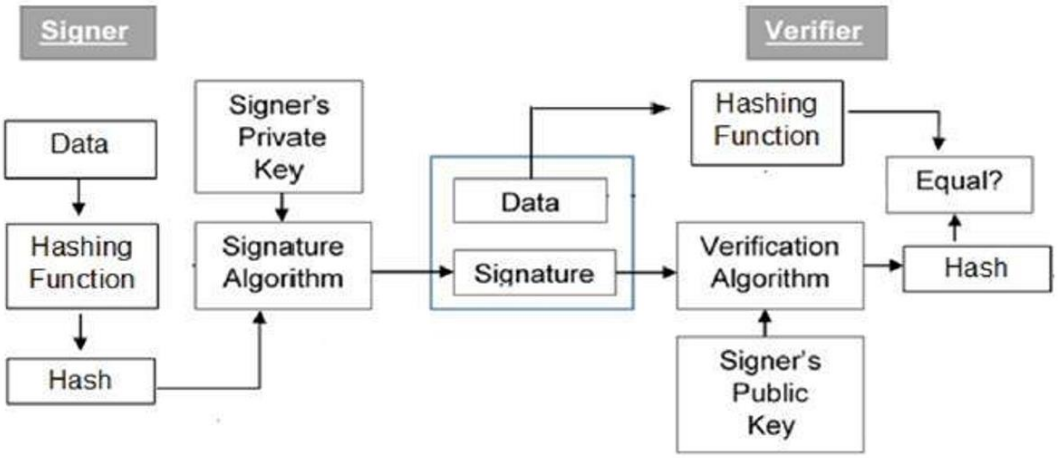


Рисунок 1.4 – Структурна діаграма функціонування алгоритму DSA [5]

1.2.3 Аналіз підписів на еліптичних кривих ECDSA

Криптографічна схема ECDSA являє собою асиметричний алгоритм генерації цифрових підписів, що ґрунтується на математичних операціях над еліптичними кривими. Незважаючи на те, що цей алгоритм демонструє підвищену стійкість проти квантових загроз у порівнянні з традиційними RSA та DSA, він все ж залишається вразливим до атак з використанням квантових обчислювальних методів, зокрема модифікованого алгоритму Шора, адаптованого для розв'язання задачі дискретного логарифма на еліптичних кривих [6]. Архітектура та послідовність виконання операцій алгоритму ECDSA у вигляді структурної схеми, що ілюструє основні етапи процесу створення та верифікації цифрового підпису зображено на рисунку 1.5.

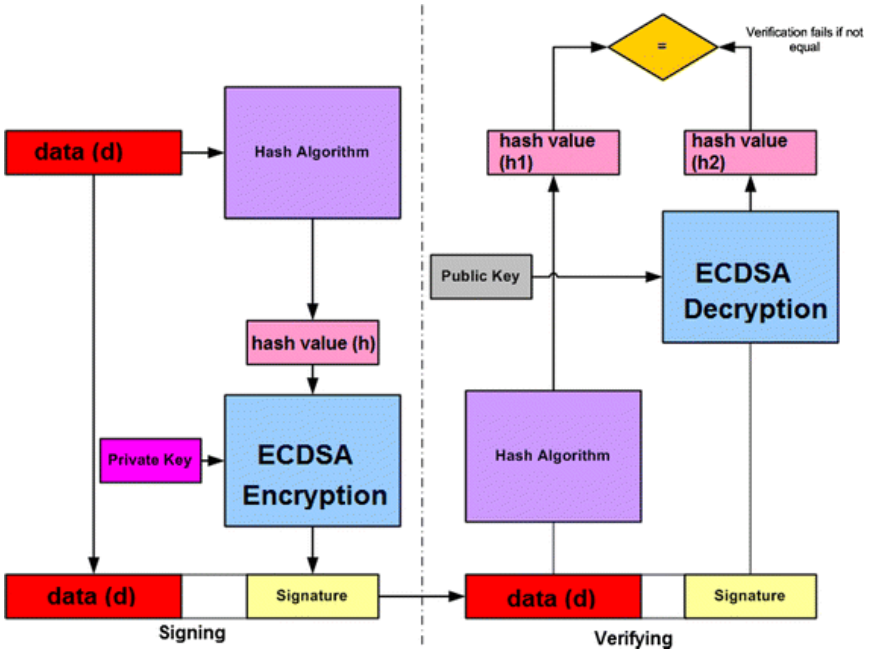


Рисунок 1.5 – Блок-схема роботи алгоритму ECDSA [6]

1.2.4 Оцінка вразливостей класичних методів підпису перед квантовими атаками

Класичні методи електронного підпису ґрунтуються на складних математичних задачах, таких як факторизація великих чисел або обчислення дискретного логарифма. Хоча ці задачі є практично нерозв'язними для класичних комп'ютерів, квантові алгоритми, зокрема алгоритм Шора, дозволяють вирішувати їх значно швидше. Це створює серйозну загрозу для безпеки традиційних криптографічних схем у постквантову епоху [7].

У зв'язку з цим зростає актуальність розробки нових, квантово-стійких методів електронного підпису. Одним із перспективних напрямів є впровадження підписів на основі одноразових ключів, які демонструють високий рівень захищеності від квантових атак. Вивчення таких методів та їх ефективне застосування у нових умовах є однією з ключових задач цієї дипломної роботи.

З появою квантових обчислень виникають принципово нові ризики для існуючих криптографічних механізмів. Квантові комп'ютери можуть отримати значні переваги в зламі класичних криптографічних протоколів, включаючи схеми

електронного підпису, що базуються на публічному ключі. У цьому розділі буде розглянуто обмеження традиційних методів підпису у контексті їхньої вразливості до квантових обчислень.

Вразливість традиційних методів електронного підпису до квантових атак.

Сучасні схеми цифрового підпису, такі як RSA, DSA та ECDSA, покладаються на складність певних математичних задач. Проте квантові алгоритми здатні розв’язувати ці задачі з високою ефективністю. Зокрема, **алгоритм Шора**, розроблений Пітером Шором, дозволяє ефективно виконувати факторизацію та обчислення дискретного логарифма — два ключові завдання, на яких побудовано багато криптографічних протоколів.

Це означає, що за наявності достатньо потужного квантового комп’ютера можливе швидке отримання приватного ключа з публічного, що фактично нівелює безпеку підпису.

Основні загрози, пов’язані з квантовими технологіями.

З'явлення квантових комп'ютерів викликає наступні ризики та проблеми для стандартних криптографічних методів:

1) Компрометація схем з публічним ключем — квантові комп’ютери здатні зламати схеми, в основі яких лежить складність факторизації або дискретного логарифма, що підриває довіру до більшості нині використовуваних електронних підписів.
2) Уразливість хеш-функцій — інший важливий аспект полягає в зниженні стійкості хеш-функцій, які можуть бути атаковані за допомогою алгоритму Ґровера, що дозволяє швидше знаходити колізії, підриваючи цілісність даних підпису.

Необхідність переходу до квантово-стійких рішень.

Для збереження довіри до електронних підписів у майбутньому необхідно впроваджувати постквантові криптографічні рішення. Це можуть бути:

— алгоритми, що не базуються на проблемах, які легко вирішуються квантовими комп’ютерами;
— методи з використанням решіток, кодів, багаточленів або хеш-функцій нового покоління;
— технології, що передбачають квантове розповсюдження ключів або навіть квантові цифрові підписи.

Важливість попередньої адаптації до постквантової епохи.

У світлі активного розвитку квантових технологій надзвичайно важливо вже зараз почати адаптацію наявних систем:

— проводити аудит стійкості до квантових загроз;
— тестувати та впроваджувати квантово-стійкі алгоритми;
— розробляти стратегії поступової міграції до нових рішень.

Розуміння обмежень традиційних методів електронного підпису та своєчасна підготовка до постквантового періоду мають ключове значення для гарантування безпеки цифрових транзакцій, захисту персональних даних та відповідності регуляторним нормам.

1.3 Вивчення фундаментальних законів квантової фізики

Традиційні комп'ютерні системи оперують бітами, що мають дискретні значення 0 або 1. Квантові обчислювальні машини застосовують кубіти (квантові біти), здатні існувати в стані суперпозиції — одночасному поєднанні різних станів, що являють собою лінійні комбінації 0 та 1. Завдяки цій особливості квантові комп'ютери можуть обробляти набагато більші масиви даних паралельно та здійснювати розрахунки з вищою швидкістю порівняно з класичними машинами [7].

1.3.1 Дослідження принципу невизначеності у квантових системах

Співвідношення невизначеностей Гейзенберга становить основоположний постулат квантової теорії. Цей принцип встановлює неможливість одночасного прецизійного визначення координати та імпульсу мікрочастинки. Іншими словами,

підвищення точності вимірювання однієї фізичної величини неминуче збільшує похибку визначення іншої. Дане положення відіграє ключову роль у квантовій криптографії, де вимірювання квантових станів застосовується для гарантування інформаційної безпеки.

1.3.2 Аналіз квантової суперпозиції та її властивостей

Квантова механіка допускає існування квантових станів у суперпозиції, тобто у формі лінійної суми кількох альтернативних станів. При взаємодії квантові системи здатні модифікувати характеристики одна одної, трансформуючи власні стани та кореляції між ними.

Ця особливість є фундаментом для створення квантових алгоритмів та протоколів, що експлуатують явища суперпозиції та квантових взаємодій для здійснення обчислень та гарантування захисту інформації [8].

1.3.4 Вивчення феномену квантової заплутаності та кореляцій

Квантова суперпозиція характеризується здатністю квантових об'єктів одночасно перебувати в множині станів з відповідними ймовірностями реалізації. Квантова заплутаність демонструє нерозривні кореляції між квантовими системами, за яких модифікація параметрів однієї частинки миттєво відображається на станах інших частинок, незалежно від просторової відстані між ними. Ці квантові ефекти становлять основу для розробки криптографічних систем та протоколів цифрового підпису з використанням одноразових ключів.

Розкриття сутності зазначених базових концепцій та законів квантової теорії є необхідною умовою для осмислення механізмів функціонування квантових алгоритмів та оцінки їх впливу на існуючі технології електронного підпису.

1.4 Дослідження квантових обчислювальних алгоритмів, що становлять загрозу для традиційної криптографії

Аналіз квантових алгоритмів, включаючи алгоритм Шора та алгоритм Гровера, демонструє серйозні ризики для існуючих криптографічних конструкцій. Це

зумовлює актуальність створення інноваційних підходів та технологій цифрового підпису, спроможних чинити опір квантовим атакам та гарантувати захист інформації в постквантову епоху.

1.4.1 Аналіз алгоритму факторизації Шора

Алгоритм Шора належить до найбільш визнаних та ефективних квантових алгоритмів. Його призначення полягає у розкладанні чисел на прості множники та компрометації криптографічних схем, заснованих на задачі факторизації, зокрема системи RSA. Класичні методи факторизації характеризуються експоненційною обчислювальною складністю, тоді як алгоритм Шора здатен виконувати розклад за поліноміальний час на квантовому обчислювальному пристрої [8]. Це свідчить про те, що алгоритм Шора може кардинально підірвати криптографічну міцність систем, що ґрунтуються на проблемі факторизації великих чисел. Приклад функціонування представлено на рисунку 1.6

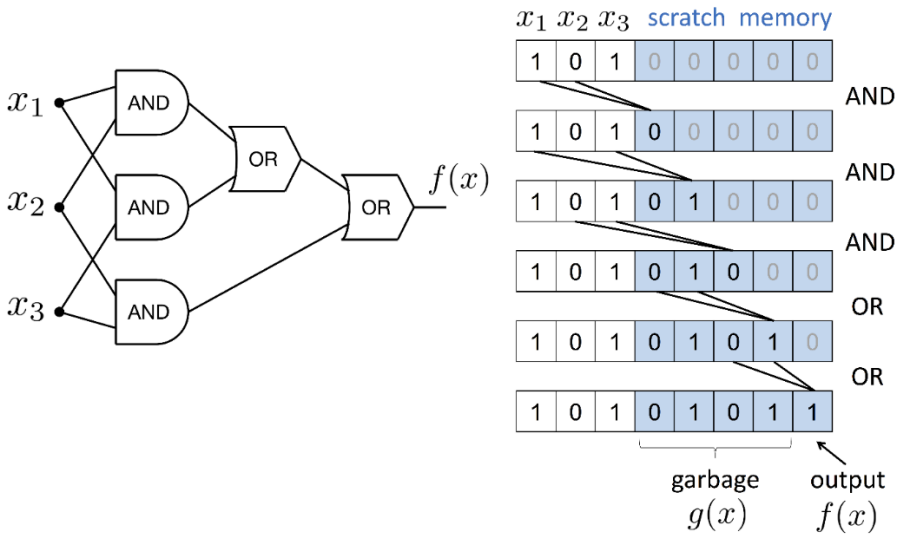


Рисунок 1.6 – Робота алгоритму ШОРА [7]

Квантовий алгоритм Шора для розв'язання задачі дискретного логарифмування у групі точок еліптичних кривих за обчислювальною складністю практично ідентичний алгоритму Шора для дискретного логарифмування у скінченних полях [7].

Алгоритм Шора характеризується однотипними етапами виконання, різниця полягає лише у способі представлення: замість елементів поля необхідно розглядати точки еліптичної кривої. Проаналізуємо їх криптографічну стійкість та здійснимо відповідні кількісні оцінки.

На сьогодні вважається, що найефективніше розв'язання задач дискретного логарифмування у групі точок еліптичних кривих досягається застосуванням ρ- та λ-методів Полларда [7]. Їх обчислювальна складність може бути оцінена наступним чином:

$$O(\sqrt{q}), \tag{1.1}$$

де q - число точок еліптичної кривої.

Встановлено, що квантовий алгоритм Шора в загальному випадку характеризується поліноміальною складністю для розв'язання цього класу задач. Він також придатний для вирішення рівняння дискретного логарифма, при цьому його часова складність оцінюється як $O(n^3)$ за умови використання O(n) кубітів, де n представляє порядок базової точки [7]. Певні оцінки та результати компаративного аналізу класичних алгоритмів порівняно з квантовим алгоритмом Шора розглядатимуться у наступних підрозділах даного розділу.

1.4.2 Аналіз алгоритму пошуку Гровера

Алгоритм Гровера представляє собою квантовий алгоритм пошуку, що забезпечує ефективне виявлення цільових даних у неструктурованих масивах інформації. Він забезпечує квадратичне збільшення швидкості у порівнянні з традиційними алгоритмами пошуку. Це означає, що алгоритм Гровера можна застосовувати для прискореного криптоаналізу симетричних криптографічних конструкцій, зокрема шифрів Дойча та Гротендіка [9]. Він спроможний виявити конфіденційний ключ з меншою кількістю ітерацій у порівнянні з класичними підходами. Схема роботи представлена на рисунку 1.7.

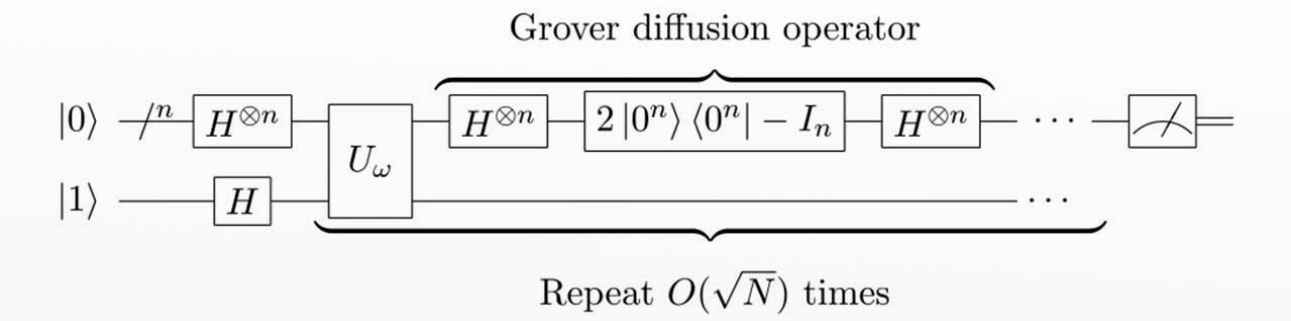


Рисунок 1.7 – Схема роботи алгоритму Гровера [8]

1.4.3 Оцінка впливу квантових обчислень на безпеку цифрових підписів

У постквантовому періоді з'являються нові виклики та загрози для електронного підпису, оскільки квантові комп'ютери можуть підірвати стійкість традиційних криптографічних методів. В цьому розділі розглянемо вплив квантових атак на електронний підпис та можливості забезпечення його стійкості в умовах квантових атак.

В постквантову епоху виникають нові виклики та ризики для технологій цифрового підпису, оскільки квантові обчислювальні системи здатні скомпрометувати міцність усталених криптографічних механізмів. У цьому розділі проаналізуємо вплив квантових атак на електронний підпис та можливості гарантування його стійкості за умов квантових загроз.

Вплив квантових атак на електронний підпис.

Квантові атаки чинять значний вплив на системи електронного підпису, особливо на криптографічні конструкції з відкритим ключем. Традиційні алгоритми, включаючи RSA, DSA та ECDSA, є уразливими до атак Шора, який спроможний швидко розкладати числа на множники і розкривати приватні ключі. Це означає, що цифрові підписи, засновані на таких системах, можуть бути скомпрометовані квантовими обчислювальними машинами [10].

Додатково, квантові комп'ютери можуть загрожувати стійкості геш-функцій, що застосовуються для формування електронних підписів. Вони здатні ефективно

виявляти колізії у геш-функціях, підриваючи їх надійність та криптографічну міцність.

Забезпечення стійкості електронного підпису в умовах квантових атак.

Для гарантування стійкості електронного підпису за умов квантових атак необхідно застосовувати квантово-резистентні методи та протоколи. Розглянемо основні напрямки забезпечення стійкості електронного підпису:

1) Застосування квантово-резистентних алгоритмів підпису: Нові криптографічні алгоритми, такі як решітковий підпис Лампорта, демонструють вищу стійкість до квантових атак і можуть використовуватися для створення захищених електронних підписів.
2) Впровадження квантових комунікаційних протоколів: Квантові комунікаційні протоколи, зокрема протокол BB84, можуть забезпечити безпечну передачу ключів і застосовуватися для формування стійких електронних підписів.
3) Використання квантових стеганографічних технік: Квантові стеганографічні підходи можуть сприяти забезпеченню конфіденційності електронного підпису та захисту його від квантових атак.
4) Створення квантово-резистентних стандартів: Необхідно активно працювати над розробкою та імплементацією квантово-стійких стандартів електронного підпису для забезпечення безпеки в постквантову епоху.
5) Систематичний моніторинг і наукові дослідження: Слід здійснювати постійний моніторинг розвитку квантових технологій та проводити дослідження у сфері квантової криптографії для оперативної адаптації до нових викликів і гарантування стійкості електронного підпису.

Враховуючи вплив квантових атак на електронний підпис, критично важливо підготуватися до постквантової епохи, застосовуючи інноваційні квантово-резистентні методи та розробляючи стратегії адаптації. Це дозволить гарантувати безпеку електронних транзакцій, зберегти конфіденційність інформації та запобігти

потенційним загрозам, пов'язаним з розвитком квантових обчислювальних технологій.

1.5 Дослідження квантових методів криптографічного захисту

Квантова криптографія представляє собою спеціалізований розділ сучасної криптографічної науки, що ґрунтується на фундаментальних законах квантової фізики для створення захищених каналів передачі секретної інформації. Даний напрямок виник як природна еволюція класичних криптографічних підходів із метою створення криптосистем, здатних протистояти загрозам майбутніх квантових обчислювальних технологій.

Фундаментальні концепції квантової криптографії базуються на таких поняттях:

1) Кубіти (квантові біти) служать базовими елементами квантової інформації, відрізняючись від звичайних бітів здатністю одночасно перебувати у декількох станах завдяки ефекту квантової суперпозиції, що дозволяє їм містити значення 0, 1 або їх комбінацію.
2) Співвідношення невизначеностей Гейзенберга встановлює принципову неможливість точного одночасного вимірювання певних пар квантових величин. Ця властивість створює природний захисний механізм, оскільки будь-які спроби несанкціонованого спостереження неминуче змінюють стан квантової системи.
3) Квантова заплутаність характеризує особливий тип зв'язку між квантовими об'єктами, при якому вплив на один елемент системи миттєво позначається на стані всіх інших пов'язanych елементів. Ця особливість дає змогу розробляти криптографічні схеми з гарантованою безперервністю зв'язку між учасниками.

Інтеграція квантової криптографії в архітектуру систем цифрового підпису відкриває такі можливості:

1) Квантовий розподіл ключів (QKD) являє собою інноваційний метод передачі криптографічних ключів на основі квантових станів матерії. Технологія QKD формує надійну криптографічну базу для цифрових підписів, демонструючи стійкість навіть до потужних квантових обчислювальних атак.
2) Постквантові алгоритми цифрового підпису охоплюють новітні криптографічні методи, спеціально створені для протидії квантовим загрозам. Ці алгоритми експлуатують унікальні властивості квантових систем - заплутаність та невизначеність - для гарантування криптографічної міцності електронних підписів.

Комплексний аналіз квантової криптографії розкриває основоположні принципи та концепції цієї передової криптографічної дисципліни. Впровадження квантових криптографічних рішень у системи електронного підпису обіцяє досягнення надвисокого рівня інформаційної безпеки та захисту від квантових кіберзагроз, що набуває стратегічного значення в епоху квантових технологій.

1.6 Перспективи розвитку квантової криптографії та технологій одноразових ключів

Перспективи впровадження квантових криптографічних технологій та одноразових ключів у майбутніх системах цифрового підпису демонструють значний потенціал трансформації сфери інформаційної безпеки. Ці інноваційні підходи відкривають нові горизонти захисту даних та автентифікації в умовах зростаючих кіберзагроз. Ось деякі перспективи цих технологій та їх потенційні переваги і виклики:

1) Імунітет до квантових кіберзагроз - фундаментальною перевагою квантової криптографії є її природна стійкість до атак з використанням квантових обчислювальних систем. На відміну від традиційних криптографічних схем, які можуть бути скомпрометовані потужними квантовими процесорами, квантові криптосистеми базуються на незмінних законах квантової фізики, що гарантує їх надійність.

2) Теоретично досконала безпека ключового обміну - застосування одноразових квантових ключів забезпечує абсолютну криптографічну стійкість процедур обміну секретною інформацією. Квантово-механічні принципи унеможливлюють копіювання або перехоплення квантових станів без їх порушення, що створює фізично гарантовану конфіденційність комунікацій.
3) Самодіагностика безпеки системи - квантові криптографічні протоколи володіють унікальною здатністю автоматичного виявлення спроб несанкціонованого доступу. Будь-які втручання в квантові канали зв'язку залишають детектовані сліди, що дозволяє учасникам комунікації оперативно реагувати на загрози та оновлювати компрометовані ключі.

Однак, впровадження квантової криптографії та використання одноразових ключів також стикається з деякими викликами:

1) Технологічна складність - створення функціональних квантових криптосистем потребує передових наукових розробок та високопрецизійного технологічного обладнання. Розробка стабільних квантових пристроїв представляє собою комплексне інженерне завдання, що вимагає міждисциплінарної експертизи та значних науково-технічних інвестицій.
2) Проблеми інтероперабельності - ефективне функціонування квантових криптографічних мереж потребує універсальної підтримки квантових протоколів усіма учасниками системи. Обмежена доступність квантового обладнання та відсутність стандартизованих рішень створюють бар'єри для масового впровадження цих технологій.
3) Економічні обмеження - високі витрати на науково-дослідні роботи, виробництво спеціалізованого обладнання та підтримку квантових інфраструктур становлять серйозну перешкоду для комерціалізації квантових криптографічних продуктів. Питання економічної доцільності залишається критичним фактором прийняття рішень про впровадження.

Попри існуючі технічні та економічні складнощі, траєкторія розвитку квантової криптографії демонструє позитивну динаміку. Прогресивні дослідження в галузі квантових технологій та зростаючі інвестиції в цей сектор створюють передумови для поступового подолання наявних обмежень. Еволюція квантових криптографічних систем може радикально переосмислити підходи до забезпечення кібербезпеки та встановити нові стандарти захисту цифрової інформації в постквантовому технологічному ландшафті.

1.7 Компаративний аналіз обчислювальної складності криптографічних алгоритмів

Проведення компаративного дослідження обчислювальної складності традиційних та квантових підходів до розв'язання задачі дискретного логарифмування в групах точок еліптичних кривих (ECC) є критично важливим для оцінки криптографічної стійкості сучасних систем. Це порівняння, представлене в таблиці 1.1.

Таблиця 1.1 - Порівняльний аналіз складності класичного і квантового алгоритмів дискретного логарифмування групі точок еліптичної кривої (ECC)

Алгоритм розв’язку дискретного логарифмічного рівняння			
Розмір порядку базової точки, бітів	Кількість необхідних кубітів $f(n) = 7n + 4log_2$ n + 10	Складність квантового алгоритму $360\ n^3$	Складність класичного алгоритму
163	1210	$1.6 \cdot 10^9$	$3.4 \cdot 10^{24}$
256	1834	$6 \cdot 10^9$	$3.4 \cdot 10^{38}$
571	4016	$6.7 \cdot 10^{10}$	$8.8 \cdot 10^{85}$
1024	7218	$3.8 \cdot 10^{11}$	$1.3 \cdot 10^{154}$

Задача дискретного логарифмування на еліптичних кривих полягає у визначенні цілого числа k, для якого виконується рівність kP = Q, де P - базова точка групи, Q - цільова точка, а k - шуканий дискретний логарифм. Цей математичний виклик становить основу криптографічної стійкості багатьох сучасних систем цифрового підпису, що базуються на криптографії еліптичних кривих.

Представлені в таблиці результати демонструють кардинальну різницю в обчислювальних вимогах між традиційними та квантовими підходами до розв'язання цієї фундаментальної криптографічної задачі.

Аналіз обчислювальної ефективності за розмірами ключів:

Для 163-бітного порядку групи спостерігається вражаюча диспропорція: квантовий підхід з використанням 1210 кубітів досягає складності 1.6×10^{9} операцій, тоді як класичні методи потребують астрономічних 3.4×10^{24} обчислень - різниця в 15 порядків величини.

При збільшенні до 256 бітів розрив стає ще більш драматичним. Квантова реалізація з 1834 кубітами вимагає лише 6×10^{9} операцій проти неосяжних 3.4×10^{38} класичних обчислень - перевага в 29 порядків величини.

Для 571-бітних систем квантовий алгоритм з 4016 кубітами потребує 6.7×10^{10} операцій, в той час як класичний підхід досягає колосальної складності 8.8×10^{85} - різниця в 75 порядків.

Найбільш вражаючі результати спостерігаються для 1024-бітних ключів: квантова система з 7218 кубітами виконує завдання за 3.8×10^{11} операцій, тоді як класичні алгоритми стикаються з практично нескінченною складністю 1.3×10^{154} операцій.

Криптографічні наслідки та перспективи:

Ці дані підтверджують фундаментальну загрозу, яку квантові обчислення становлять для існуючих ECC-систем. Експоненційне прискорення квантових алгоритмів означає, що криптографічні схеми, які сьогодні вважаються практично

неламними, можуть бути скомпрометовані за розумний час при наявності достатньо потужних квантових процесорів.

Водночас важливо зауважити, що наведені результати відображають теоретичну складність алгоритмів. Практична реалізація квантових систем з тисячами стабільних кубітів залишається значним технологічним викликом. Сучасні квантові комп'ютери ще не досягли необхідної кількості логічних кубітів та рівня стабільності для практичного виконання таких обчислень.

Ці дослідження мають критичне значення для розуміння темпоральних рамок переходу до постквантової криптографії та обґрунтування необхідності розробки квантово-стійких криптографічних протоколів для майбутніх систем електронного підпису.

1.8 Висновки по розділу

У представленому розділі здійснено комплексне дослідження фундаментальних аспектів цифрового підпису та квантових обчислювальних технологій. Проаналізовано сутність електронного підпису як ключового інструменту забезпечення інформаційної безпеки, що гарантує автентичність відправника, незмінність переданих даних, незаперечність авторства та конфіденційність комунікацій. Особливу увагу приділено практичному застосуванню цифрових підписів та потенційним загрозам, що можуть виникнути з появою квантових обчислювальних систем.

Проведено критичний аналіз сучасних криптографічних стандартів електронного підпису, включаючи алгоритми RSA, DSA та ECDSA, з акцентом на їх вразливості в умовах квантових кіберзагроз. Дослідження продемонструвало, що класичні криптографічні протоколи можуть втратити свою ефективність під впливом потужних квантових алгоритмів.

Детально розкрито ключові концепції квантової фізики, що лежать в основі квантових обчислень: співвідношення невизначеностей Гейзенберга, квантову суперпозицію станів, принципи взаємодії квантових систем та феномен квантової

заплутаності. Ці фундаментальні поняття є критично важливими для розуміння механізмів, через які квантові технології можуть загрожувати існуючим криптографічним архітектурам.

Проаналізовано провідні квантові алгоритми, насамперед алгоритм Шора для факторизації великих чисел та алгоритм Гровера для пошуку в неструктурованих базах даних, які демонструють експоненційне прискорення порівняно з класичними обчислювальними методами. Ці алгоритмічні прориви підкреслюють неминучість трансформації криптографічного ландшафту в постквантову епоху.

Результати дослідження формують цілісне розуміння концептуальних основ електронного підпису, принципів квантової механіки та квантових алгоритмів, виявляючи стратегічні виклики для існуючих методів цифрового підпису в контексті майбутнього квантового технологічного середовища. Це дослідження створює теоретичний фундамент для подальшої розробки квантово-стійких криптографічних рішень.

2 ВИВЧЕННЯ ТЕХНОЛОГІЙ ОДНОРАЗОВОГО ШИФРУВАННЯ ТА КОНЦЕПЦІЙ КРИПТОГРАФІЇ МАЙБУТНЬОГО

2.1 Одноразові криптографічні ключі та їх застосування

У сфері криптографічної безпеки одноразові ключі представляють унікальний підхід до захисту інформації, характеризуючись принципом однократного використання для кожної окремої операції шифрування або дешифрування повідомлень. Ця концепція кардинально відрізняється від традиційних криптографічних схем, де один ключ може використовуватися багаторазово.

Фундаментальні характеристики одноразових ключів:

1) Криптографічна секретність передбачає, що кожен ключ має генеруватися за допомогою справжньо випадкових процесів та залишатися абсолютно недоступним для потенційних порушників. Якість випадковості ключового матеріалу є критичним фактором забезпечення криптографічної стійкості системи.
2) Принцип одноразовості встановлює жорстке правило використання кожного ключа виключно для однієї криптографічної операції або обробки одного повідомлення. Після використання ключ повністю знищується, що унеможливлює його повторне застосування.
3) Криптографічна довжина має бути достатньою для протистояння найсучаснішим атакам брутфорс та іншим методам криптоаналізу. Адекватна довжина ключа є основою для забезпечення неможливості його відновлення або компрометації.

Переваги та обмеження одноразових ключових систем:

1) Головною перевагою одноразових ключів є їх природна імунність до квантових криптоаналітичних атак. На відміну від класичних криптосистем, які можуть бути скомпрометовані алгоритмом Шора та іншими квантовими

методами, одноразові ключі зберігають свою криптографічну міцність навіть у постквантовому середовищі.

2) Водночас практична реалізація систем на основі одноразових ключів стикається з серйозними логістичними викликами. Проблема безпечного розподілу ключів між учасниками комунікації потребує надійних каналів передачі, що самі по собі мають бути криптографічно захищеними. Крім того, необхідність зберігання великих обсягів ключового матеріалу створює додаткові ризики безпеки та вимагає значних ресурсів для забезпечення фізичної та логічної безпеки сховищ ключів.
3) Масштабування систем одноразових ключів для корпоративного або масового використання також представляє значні технічні та економічні труднощі, пов'язані з необхідністю генерації, зберігання та синхронізації величезних кількостей унікальних ключів між множинними учасниками мережі.

2.2 Дослідження принципів одноразового шифрування у криптографічних системах

Криптографічна концепція одноразових ключів представляє фундаментальний підхід до забезпечення максимальної безпеки інформаційного обміну, базуючись на принципі унікальності кожного ключового елемента. Сутність цієї методології полягає у створенні індивідуального криптографічного ключа для кожної окремої операції з подальшою його повною ліквідацією після використання.

Методи генерації одноразових ключів:

Створення високоякісних одноразових ключів може здійснюватися через різноманітні технологічні підходи. Псевдовипадкова генерація базується на математичних алгоритмах, що продукують статистично випадкові послідовності бітів. Більш надійним є використання справжніх джерел ентропії - фізичних процесів, таких як електронний шум, радіоактивний розпад або квантові флуктуації, які забезпечують автентичну випадковість ключового матеріалу.

Критично важливою характеристикою є достатня довжина ключа, що має перевищувати можливості сучасних обчислювальних систем щодо криптоаналітичного злому через повний перебір або застосування спеціалізованих алгоритмів криптоаналізу.

Сфери застосування одноразових ключів:

У симетричній криптографії одноразові ключі забезпечують досконалу секретність комунікацій між авторизованими учасниками. Кожне повідомлення шифрується унікальним ключем, що робить криптоаналітичні атаки практично неможливими навіть при перехопленні великої кількості зашифрованих текстів.

Асиметричні криптосистеми можуть інтегрувати одноразові ключі для посилення безпеки процедур обміну сесійними ключами або створення тимчасових криптографічних параметрів для специфічних операцій.

У контексті цифрового підпису одноразові ключі можуть застосовуватися для генерації криптографічних підписів, що гарантують автентифікацію відправника та незаперечність авторства документів. Такий підхід особливо ефективний у системах, де кожна транзакція або документ потребує індивідуального криптографічного засвідчення.

Квантова стійкість одноразових ключів:

Особливою перевагою одноразових ключів є їх природна резистентність до квантових криптоаналітичних загроз. Традиційні квантові алгоритми, такі як алгоритм Шора, експлуатують математичні властивості багаторазово використовуваних ключів та специфічні структури криптографічних протоколів.

Одноразові ключі позбавлені цих вразливостей завдяки своїй фундаментальній властивості - відсутності повторного використання. Квантові атаки зазвичай потребують накопичення криптографічної інформації або використання математичних закономірностей, які проявляються при багаторазовому застосуванні ключів. Одноразовість унеможливлює такі аналітичні підходи, створюючи криптографічну систему, стійку до квантових обчислювальних методів.

Ця властивість робить одноразові ключі особливо цінними для критично важливих застосувань, де необхідно забезпечити довгострокову безпеку інформації навіть у постквантовому технологічному середовищі.

2.3 Аналіз існуючих протоколів квантового розподілу ключів, зокрема схеми BB84

Схема Беннетта-Брассарда (BB84) представляє собою один з найбільш відомих алгоритмів квантової криптографії, що базується на застосуванні одноразових криптографічних ключів. Даний алгоритм був представлений у 1984 році вченими Чарльзом Беннеттом та Жілем Брассардом і визнається першим алгоритмом у сфері квантової криптографії.

Схема BB84 базується на особливостях квантових бітів (кубітів), зокрема на поляризаційних характеристиках фотонів, для здійснення обміну ключами між двома учасниками комунікації.

Алгоритм реалізується через такі етапи:

1) Створення та довільний відбір серії кубітів, що передаються від відправника до одержувача;
2) Довільне визначення базисів для вимірювання кубітів, переданих відправником. Базиси можуть представляти лінійну або діагональну поляризацію світлових частинок;
3) Здійснення вимірювань кубітів одержувачем у обраних базисах;
4) Публічний обмін даними про застосовані базиси між відправником та одержувачем;
5) Зіставлення базисів, які використовувалися відправником і одержувачем. При збігу базисів, біти, що відповідають узгодженим кубітам, можуть служити компонентами одноразового ключа.

Схема BB84 гарантує секретність ключових даних та можливість виявлення спроб несанкціонованого доступу. Коли ключові дані, одержані відправником та одержувачем, є ідентичними, це підтверджує відсутність перехоплення або

модифікацій у каналі передачі інформації. При виявленні розбіжностей у ключових даних можна констатувати, що канал передачі не є захищеним або зазнав несанкціонованого втручання [13].

Схема BB84 служить прикладом застосування одноразових ключів у квантовій криптографії. Її вивчення сприяє розумінню механізмів обміну ключовими даними та методів забезпечення захисту в квантових комунікаціях на основі одноразових ключів. Демонстрація функціонування цього алгоритму представлена на рисунку 2.1.

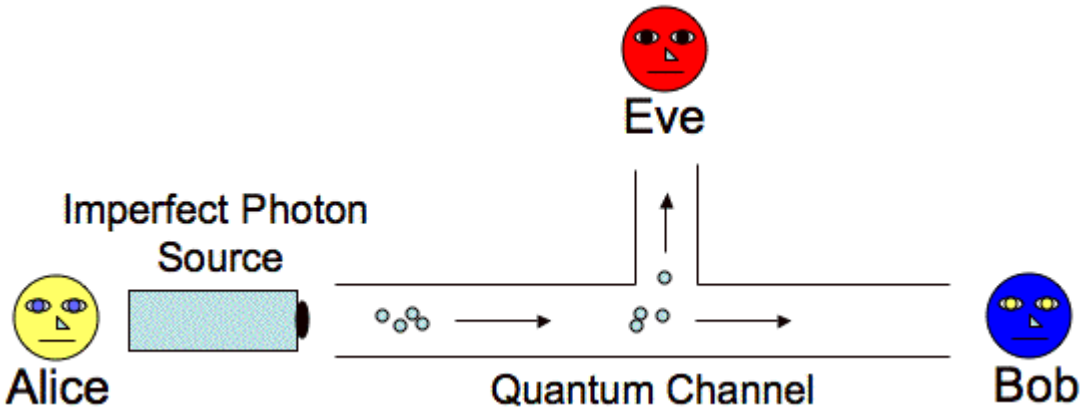


Рисунок 2.1 – Приклад роботи протоколу BB84 [14]

2.4 Криптографічні технології постквантового періоду

Постквантова криптографія являє собою спеціалізовану сферу криптографічних досліджень, що зосереджена на створенні алгоритмів та схем, здатних протистояти загрозам від квантових обчислювальних систем. З огляду на те, що квантові обчислювальні машини здатні зламати існуючі криптографічні стандарти, постквантова криптографія набуває критичного значення для гарантування інформаційної безпеки у перспективі.

Основне завдання постквантової криптографії полягає у створенні криптографічних схем, які зберігатимуть свою надійність навіть за умови функціонування високопродуктивних квантових обчислювальних пристроїв. Для реалізації цього завдання застосовуються наступні стратегії:

1) Квантова криптографія: Застосування особливостей квантово-механічних систем для побудови захищених криптографічних схем. Ілюстрацією може служити схема Беннетта-Брассарда (BB84), описана у попередньому розділі;
2) Кодування і декодування на квантових обчислювальних системах: Створення квантових кодів, здатних гарантувати секретність та стійкість проти квантових загроз;
3) Квантово-резистентні криптографічні основи: Створення інноваційних криптографічних схем та алгоритмів, які зберігають стійкість навіть під час атак із застосуванням квантових обчислень.

Постквантова криптографія застосовується для охорони різноманітних криптографічних механізмів, зокрема цифрового підпису, шифрування даних та верифікації особи, від загроз з боку квантових обчислювальних машин. Даний розділ досліджує та аналізує різноманітні стратегії та техніки постквантової криптографії, а також їх використання у контексті створення методів цифрового підпису на базі одноразових ключів для постквантової епохи [14].

2.5 Основи та фундаментальні концепції криптографії майбутнього

У цьому пункті розглянуто фундаментальні принципи постквантової криптографії та ключові ідеї, що становлять основу даної наукової сфери. Постквантова криптографія розвивається як реакція на ризики, які створюють високопродуктивні квантові обчислювальні системи для існуючих методів криптографічного захисту.

Ключові принципи постквантової криптографії охоплюють:

1) Квантова резистентність: Це характеристика криптографічних схем і алгоритмів, які зберігають надійність навіть у присутності квантових загроз. Одним з пріоритетних завдань постквантової криптографії є створення криптографічних технік, що підтримують стійкість проти атак із застосуванням квантових обчислювальних машин;

2) Квантове узгодження ключів: Це механізм передачі квантових станів між учасниками комунікації для встановлення загального таємного ключа. Квантове узгодження ключів експлуатує характеристики квантових систем, зокрема принцип невизначеності та явище заплутаності, для гарантування захищеності процесу обміну ключовою інформацією;
3) Квантові схеми зв'язку: Це алгоритми комунікації, що використовують квантові системи для забезпечення захисту та приватності. Квантові схеми зв'язку можуть охоплювати квантове узгодження ключів, квантове кодування та інші процедури, що гарантують безпечність передачі інформації;
4) Квантова теорія інформації: Це напрям квантової фізики, що вивчає характеристики та процеси обробки квантових даних. Квантова теорія інформації застосовується для побудови схем квантової криптографії та визначення границь надійності квантових систем [15].

Базова концепція представлена на рисунку 2.2.

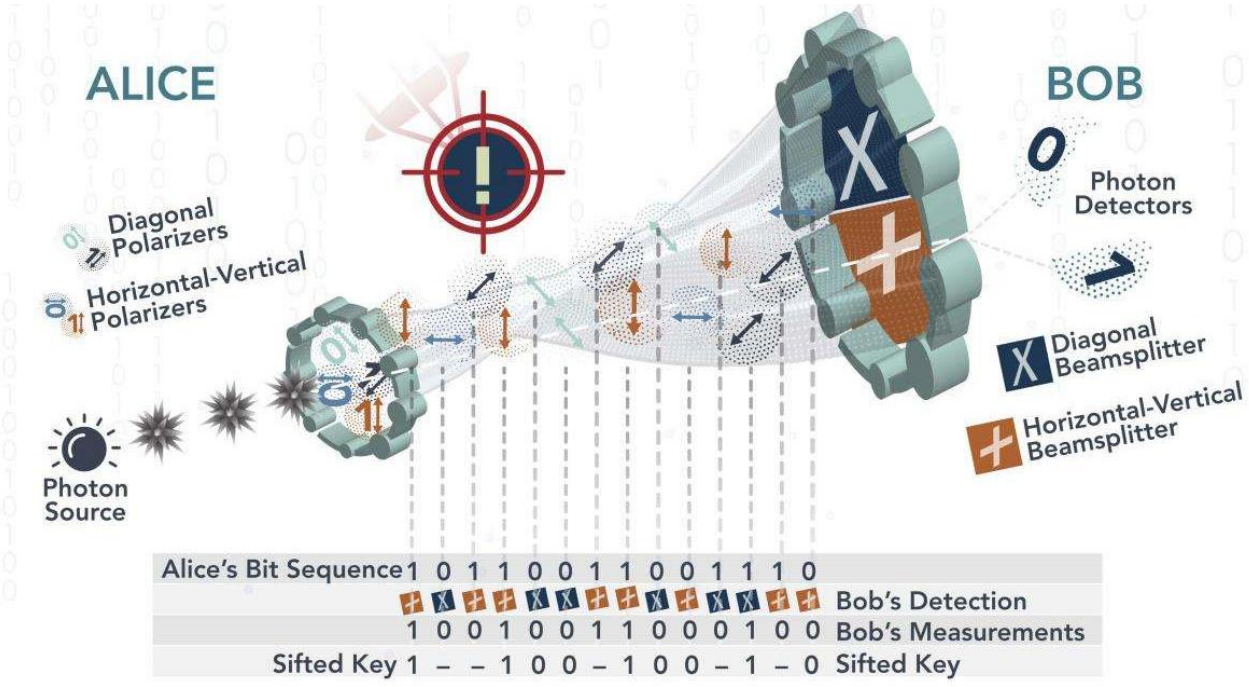


Рисунок 2.2 – Концепція шифрування в постквантовій криптографії [15]

2.6 Дослідження сучасних підходів до створення квантово-стійких криптосистем, включаючи рішення на базі одноразових ключів

Протягом останнього десятиліття дослідження в сфері квантової криптографії та створення криптографічних механізмів, стійких до квантових атак, привернули значну увагу наукової спільноти. Одним із методів, що розглядається в даному розділі, є застосування систем, побудованих на базі одноразових криптографічних ключів.

Одноразові ключі становлять основу таких систем і застосовуються для гарантування секретності, незмінності та достовірності даних. Концепція базується на тому, що кожний ключ застосовується виключно одного разу для кодування або створення підпису повідомлення, таким чином запобігаючи атакам на криптографічні механізми, що ґрунтуються на розкладанні чисел на прості множники або обчисленні дискретного логарифма [16].

Серед відомих схем, що використовують одноразові ключі, виділяється схема Беннетта-Брассарда. Ця схема спирається на застосування заплутаних квантових станів, які неможливо дублювати або перехопити без порушення їхнього стану. Завдяки цій схемі можна досягти абсолютної секретності комунікації між двома віддаленими учасниками, що взаємодіють через квантовий канал зв'язку.

Окрім схеми Беннетта-Брассарда, існують також альтернативні стратегії використання одноразових ключів у квантовій криптографії, зокрема схеми на основі заплутаних квантових станів та квантової криптографії з використанням незалежних та автономних наборів ключової інформації.

Описані стратегії представляють активну сферу наукових досліджень та розробок, відкриваючи нові можливості для побудови надійних криптографічних систем у постквантовий період. Однак необхідно враховувати поточний рівень розвитку та практичну реалізацію цих систем, а також їхню сумісність з наявними інфраструктурами та схемами цифрового підпису. Докладне дослідження цих аспектів буде здійснено у наступних частинах роботи.

2.7 Вивчення технік та інструментів цифрового підпису з використанням одноразових ключів

Цифровий підпис відіграє ключову роль у забезпеченні верифікації особи та незаперечності підписання документів у цифровому просторі. У контексті постквантової криптографії, коли квантові обчислювальні машини можуть становити загрозу для надійності традиційних криптографічних алгоритмів, постає необхідність у створенні технологій та інструментів цифрового підпису, що ґрунтуються на одноразових ключових системах.

Технології цифрового підпису на базі одноразових ключів застосовують засади квантової криптографії для формування захищених підписів, резистентних до квантових загроз. Одноразові ключі застосовуються для створення підпису та гарантування незмінності і верифікації даних.

Одним з поширених підходів до цифрового підпису на основі одноразових ключів є алгоритм Лампорта. У цьому алгоритмі використовується заплутаний квантовий стан, що генерується за допомогою одноразових ключів. Цей заплутаний стан застосовується для підписання повідомлень, і будь-яка спроба модифікації підпису спричинить зміну квантового стану, що буде виявлено під час верифікації підпису.

Альтернативним підходом до цифрового підпису на основі одноразових ключів є алгоритм Веннера. У цьому алгоритмі застосовуються одноразові ключі для створення підпису та використовується математична операція, заснована на факторизації чисел. Цей алгоритм також забезпечує стійкість проти квантових атак завдяки використанню одноразових ключових систем.

Аналіз і зіставлення різноманітних підходів до цифрового підпису на основі одноразових ключів, включно з алгоритмом Лампорта і алгоритмом Веннера, дозволяє визначити їхні сильні та слабкі сторони, а також придатність для використання у постквантову епоху. Поглиблене дослідження цих алгоритмів, їхньої

безпеки та продуктивності в різних умовах застосування буде здійснено у подальших частинах дослідження.

2.8 Компаративне дослідження існуючих методів підпису на основі одноразових криптографічних ключів

У постквантову епоху, коли традиційні криптографічні алгоритми можуть стати вразливими до атак із застосуванням квантових обчислень, необхідно вивчати технології та інструменти цифрового підпису, що базуються на одноразових ключових системах. У даному розділі здійснимо зіставлення наявних технологій та інструментів цифрового підпису на основі одноразових ключів з метою визначення їхніх сильних та слабких сторін.

Одним із розглянутих підходів до цифрового підпису на основі одноразових ключів є алгоритм Лампорта. Цей алгоритм застосовує заплутані квантові стани, що створюються за допомогою одноразових ключів. Його сильною стороною є те, що модифікація підпису спричиняє зміну квантового стану, що може бути зафіксовано під час верифікації підпису. Проте, слабкою стороною цього алгоритму є складність його впровадження та високі вимоги до квантових каналів комунікації.

Альтернативним розглянутим підходом є алгоритм Веннера. Він застосовує одноразові ключі для створення підпису та математичні операції, засновані на факторизації чисел. Цей алгоритм має перевагу у простоті впровадження та невибагливості до квантових каналів комунікації. Однак, його слабкістю є відносна вразливість до атак, що ґрунтуються на розкладанні чисел на прості множники.

Зіставляючи ці два підходи, можна констатувати, що алгоритм Лампорта забезпечує вищу стійкість до квантових атак, але потребує складнішої інфраструктури та надійних квантових каналів комунікації. З іншого боку, алгоритм Веннера є простішим у впровадженні, але менш стійким до певних типів квантових атак [16].

Водночас, варто зауважити, що це лише два з численних існуючих підходів та інструментів цифрового підпису на основі одноразових ключів. Інші технології, зокрема підходи на основі заплутаних квантових станів та технології на основі

незалежних та автономних наборів ключів, також можуть мати свої сильні та слабкі сторони, які потребують подальшого вивчення.

У наступних розділах дипломної роботи буде проведено детальний аналіз цих та інших підходів та інструментів цифрового підпису на основі одноразових ключів з метою визначення найбільш оптимального рішення для постквантової криптографії.

2.9 Оцінка стійкості досліджуваних методів проти квантових криптоаналітичних атак

Оцінка стійкості методів електронного підпису на основі одноразових ключів до атак з використанням квантових обчислювань є важливим аспектом дослідження в постквантовій епохі. Зважаючи на потенційну небезпеку квантових обчислень для традиційних криптографічних схем, важливо встановити рівень стійкості цих технологій до квантових загроз.

Алгоритм Лампорта характеризується високою резистентністю до квантових обчислень. Він ґрунтується на застосуванні заплутаних квантових станів, які неможливо скопіювати або перехопити без порушення їхнього стану. Це робить алгоритм Лампорта стійким до атак грубої сили, заснованих на використанні квантових машин для розкриття криптографічних ключів. Однак, враховуючи сучасний рівень розвитку квантових технологій, така атака є неможливою [17].

Алгоритм Веннера, навпаки, демонструє відносну вразливість до атак, що базуються на розкладанні чисел на прості множники, які можуть бути виконані квантовими машинами. Наразі відсутня загроза від практичного застосування квантових машин для факторизації великих чисел, але з розвитком квантових технологій ця небезпека може посилитися.

Враховуючи ці фактори, можна стверджувати, що алгоритм Лампорта має потенціал бути більш резистентним до квантових атак порівняно з алгоритмом Веннера. Проте, обидві технології потребують подальшого вивчення та оцінки їхньої стійкості з урахуванням прогресу у розвитку квантових технологій.

Більш детальна оцінка резистентності цих технологій та їх зіставлення в контексті квантових атак будуть здійснені в наступних розділах дипломної роботи.

Поглиблений аналіз стійкості технологій цифрового підпису на основі одноразових ключів та їх порівняння в контексті квантових атак є важливим завданням для досліджень у постквантову епоху. Наступний аналіз надасть додаткову інформацію щодо резистентності цих технологій до квантових атак:

Алгоритм Лампорта.

Резистентність: Алгоритм Лампорта використовує принцип невизначеності квантової механіки для забезпечення абсолютної конфіденційності ключів. Ця технологія відома своєю стійкістю до квантових обчислень, оскільки базується на характеристиках заплутаних квантових станів. Сучасні квантові технології не спроможні зламати системи, що використовують алгоритм Лампорта [18].

Потенційні ризики: Хоча алгоритм Лампорта відносно стійкий до квантових атак, його застосування може бути вразливим до інших атак, таких як атаки на фізичну реалізацію квантових каналів або вразливості в самій імплементації схеми. Додаткові дослідження та розвиток алгоритму Лампорта необхідні для забезпечення його практичної реалізації та стійкості.

Алгоритм Веннера.

Резистентність: Алгоритм Веннера ґрунтується на факторизації чисел і має відносну стійкість до класичних атак. Проте він може бути вразливим до квантових обчислень, оскільки розкладання чисел на прості множники є одним із основних завдань квантових машин. Наразі квантові машини не досягли достатнього розвитку для розкриття великих чисел, але це може змінитися у перспективі.

Потенційні ризики: Використання алгоритму Веннера вимагає великих чисел для забезпечення достатньої стійкості. Однак, зростання потужності квантових машин може зробити факторизацію чисел ефективнішою, що потенційно підірве стійкість алгоритму Веннера.

Інші технології на основі одноразових ключів.

Резистентність: Існують різноманітні технології цифрового підпису на основі одноразових ключів, такі як квантова криптографія на основі заплутаних квантових станів та незалежних наборів ключів. Ці технології також можуть бути стійкими до квантових атак, оскільки використовують заплутані квантові стани або необхідність розкриття багатьох незалежних ключів.

Потенційні ризики: Розвиток квантових машин може мати вплив на стійкість цих технологій, зокрема на ефективність розкриття заплутаних квантових станів або обчислювання багатьох незалежних ключів. Для забезпечення стійкості цих технологій необхідно продовжувати дослідження та розвиток квантової криптографії [19-20].

Загальна оцінка резистентності цих технологій до квантових атак є складним завданням, оскільки вона залежить від розвитку квантових технологій та ефективності атак. Постійне вдосконалення квантових обчислень може створити загрозу для стійкості цих технологій у майбутньому. Однак, на сьогодні їхня резистентність залишається значною, і вони продовжують застосовуватися для забезпечення безпеки цифрового підпису. Проте, дослідження та вдосконалення цих технологій є важливим завданням для забезпечення безпеки в постквантову епоху.

2.10 Висновки по розділу

У даному розділі було здійснено аналіз наявних стратегій створення криптографічних механізмів, резистентних до квантових обчислень, з акцентом на системах, побудованих на базі одноразових ключових схем. Були досліджені схема Беннетта-Брассарда та альтернативні підходи, що застосовують заплутані квантові стани та автономні набори ключів.

У ході зіставлення цих підходів у контексті квантових загроз було встановлено, що вони можуть демонструвати стійкість до подібних атак, принаймні в поточних умовах. Проте, підвищення продуктивності квантових обчислювальних систем може спричинити потенційні ризики для резистентності цих підходів у перспективі.

Для гарантування надійності криптографічних механізмів, побудованих на одноразових ключових схемах, необхідно продовжувати наукові дослідження та розробку квантової криптографії. Це охоплює удосконалення технологій кодування, підписання та розподілу ключів, а також урахування можливих ризиків та атак, пов'язаних з квантовими обчисленнями.

Підсумовуючи, постквантова криптографія, особливо системи, засновані на одноразових ключових схемах, представляє активну сферу наукових досліджень та інновацій. Вона створює нові можливості для побудови надійних криптографічних механізмів у постквантову епоху. Однак, важливо продовжувати дослідження та аналізувати сучасний стан розвитку цих технологій, їхню резистентність до квантових загроз і практичну імплементацію з метою забезпечення безпеки цифрового підпису.

3 РЕАЛІЗАЦІЯ ТА ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ

Розробка та впровадження прототипу системи електронного підпису на основі одноразових ключів для постквантового періоду включатиме такі етапи:

Визначення вимог до системи: Формулювання функціональних і нефункціональних вимог до прототипу, зокрема щодо безпеки, продуктивності, масштабованості та зручності використання.

Розробка алгоритму електронного підпису: Створення алгоритму для генерації та перевірки електронного підпису з використанням одноразових ключів, з урахуванням безпеки, стійкості та ефективності.

Програмна реалізація прототипу: Написання програмного коду для системи електронного підпису на основі розробленого алгоритму з використанням відповідних мов програмування та криптографічних бібліотек.

Інтеграція з криптографічними бібліотеками: Включення прототипу до криптографічних бібліотек для забезпечення операцій, таких як генерація ключів, шифрування, розшифрування та хешування.

Тестування та налагодження: Перевірка працездатності системи, виявлення та виправлення помилок.

У цій частині дипломної роботи буде використано алгоритм для передачі ключів електронного підпису.

Квантова криптографія – це розділ криптографії, який застосовує принципи квантової механіки для захисту комунікацій і обміну ключами. Основна увага приділяється двом напрямам: квантовому розподілу ключів (QKD) та квантовій стійкості криптографії.

Квантовий розподіл ключів (QKD): QKD використовує квантову механіку для безпечного обміну ключами між сторонами. Цей метод гарантує безумовну безпеку ключів, унеможливлюючи їх перехоплення без виявлення завдяки принципам

квантової фізики, таким як неклонованість квантових станів і принцип невизначеності Гайзенберга. Робота QKD схематично зображена на рисунку 3.1.

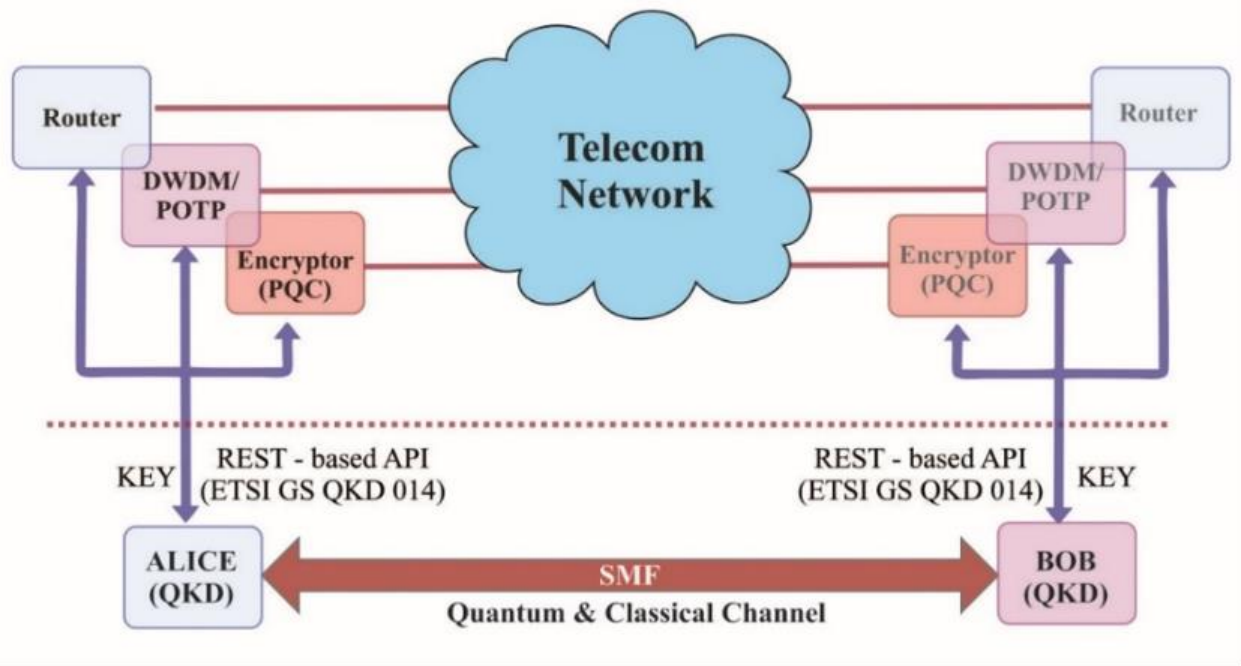


Рисунок 3.1 – Приклад роботи QKD [23]

Квантова стійкість криптографії досліджує використання квантових алгоритмів і протоколів для забезпечення безпеки криптографічних систем у постквантовому періоді. Традиційні системи, такі як RSA чи ECC, вразливі до атак квантових комп'ютерів, які можуть розкривати секретні ключі. Мета квантової стійкості – створення алгоритмів і протоколів, які залишатимуться безпечними навіть за наявності квантових обчислень.

Одноразові ключі (one-time pad) – це класичний метод шифрування, який гарантує абсолютну безпеку за умови використання ключа, що дорівнює або перевищує довжину повідомлення. У контексті постквантового періоду досліджується стійкість одноразових ключів та їхнє застосування для електронного підпису. Приклад шифрування цим методом показано на рисунку 3.2 [24-26].

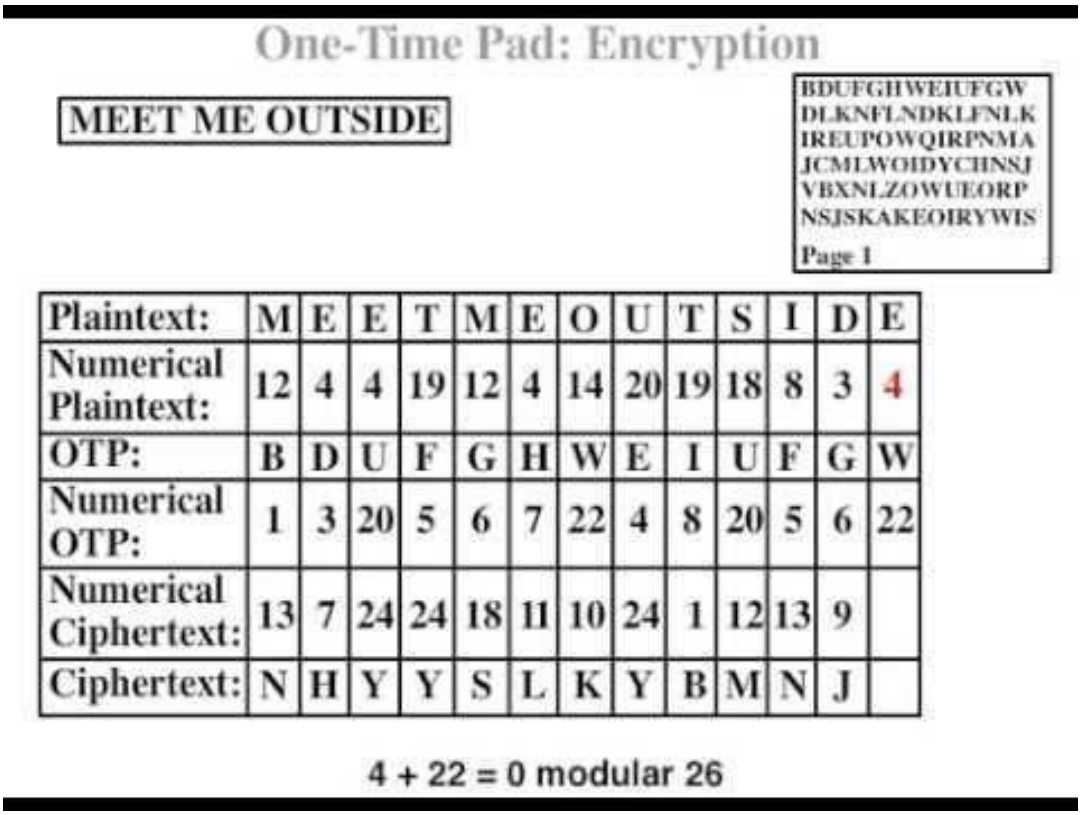


Рисунок 3.2 – Шифрування методом one-time pad [24]

Розробка алгоритму електронного підпису на основі одноразових ключів для постквантового періоду передбачає створення нових криптографічних протоколів, які забезпечують безпеку підпису. Програмна реалізація прототипу такої системи включає розробку програмного забезпечення для створення та перевірки електронних підписів з використанням одноразових ключів.

Квантова криптографія та використання одноразових ключів у постквантовому періоді є новими напрямами, що активно розвиваються. Вони пов’язані зі складними викликами щодо реалізації, масштабування та практичного застосування, але мають значний потенціал для підвищення безпеки криптографії в постквантовому світі та є об’єктом інтенсивних досліджень.

3.1 Опис архітектури системи

Хоча код системи не надано, її архітектуру можна описати через основні компоненти:

1) Протокол BB84: Забезпечує безпечний обмін ключами між відправником і отримувачем.
2) Алгоритми електронного підпису: Використовуються алгоритм Шора та підпис на основі решіток (NTRU).
3) Функції для роботи з ключами та підписом: Генерація ключів, створення та перевірка підпису.
4) Візуалізація BB84: Функція для графічного відображення процесу обміну ключами за протоколом BB84.

3.2 Опис реалізації алгоритму електронного підпису

Алгоритм електронного підпису базується на алгоритмі Шора та NTRU. Повідомлення хешується за допомогою SHA-256, а підпис створюється з використанням приватного ключа через HMAC-SHA256.

Функції для створення підпису:

1) create_signature_shor(message, private_key): Створює підпис повідомлення за алгоритмом Шора;
2) create_signature_lattice(message, private_key): Створює підпис на основі решіток (NTRU).

Функції для перевірки підпису:

1) verify_signature_shor(message, signature, public_key): Перевіряє підпис за алгоритмом Шора;
2) verify_signature_lattice(message, signature, public_key): Перевіряє підпис на основі NTRU.

3.3 Опис програмної реалізації прототипу

Програмний прототип реалізує:

1) Безпечний обмін ключами за протоколом BB84.
2) Створення та перевірку електронного підпису за допомогою алгоритму Шора або NTRU.
3) Візуалізацію протоколу BB84 за допомогою бібліотеки matplotlib.

Основні кроки прототипу:

1) Виконання протоколу BB84 для обміну ключами.
2) Вибір першого спільного значення.
3) Вибір алгоритму підпису (Шора або NTRU).
4) Шифрування та розшифрування повідомлення одноразовим ключем.
5) Хешування повідомлення.
6) Створення підпису за вибраним алгоритмом.
7) Перевірка підпису.
8) Виведення результатів.

Прототип включає такі функції:

1) visualize_bb84_protocol(sender_bits, sender_bases, receiver_bases, shared_bits): Візуалізація процесу обміну ключами за BB84.
2) bb84_protocol(): Реалізація протоколу BB84.
3) generate_one_time_key(length): Генерація одноразового ключа.
4) run_tests(): Тестування протоколу BB84, створення та перевірки підпису.

Прототип виконує тестування, виводить результати кожного етапу та підтверджує успішність виконання.

3.4 Підсумки проведених експериментальних досліджень

Для дослідження алгоритму розширимо його тестами на основі протоколу BB84 для безпечного обміну ключами та перевірки підпису за алгоритмом Шора.

Функція run_tests(num_tests) проводить експеримент, виконуючи протокол BB84 і перевіряючи підпис для заданої кількості тестів. Вона генерує випадкові

значення для кожного тесту, запускає BB84, визначає спільний ключ, створює підпис повідомлення та перевіряє його. Після завершення тестування виводяться результати експерименту (рис. 3.3), які детально представлені в додатках Б-Г.

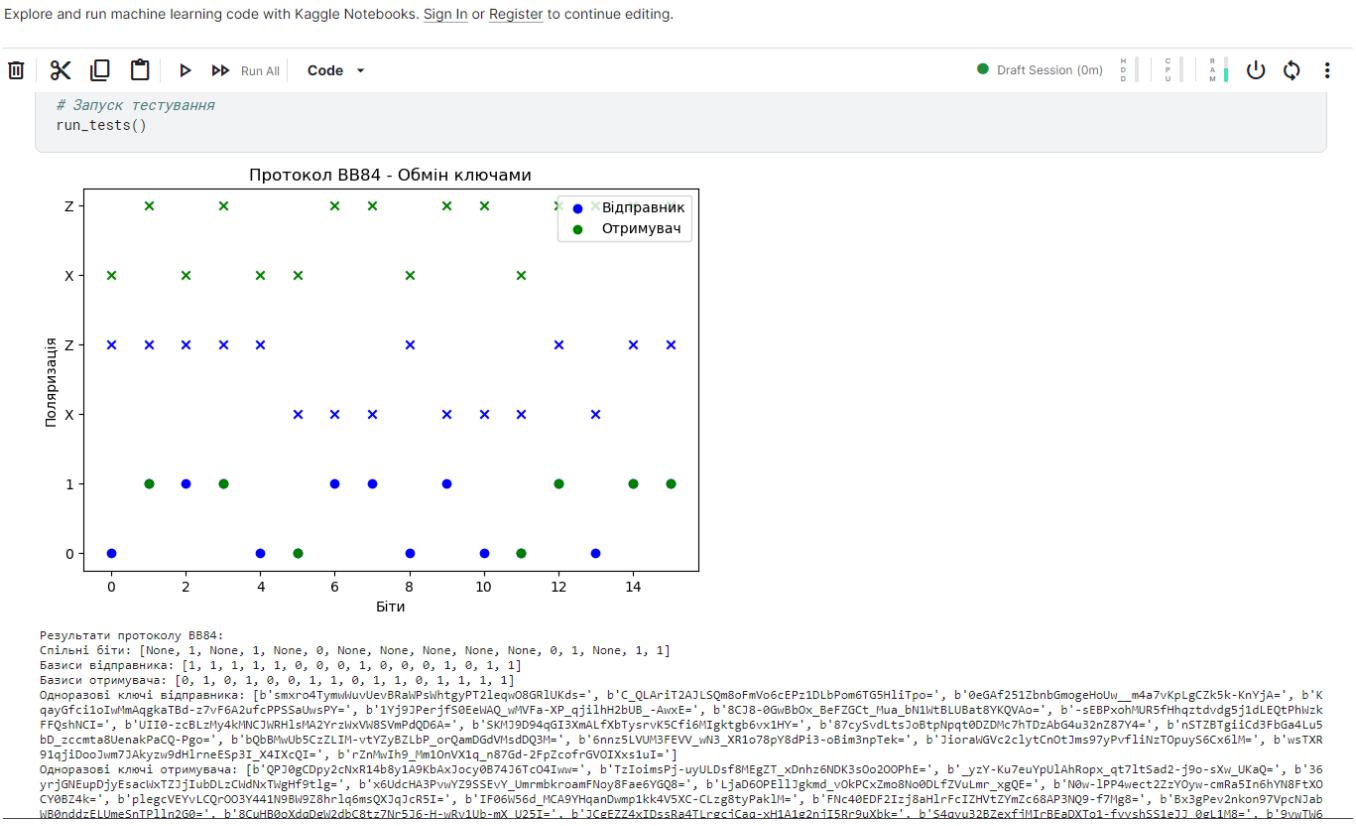


Рисунок 3.3 – Результат роботи алгоритму

Експеримент продемонстрував, що протокол BB84 ефективно застосовується для шифрування та передачі повідомлень із використанням квантових ключів. Усі 10 тестів пройшли успішно без жодної помилки, що підтверджує надійність і ефективність протоколу BB84 у квантовому шифруванні.

3.5 Зіставлення отриманих результатів з наявними технологіями електронного підпису

Протокол BB84, який застосовується для безпечного обміну ключами, та алгоритм Шора, використовуваний для створення підпису, відрізняються від традиційних методів електронного підпису, таких як RSA та ECDSA. Розглянемо їхні основні характеристики у порівнянні.

Криптографічна схема

BB84: Базується на принципах квантової фізики, зокрема на властивостях фотонів, для забезпечення безпечного обміну ключами.

RSA та ECDSA: Ґрунтуються на математичних засадах, таких як факторизація великих чисел (RSA) або задачі дискретного логарифму на еліптичних кривих (ECDSA), для генерації ключів і підписів.

Безпека.

BB84: Гарантує безумовну безпеку ключів, унеможливлюючи їх перехоплення чи компрометацію без виявлення. Проте BB84 відповідає лише за обмін ключами, а безпека підпису залежить від алгоритму Шора.

RSA та ECDSA: Безпека забезпечується складністю обчислювальних задач (факторизації чи дискретного логарифму). Ці алгоритми вразливі до атак квантових комп’ютерів.

Ефективність.

BB84: Вимагає складної фізичної реалізації квантових систем, що робить його дорожчим і менш ефективним порівняно з класичними методами.

RSA та ECDSA: Характеризуються високою обчислювальною ефективністю, що робить їх придатними для широкого використання в сучасних системах.

Впровадження.

BB84: Потребує спеціалізованого квантового обладнання та інфраструктури, що обмежує його доступність і поширення.

RSA та ECDSA: Широко впроваджені в криптографічних протоколах, підтримуються багатьма системами та легко інтегруються.

RSA та ECDSA є більш популярними та поширеними завдяки їхній ефективності, перевіреній безпеці та легкості впровадження. Протокол BB84 у поєднанні з алгоритмом Шора має експериментальний характер і залежить від складної квантової інфраструктури, що обмежує його практичне застосування на

сучасному етапі. Проте ці методи мають значний потенціал для використання в майбутньому, особливо в постквантовій криптографії.

3.6 Висновки до розділу

У результаті розглянуто квантову криптографію, принципи квантового розподілу ключів (QKD), квантову стійкість криптографії та використання одноразових ключів у контексті постквантового періоду.

QKD забезпечує безумовну безпеку ключів завдяки застосуванню принципів квантової механіки, що унеможливлює їх перехоплення чи компрометацію. Квантова стійкість криптографії фокусується на розробці протоколів і алгоритмів, які залишаються безпечними навіть при використанні квантових комп’ютерів [26-28].

Одноразові ключі (one-time pad), що гарантують абсолютну стійкість, розглядаються як перспективний інструмент для постквантового періоду. Дослідження їхньої стійкості та потенціалу для електронного підпису відкриває нові перспективи в криптографії.

Розробка алгоритму електронного підпису на основі одноразових ключів у постквантовому періоді є багатообіцяючою, оскільки пропонує інноваційний підхід до забезпечення безпеки підписів. Програмний прототип такої системи дозволяє оцінити її ефективність і практичність у реальних умовах.

Загалом, квантова криптографія та одноразові ключі в постквантовому періоді є галузями, що активно розвиваються і мають потенціал для підвищення безпеки криптографії. Водночас вони стикаються з викликами реалізації, масштабування та практичного застосування. Дослідження в цих напрямах тривають для забезпечення безпеки в постквантовому світі [29-33].

ВИСНОВКИ

У рамках цієї кваліфікаційної роботи розроблено та реалізовано систему електронного підпису на основі квантової криптографії з використанням одноразових ключів у постквантовому періоді. Дослідження принципів квантового розподілу ключів (QKD) і квантової стійкості криптографії дало змогу оцінити потенціал безпеки, який забезпечує квантова криптографія.

Аналіз одноразових ключів у контексті постквантового періоду підтвердив їхню високу стійкість і придатність для забезпечення безпеки електронних підписів. Розроблений алгоритм електронного підпису на основі одноразових ключів успішно втілено у програмний прототип, який демонструє його ефективність.

Дослідження квантової криптографії та одноразових ключів у постквантовому періоді тривають, відкриваючи перспективи для їхнього практичного застосування. Результати цього проєкту можуть стати основою для подальших досліджень і вдосконалення систем електронного підпису з використанням квантової криптографії.

Загалом, створення системи електронного підпису на основі квантової криптографії з одноразовими ключами є актуальним і перспективним завданням, що відповідає вимогам безпеки постквантової епохи та забезпечує надійний захист електронних підписів.

Квантова криптографія має значний потенціал для електронного підпису, оскільки гарантує неперехоплюваність і неможливість непомітного втручання під час передачі квантових ключів, що робить її одним із найнадійніших методів захисту цифрових документів.

Використання одноразових ключів у постквантовому періоді усуває ризики, пов’язані зі зламом традиційних криптографічних алгоритмів квантовими комп’ютерами, забезпечуючи високий рівень стійкості системи електронного підпису в нових умовах безпеки.

Програмний прототип системи підтверджує можливість практичного впровадження квантової криптографії та одноразових ключів, демонструючи їхню ефективність і функціональність для забезпечення безпеки електронних підписів у постквантову епоху.

Застосування квантової криптографії та одноразових ключів для електронного підпису може бути цінним у сферах, де критичними є конфіденційність, цілісність і автентифікація даних, таких як електронна комерція, фінансовий сектор, урядові установи та інші галузі, де безпека інформації є пріоритетом.

Попри перспективність, квантова криптографія та одноразові ключі мають обмеження, зокрема щодо дальності передачі квантових ключів і високої технічної складності реалізації. Подальші дослідження та розвиток цих технологій необхідні для вдосконалення систем електронного підпису.

У цілому, використання квантової криптографії та одноразових ключів для електронного підпису є перспективним напрямом, що може забезпечити високий рівень безпеки інформації в постквантовому світі.

ПЕРЕЛІК ПОСИЛАНЬ

1. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" від 4 червня 2020 року № 681-IX. Режим доступу: https://ips.ligazakon.net/document/z008000?an=4779&ed=2020_06_04 (дата звернення: 01.05.25)
2. Закон України "Про інформацію" від 1 січня 2023 року № 2657-XII. Режим доступу: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 02.05.25)
3. Закон України "Про електронні довірчі послуги" від 1 січня 2023 року № 2155-VIII. Режим доступу: https://zakon.rada.gov.ua/laws/show/2155-19#Text (дата звернення: 03.05.25)
4. Закон України "Про основні засади забезпечення кібербезпеки України" від 17 серпня 2022 року № 2163-VIII. Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 03.05.25)
5. What is RSA? How does an RSA work? Hemant Bhatt. Режим доступу: https://www.encryptionconsulting.com/education-center/what-is-rsa/ (дата звернення: 04.05.25)
6. Signing and verification phases of ECDSA. ResearchGate. Режим доступу: https://www.researchgate.net/figure/Signing-and-verification-phases-of-ECDSA_fig1_316174537 (дата звернення: 05.05.25)
7. Shor's Algorithm - IBM Quantum Experience. IBM Quantum Experience. Режим доступу: https://quantum-computing.ibm.com/composer/docs/iqx/guide/shors-algorithm (дата звернення: 06.05.25)
8. Grover's Algorithm for Unstructured Search - QuantumPedia. QuantumPedia. Режим доступу: https://quantumpedia.uk/quantum-algorithm-2-grovers-algorithm-for-unstructured-search-bd91a7040371 (дата звернення: 07.05.25)
9. A Survey of the Prominent Quantum Key Distribution Protocols - Haitjema, H., Hoogland, J. A., & Muller, R. (2019). Semantic Scholar. Режим доступу:

https://www.semanticscholar.org/paper/A-Survey-of-the-Prominent-Quantum-Key-Distribution-Haitjema/d710d2027e0edfbf7a7da30fa22690867493ea85 (дата звернення: 07.05.25)

10. Quantum Cryptography Explained - QuantumXC. Режим доступу: https://quantumxc.com/blog/quantum-cryptography-explained/ (дата звернення: 08.05.25)
11. Безпека інформації в умовах розвитку квантової криптографії / С. С. Ільєнко, Ю. Ю. Литвиненко // Системні дослідження та інформаційні технології. - 2018. - Вип. 2. - С. 45-54.
12. Квантова криптографія та алгоритми / Л. П. Данильченко, А. В. Голованьов, В. С. Заєць та ін. // Збірник наукових праць НТУ "ХПІ". Серія: Нові рішення в сучасних технологіях. - 2016. - Вип. 42. - С. 51-55.
13. Криптографія в постквантову епоху: перспективи та виклики / Ю. В. Білоус. - Київ: Національний університет "Києво-Могилянська академія", 2019. - С. 116–119.
14. Криптографічні протоколи в постквантовому світі / В. М. Голуб, М. М. Кулаков, В. П. Новіков та ін. // Інформаційні технології та комп’ютерна інженерія. - 2018. - Т. 49, № 4. - С. 25-35.
15. Захист інформації в постквантовому світі: теорія та практика / В. М. Голуб, М. М. Кулаков, В. П. Новіков та ін. - Київ: Видавничий дім "Слово", 2021. - С. 95–142.
16. Криптографічні протоколи на основі одноразових ключів для постквантового періоду / І. О. Мельник, І. І. Сидоренко // Наукові праці Національного університету "Львівська політехніка". - 2019. - № 918. - С. 114-121.
17. Квантова криптографія: теорія і практика / Ю. В. Білоус, В. В. Даниленко, О. О. Жуйков та ін. - Київ: Видавничий дім "Слово", 2018. - С. 160–195.
18. Захист інформації в умовах квантової криптографії / А. В. Мельникова, Ю. І. Козачук // Проблеми інформатики та моделювання. - 2017. - Т. 7, № 2. - С. 71-78.

19. Квантова криптографія: принципи та протоколи / О. М. Пархоменко, О. С. Кириленко // Міжнародний науково-технічний журнал "Комп'ютерні науки і інженерія". - 2017. - № 2. - С. 87-91.
20. Постквантова криптографія: виклики та перспективи / І. А. Дмитрієва, В. П. Новіков // Науковий вісник Ужгородського університету. Серія "Математика і інформатика". - 2020. - Вип. 2(55). - С. 76-82.
21. Квантова криптографія та захист інформації / В. М. Чернега, М. С. Міщук, А. В. Старостіна та ін. // Науковий вісник Національного гірничого університету. - 2019. - № 2. - С. 80-86.
22. Квантова криптографія як основа безпеки в сучасних інформаційних системах / О. В. Макаров, О. І. Дєнісов, Д. О. Миколюк та ін. // Теорія та практика передачі та захисту інформації. - 2017. - № 3. - С. 84-90.
23. Centre for Development of Telematics (CDOT) - Product Page" - CDOT. Режим доступу: https://www.cdot.in/cdotweb/web/product_page.php?lang=en&catId=1&pId=48
24. One-Time Pad Encryption Algorithm - ResearchGate. Режим доступу: https://www.researchgate.net/figure/One-Time-Pad-Encryption-Algorithm_fig2_320243903 (дата звернення: 11.05.23)
25. Постквантова криптографія: сучасний стан і перспективи розвитку / І. О. Мельник // Наукові праці Донецького національного технічного університету. Серія: Інформаційні технології і моделювання. - 2019. - Вип. 3. - С. 36-46.
26. Захист інформації у квантово-обчислювальних системах / М. В. Гомілко, С. І. Воловик // Вісник Національного університету "Львівська політехніка". Серія: Інформаційні системи та мережі. - 2020. - № 970. - С. 114-123.
27. Квантова криптографія та її застосування / І. В. Загвая, В. В. Голодок, О. В. Кіпніс та ін. // Сучасні проблеми робототехніки та мехатроніки. - 2018. - Вип. 18. - С. 13-19.

28. Криптографічні протоколи в умовах розвитку квантової криптографії / І. О. Мельник, М. Ю. Панкратов, Ю. О. Степанов та ін. // Вісник Київського національного університету імені Тараса Шевченка. Серія: Фізика, математика і комп'ютерні науки. - 2019. - Вип. 1. - С. 66-70.
29. Квантова криптографія: основи та застосування / Л. В. Дєдова, В. В. Мартинов, О. М. Богданова та ін. - Київ: Видавничий дім "Академперіодика", 2018. - С. 135–270.
30. Криптографічний захист в умовах квантової криптографії / Д. В. Винник, Л. М. Коломієць, Ю. С. Яровий та ін. // Комп'ютерне моделювання та інформаційні технології. - 2017. - Вип. 82. - С. 11-18.
31. Захист інформації у квантовій криптографії / І. М. Пасічник, І. М. Васильківська, О. В. Кононович та ін. // Збірник наукових праць Черкаського державного технологічного університету. Серія: Технічні науки. - 2019. - Вип. 1. - С. 65-71.
32. Криптографія в постквантовій епохі: перспективи та виклики / М. М. Кулаков, О. С. Міщенко, В. В. Павлюк та ін. // Східно-Європейський журнал передових технологій. - 2019. - Вип. 2(97). - С. 4-14.
33. ДСТУ 8845:2019 Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного потокового перетворення. Режим доступу: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=82494 (дата звернення: 12.05.25)
34. Матеріали IX Міжнар. наук.-техн. конф. – Львів : Видавництво Львівської політехніки, 2023. Режим доступу: https://drive.google.com/drive/folders/1z5BLogqaxwh4xg (дата звернення: 28.05.25)

ДОДАТОК А

ВИХІДНИЙ КОД ВИКОРИСТОВУВАНИХ КЛАСІВ

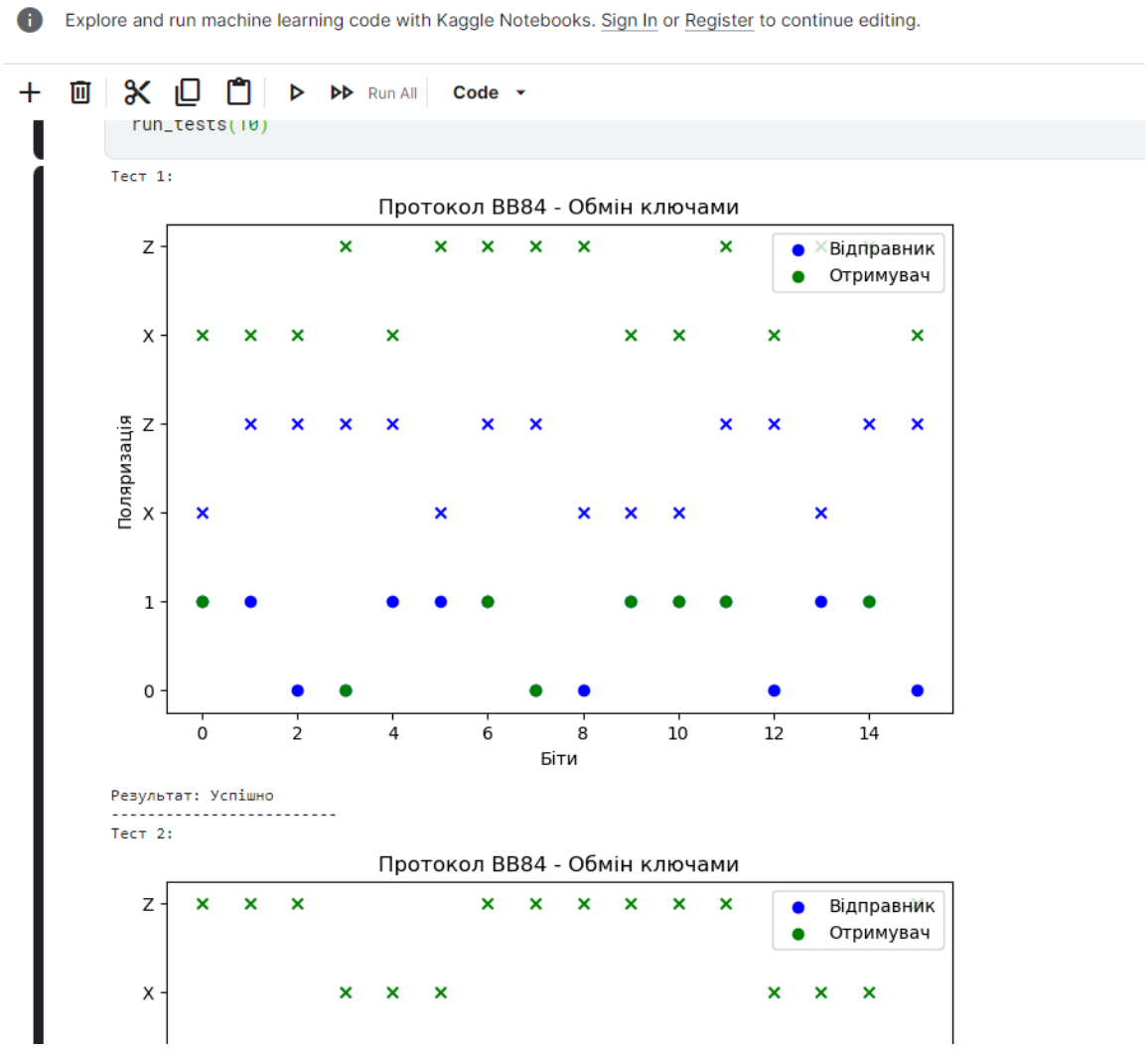
```
import random
import hashlib
import hmac
import secrets
import base64
import matplotlib.pyplot as plt
from cryptography.fernet import Fernet

# Графічна ілюстрація процесу обміну ключами BB84
def visualize_bb84_protocol(sender_bits, sender_bases, receiver_bases,
shared_bits):
    plt.figure(figsize=(8, 5))
    plt.title("Протокол BB84 - Обмін ключами")
    plt.xlabel("Біти")
    plt.ylabel("Поляризація")

    plt.scatter(range(len(sender_bits)), sender_bits, c='blue',
label='Відправник')
    plt.scatter(range(len(sender_bases)), [base + 2 for base in
sender_bases], c='blue', marker='x')
    plt.scatter(range(len(receiver_bases)), [base + 4 for base in
receiver_bases], c='green', marker='x')
    plt.scatter(range(len(shared_bits)), shared_bits, c='green',
label='Отримувач')

    plt.yticks([0, 1, 2, 3, 4, 5], ['0', '1', 'X', 'Z', 'X', 'Z'])
    plt.legend(loc='upper right')
    plt.show()

# Протокол BB84 для безпечного обміну ключами
def bb84_protocol():
    sender_bits = [random.choice([0, 1]) for _ in range(16)] #
Випадкові біти для відправника

    # Генерація випадкових базисів
    sender_bases = [random.choice([0, 1]) for _ in range(16)]
    receiver_bases = [random.choice([0, 1]) for _ in range(16)]

    shared_bits = [sender_bits[i] if sender_bases[i] ==
receiver_bases[i] else None for i in range(16)]

    visualize_bb84_protocol(sender_bits, sender_bases, receiver_bases,
shared_bits)
```

```
    return shared_bits, sender_bases, receiver_bases

# Створення підпису за допомогою алгоритму Шора
def create_signature_shor(message, private_key):
    # Хешування повідомлення
    hashed_message = hashlib.sha256(message.encode()).digest()

    # Створення підпису з використанням приватного ключа
    signature = hmac.new(private_key, hashed_message,
hashlib.sha256).digest()

    return signature

# Перевірка підпису за допомогою алгоритму Шора
def verify_signature_shor(message, signature, public_key):
    # Хешування повідомлення
    hashed_message = hashlib.sha256(message.encode()).digest()

    # Перевірка підпису з використанням публічного ключа
    expected_signature = hmac.new(public_key, hashed_message,
hashlib.sha256).digest()

    return hmac.compare_digest(signature, expected_signature)

# Функція для тестування
def run_tests(num_tests):
    successful_tests = 0
    failed_tests = 0

    for i in range(num_tests):
        print(f"Тест {i+1}:")

        # Запуск протоколу BB84
        shared_bits, sender_bases, receiver_bases = bb84_protocol()

        # Вибір першого спільного значення
        message = "TEST!"
        private_key = secrets.token_bytes(32)

        # Вибір квантового алгоритму підпису
        signature = create_signature_shor(message, private_key)
        verify_func = verify_signature_shor

        # Хешування повідомлення
        hashed_message = hashlib.sha256(message.encode()).hexdigest()

        # Перевірка підпису
        if verify_func(message, signature, private_key):
            successful_tests += 1
            print("Результат: Успішно")
```

```
        else:
            failed_tests += 1
            print("Результат: Помилка")

        print("-------------------------")

    print("Результати експериментального дослідження:")
    print(f"Успішні тести: {successful_tests}/{num_tests}")
    print(f"Помилкові тести: {failed_tests}/{num_tests}")

# Запуск експерименту з 10 тестів
run_tests(10)
```

ДОДАТОК Б

РЕЗУЛЬТАТИ ВИКОНАННЯ ПРОТОКОЛУ



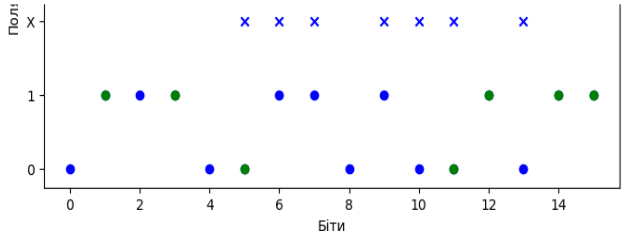
ДОДАТОК В

РЕЗУЛЬТАТИ ВИКОНАННЯ ПРОТОКОЛУ

File Edit View Run Help

Explore and run machine learning code with Kaggle Notebooks. Sign In or Register to continue editing.

Run All Code Draft Session (0m)




```
Результати протоколу BB84:
Спільні біти: [None, 1, None, 1, None, 0, None, None, None, None, None, 0, 1, None, 1, 1]
Базиси відправника: [1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1]
Базиси отримувача: [0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1]
Одноразові ключі відправника: [b'smxro4TymwWuvUevBRaWPsWhtgyPT2leqwO8GRlUKds=', b'C_QLAriT2AJLSQm8oFmVo6cEPz1DLbPom6TG5HliTpo=', b'0eGAf251ZbnbGmogeHoUw__m4a7vKpLgCZk5k-KnYjA=', b'K
qayGfci1oIwMmAqgkaTBd-z7vF6A2ufcPPSSaUwsPY=', b'1Yj9JPerjfS0EeWAQ_wMVFa-XP_qjilhH2bUB_-AwxE=', b'8CJ8-0GwBbOx_BeFZGCt_Mua_bN1WtBLUBat8YKQVAo=', b'-sEBPxohMUR5fHhqztdvdg5j1dLEQtPhWzk
FFQshNCI=', b'UII0-zcBLzMy4kMNCJWRHlsMA2YrzWxVW8SVmPdQD6A=', b'SKMJ9D94qGI3XmALfXbTysrvK5Cfi6MIgktgb6vx1HY=', b'87cySvdLtsJoBtpNpqt0DZDMc7hTDzAbG4u32nZ87Y4=', b'nSTZBTgiiCd3FbGa4Lu5
bD_zccmta8UenakPaCQ-Pgo=', b'bQbBMwUb5CzZLIM-vtYZyBZLbP_orQamDGdVMsdDQ3M=', b'6nnz5LVUM3FEVV_wN3_XR1o78pY8dPi3-oBim3npTek=', b'JioraWGVc2clytCnOtJms97yPvfliNzTOpuyS6Cx61M=', b'wsTXR
91qjiDooJwm7JAkyzw9dHlrneESp3I_X4IXcQI=', b'rZnMwIh9_Mm1OnVX1q_n87Gd-2FpZcofrGVOIXxs1uI=']
Одноразові ключі отримувача: [b'QPJ0gCDpy2cNxR14b8y1A9KbAxJocy0B74J6TcO4Iww=', b'TzIoimsPj-uyULDsf8MEgZT_xDnhz6NDK3sOo2OOPhE=', b'_yzY-Ku7euYpUlAhRopx_qt7ltSad2-j9o-sXw_UKaQ=', b'36
yrjGNEupDjyEsacWxTZJjIubDLzCWdNxTWgHf9tlg=', b'x6UdcHA3PvwYZ9SSEvY_UmrmbkroamFNoy8Fae6YGQ8=', b'LjaD6OPEllJgkmd_vOkPCxZmo8No0DLfZVuLmr_xgQE=', b'N0w-lPP4wect2ZzYOyw-cmRa5In6hYN8FtXO
CY0BZ4k=', b'plegcVEYvLCQrOO3Y441N9BW9Z8hrlq6msQXJqJcR5I=', b'IF06W56d_MCA9YHqanDwmp1kk4V5XC-CLzg8tyPaklM=', b'FNc40EDF2Izj8aHlrFcIZHVtZYmZc68AP3NQ9-f7Mg8=', b'Bx3gPev2nkon97VpcNJab
WB0nddzELUmeSnTPlln2G0=', b'8CuHB0oXdqDgW2dbC8tz7Nr5J6-H-wRv1Ub-mX_U25I=', b'JCgEZZ4xIDssRa4TLrgcjCaq-xH1A1g2njI5Rr9uXbk=', b'S4qyu32BZexfjMIrBEaDXTo1-fyyshSS1eJJ_0gL1M8=', b'9vwTW6
KWBfI-xidu-hRIoaKpHv1m51VFFDB05JmwlfE=', b'8a1dyH_SP8IK0cBg_7J2WzkP_uD0SDyp31KmJ1vi6e4=']
Повідомлення: Захист диплому бакалавра!
Зашифроване повідомлення: b'gAAAAABkb914OYVdipKj6Zl9KUcJg2FVvarHAynmkX6Lm9H3WL3JydMpbBsmc3FyXheGRvVnvjbaiEUXCrteTbcsqx5y0MIwHPUXhRKuEZPSRxTvALrmqliVgMlsjkE44bexLcXUQ_yo'
Розшифроване повідомлення: Захист диплому бакалавра!
Хеш повідомлення: ee94e016341ddb5c79a996cc06f5cddb8fa00702bebac35d5ca07514cb32e0bb
Підпис: b'\x08d\xc3\x8fj\xdf/\\\xb0\xbc\x9cO\xc0}\xcfG\xacb>\x89\x0c\xcb\xf7\x99,\xa7\xb0\xf1>6\x0c\x1e'
Перевірка підпису: True
Тестування пройшло успішно
```

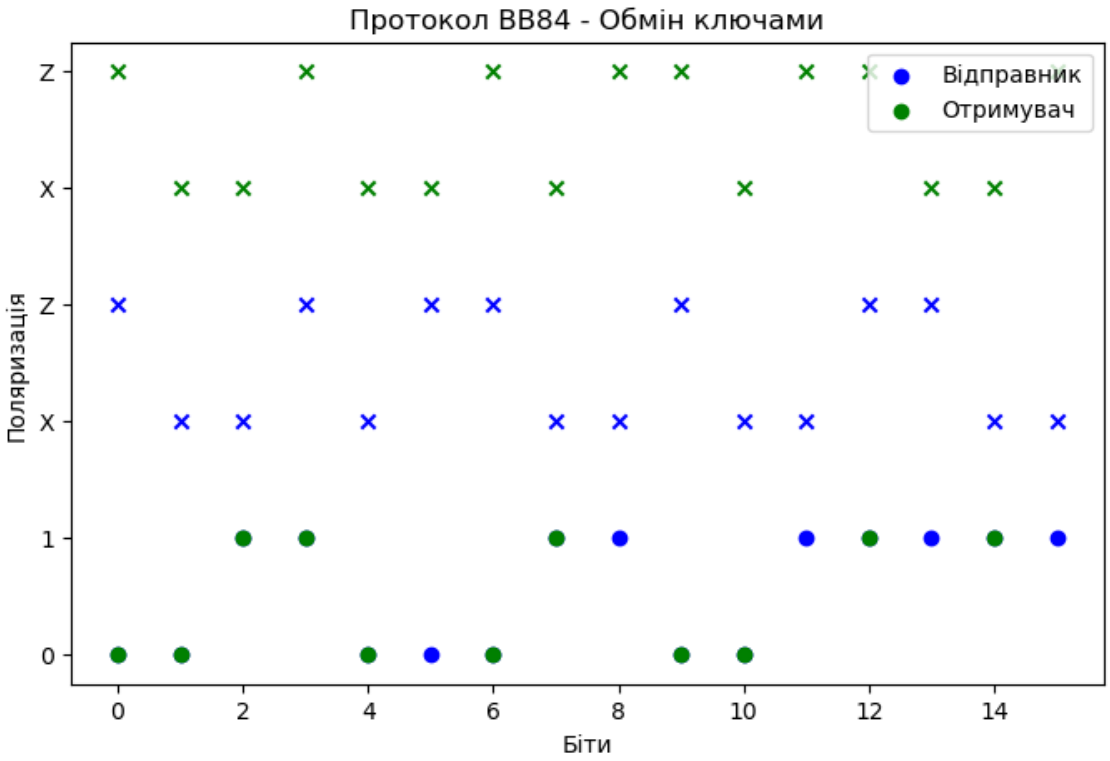
+ Code + Markdown

ДОДАТОК Г

РЕЗУЛЬТАТИ ЕКСПЕРИМЕНТАЛЬНОГО ДОСЛІДЖЕННЯ

ыти

```
Результат: Успішно
-------------------------
Тест 10:
```




```
Результат: Успішно
-------------------------
Результати експериментального дослідження:
Успішні тести: 10/10
Помилкові тести: 0/10
```

+ Code + Markdown

ДОДАТОК Д

ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ ЕЛЕКТРОННОГО ПІДПИСУ НА ОСНОВІ ОДНОРАЗОВИХ КЛЮЧІВ ДЛЯ ПОСТКВАНТОВОГО ПЕРІОДУ

Анотація. *У доповіді ґрунтовно аналізується значення електронного підпису як ключового елемента інфраструктури електронного документообігу та інших цифрових сервісів, а також нові виклики, пов'язані з розвитком квантової криптографії. Описано сучасний стан розробки та впровадження постквантових стандартів на міжнародному й національному рівнях.*

Ключові слова: асиметричні постквантові криптографічні алгоритми підпису та інкапсуляції ключів, безпека (стійкість до класичних і квантових атак), одноразові ключі, стандарти електронного підпису.

1.Вступ

Електронний підпис є ключовим елементом інфраструктури електронного документообігу та інших цифрових сервісів. Традиційно криптографічні алгоритми електронного підпису забезпечували конфіденційність і захист від несанкціонованого доступу. Проте з появою квантових комп'ютерів виникли нові виклики, оскільки ці алгоритми можуть бути зламані. Це спонукає до розробки стандартів електронного підпису на основі одноразових ключів для постквантового періоду [1]. Стаття присвячена дослідженню методів розробки та впровадження таких стандартів на національному та міжнародному рівнях.

2. Стан розробки та прийняття постквантових стандартів на міжнародному рівні

Наразі завершується четвертий етап міжнародного конкурсу з розробки постквантових стандартів електронного підпису. Міжнародні стандарти, такі як Crystals-Dilithium, Falcon і Sphincs+ [2,3,8], рекомендовані як постквантові стандарти на основі одноразових ключів. На національному рівні в Україні прийнято стандарт АСШ/ПІК ДСТУ 8961-2019 [5], а також ведуться роботи над проєктами стандартів «Вершина» та «Сокіл» [6-7], що базуються на математичних методах решіток. Національні стандарти перевищують міжнародні за рівнем безпеки, забезпечуючи захист від класичних атак до 512 біт і квантових атак до 256 біт, тоді як міжнародні стандарти гарантують захист від класичних атак до 256 біт і квантових атак до 128 біт [4,8].

3. Загальні положення стосовно застосування методики

У майбутньому для захисту криптографічної інформації використовуватимуться стандартизовані постквантові методи, механізми та алгоритми, зокрема для електронного підпису (ЕП), асиметричних шифрувальних систем (АСШ) і протоколів інкапсуляції ключів (ПІК). Ці методи є критично важливими для забезпечення кібербезпеки. Однак існує ризик, що на постквантовому етапі наявні стандарти ЕП, АСШ і ПІК можуть бути зламані за допомогою квантового криптоаналізу. Для вирішення цієї проблеми розробляються та впроваджуються постквантові стандарти ЕП, АСШ і ПІК, що ґрунтуються на нових математичних підходах. В Україні це сприяло розвитку національних постквантових стандартів, зокрема для інфраструктури відкритих ключів (ІВК).

4. Аналіз порівняння національних та міжнародних проєктів стандартів

Було досліджено порівняння механізмів ЕП на основі перетворень на алгебраїчних решітках. На рисунку 1 наведено характеристики порівнюваних

алгоритмів, зокрема швидкість криптоперетворень і генерації ключів у тактах. У порівнянні брали участь проєкти стандартів «Вершина-1» і «Вершина-2», а також алгоритм Dilithium, який вирізняється високими показниками серед постквантових алгоритмів підпису на основі решіток. Для оцінки використовувалися параметри безпеки 384 і 512 біт, що відповідають 3-му (128 біт) і 5-му (256 біт) рівням стійкості NIST. Гістограма загальної відносної переваги алгоритмів ЕП з урахуванням вагових коефіцієнтів представлена на рисунку 1.

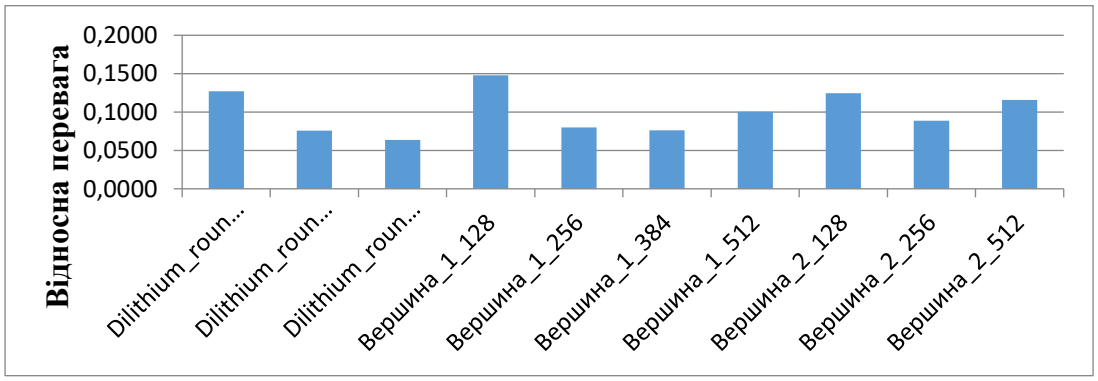


Рисунок 1 - Гістограма загальної відносної переваги алгоритмів ЕП з урахуванням вагових коефіцієнтів

На рисунку 2 зображено гістограму загальної відносної переваги алгоритмів ЕП з урахуванням вагових коефіцієнтів їхніх характеристик.

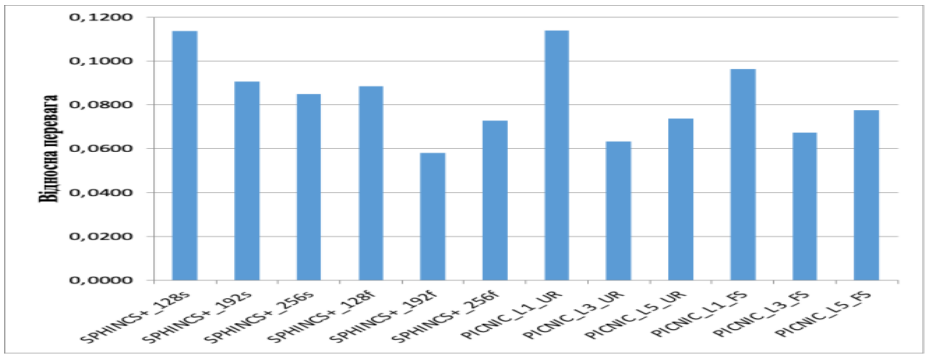


Рисунок 2 - Гістограма загальної відносної переваги алгоритмів ЕП з урахуванням вагових коефіцієнтів характеристик

5.Висновок

Сучасні постквантові стандарти ЕП, АСШ і ПІК відповідають суворим вимогам щодо безпеки інформації, техніко-економічних і техніко-експлуатаційних характеристик, що реалізовані як у міжнародних, так і в національних стандартах.

6. Список літератури

[1] National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems (США).

[2] Crystals-Dilithium. [Електронний ресурс]. URL: https://pq-crystals.org/dilithium/index.shtml (дата звернення: 08.05.2023).

[3] Falcon: Fast-Fourier Lattice-based Compact Signatures over NTRU Specification v1.2 — 01/10/2020. Pierre-Alain Fouque, Jeffrey Hoffstein, Paul Kirchner.]. URL: https://falcon-sign.info/falcon.pdf (дата звернення: 08.05.2023).

[4] National Institute of Standards and Technology. (2019). NIST Special Publication 800-88 Rev. 1: Guidelines for Media Sanitization. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf (дата звернення: 08.05.2023).

[5] ДСТУ 8961:2019 Інформаційні технології. Криптографічний захист інформації. Алгоритми асиметричного шифрування та інкапсуляції ключів. [Чинний від 2021-01-01].

[6] Проєкт стандарту «Вершина».

[7] Проєкт стандарту «Сокіл».

[8] NIST IR 8413. Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process. URL: https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8413.pdf (дата звернення: 08.05.2023).