МІЖНАРОДНИЙ ГУМАНІТАРНИЙ УНІВЕРСИТЕТ

Факультет кібербезпеки, програмної інженерії та комп'ютерних наук

Кафедра комп'ютерної інженерії та інноваційних технологій

Пояснювальна записка

до кваліфікаційної роботи
другого (магістерського) рівня

на тему **ДОСЛІДЖЕННЯ СХЕМ ЕЛЕКТРОННОГО ПІДПИСУ**

Виконав: студент 2 курсу, групи КТК-2.1
спеціальності
125 Кібербезпека
Сербин Д. В.
Керівник Онацький О. В.
Рецензент Соловська Т. М.

Одеса – 2023

ДОВІДКА

кафедри КІ та ІТ про виконану магістерську роботу
студента 2 курсу ФКПІ та КН групи КТК-2.1
Сербина Дмитра Віталійовича

на тему Дослідження схем електронного підпису

Висновок нормоконтролера пояснювальна записка до кваліфікаційної роботи виконана з незначними порушеннями ДСТУ. Оформлено згідно вимог внутрішнього положення НТУ.

Нормоконтролер к.т.н., доцент (науковий ступінь, вчене звання) (підпис, дата) В.В. Педаш (і. б. прізвище)

Висновок відповідального за перевірку на наявність плагіату згідно з сертифікатом ID 1015709274 унікальність роботи підтверджено.

Відповідальна особа к.т.н., доц. каф. КІ та ІТ (науковий ступінь, вчене звання) (підпис, дата) В.В. Педаш (і. б. прізвище)

Попередня експертиза (захист) магістерської роботи

студ. Сербин Д. В. проведена "15" грудня 2023 р.

Висновки Виконання завдання на МР відповідає завданню, усі пункти виконано якісно та згідно вимог до оформлення. Оригінальність: запропоновано модифікацію ЕП Кібера – Рюпеля на основі еліптичних кривих. Магістерська робота відповідає вимогам до ВКР за заявленою спеціальністю 125 Кібербезпека та може бути рекомендована до захисту в ДЕК.

Члени комісії (підпис, дата) к.т.н, доц. Тіора І.В. (науковий ступінь, вчене звання, прізвище і.б.)

(підпис, дата) к.т.н., доц. Педаш В.В. (науковий ступінь, вчене звання, прізвище і.б.)

(підпис, дата) викл. каф. КІ та ІТ Швець О.В. (науковий ступінь, вчене звання, прізвище і.б.)

ВІДГУК КЕРІВНИКА

магістерської роботи студента Сербина Д. В.
на тему: «Дослідження схем електронного підпису»

Магістерська робота присвячена актуальній темі аналізу методів побудови схем електронного підпису. У цій роботі подано детальну характеристику основних принципів побудови електронного підпису.

Розвиток глобальних комунікацій в діловому і повсякденному житті привів до появи нової області взаємовідносин, предметом яких є електронний обмін даними. Проблема збереження електронних документів від копіювання, модифікації і підробки вимагає для свого вирішення засобів і методів захисту.

Одним з поширених в світі засобів такого захисту є електронний підпис, який забезпечує автентичність повідомлення та автентифікацію власника електронного підпису.

У магістерській роботі розглянуто методи побудови схем електронного підпису, приведені опис і розрахунки схем. Для аналізу схем електронного підпису були обрані схеми: RSA, Ель-Гамаля, Шнорра, DSA, ДСТУ 4145-2002, Ніберга-Рюпеля. Для розрахунків були обрані схеми електронного підпису: RSA, Ель-Гамаля, Шнорра, DSA.

У роботі запропоновано модифікацію електронного підпису Ніберга-Рюпеля на еліптичних кривих. Визначено коректність підпису та приклад розрахунку. Основними перевагами підпису є: набагато менша довжина ключа в порівнянні з класичною версію підпису Ніберга-Рюпеля; швидкодія програмної й апаратної реалізації; дозволяє використовувати підпис в інфраструктурах з відкритими ключами.

Студент Сербина Д. В. показав добру теоретичну підготовку, вміння самостійно вирішувати поставлені завдання та грамотно обґрунтовувати їх з технічної сторони. Зміст пояснювальної записки написано ясно й грамотно. Графічна частина роботи виконана добре.

Робота студента Сербина Д. В. відповідає вимогам щодо кваліфікаційних робіт магістерського рівня та заслуговує оцінки «відмінно».

Студент Сербина Д. В. заслуговує присвоєння кваліфікації магістра з кібербезпеки за заявленою спеціальністю 125 Кібербезпека.

Керівник
к.т.н., доцент кафедри КІ та ІТ О.В. Онацький

ВІДГУК КЕРІВНИКА

магістерської роботи студента Сербина Д. В.
на тему: «Дослідження схем електронного підпису»

Магістерська робота присвячена актуальній темі аналізу методів побудови схем електронного підпису. У цій роботі подано детальну характеристику основних принципів побудови електронного підпису.

Розвиток глобальних комунікацій в діловому і повсякденному житті привів до появи нової області взаємовідносин, предметом яких є електронний обмін даними. Проблема збереження електронних документів від копіювання, модифікації і підробки вимагає для свого вирішення засобів і методів захисту.

Одним з поширених в світі засобів такого захисту є електронний підпис, який забезпечує автентичність повідомлення та автентифікацію власника електронного підпису.

У магістерській роботі розглянуто методи побудови схем електронного підпису, приведені опис і розрахунки схем. Для аналізу схем електронного підпису були обрані схеми: RSA, Ель-Гамаля, Шнорра, DSA, ДСТУ 4145-2002, Ніберга-Рюпеля. Для розрахунків були обрані схеми електронного підпису: RSA, Ель-Гамаля, Шнорра, DSA.

У роботі запропоновано модифікацію електронного підпису Ніберга-Рюпеля на еліптичних кривих. Визначено коректність підпису та приклад розрахунку. Основними перевагами підпису є: набагато менша довжина ключа в порівнянні з класичною версію підпису Ніберга-Рюпеля; швидкодія програмної й апаратної реалізації; дозволяє використовувати підпис в інфраструктурах з відкритими ключами.

Студент Сербина Д. В. показав добру теоретичну підготовку, вміння самостійно вирішувати поставлені завдання та грамотно обґрунтовувати їх з технічної сторони. Зміст пояснювальної записки написано ясно й грамотно. Графічна частина роботи виконана добре.

Робота студента Сербина Д. В. відповідає вимогам щодо кваліфікаційних робіт магістерського рівня та заслуговує оцінки «відмінно».

Студент Сербина Д. В. заслуговує присвоєння кваліфікації магістра з кібербезпеки за заявленою спеціальністю 125 Кібербезпека.

Керівник
к.т.н., доцент кафедри КІ та ІТ О.В. Онацький

РЕЦЕНЗІЯ

на магістерську роботу студента Сербина Д. В.
з теми: «Дослідження схем електронного підпису»

Магістерська робота виконана на 65 с. текстової частини, яка містить відповідні розділи згідно з завданням на магістерську роботу. Робота складається з чотирьох основних розділів, вступу, висновків та рекомендації, переліку джерел посилання та трьох додатків. У вступі автор теми обґрунтовує вибір теми та її актуальність.

У магістерській роботі розглянуто методи побудови схем еліптичного підпису, приведені опис і розрахунки схем. Автор за допомогою вітчизняної та зарубіжної літератури розкрив зміст проблеми, висловив власну думку щодо досліджуваної проблеми, доказав достатню практичну та теоретичну підготовку.

Для розрахунків та аналізу були обрані такі схеми електронного підпису: RSA, Ель-Гамаля, Шнорра, DSA, ДСТУ 4145-2002, Ніберга-Рюпеля.

У роботі запропоновано модифікацію електронного підпису Ніберга-Рюпеля на еліптичних кривих. Визначено коректність підпису, приклад розрахунку та основні переваги підпису. Матеріали магістерської роботи були опубліковані у виді тези доповіді на IV Міжнародній науково-практичній конференції «MODERN RESEARCH IN SCIENCE AND EDUCATION» 7-9.12.2023 р. Чикаго, США. Копія сертифіката участі та матеріали конференції представлені у додатках Б, В.

Текстова частина магістерської роботи викладена послідовно, чітко, технічно та грамотно. До недоліків магістерської роботи можна віднести:

– немає суттєвих пояснень деяких формул;

– у роботі не повністю розкрито поняття – відкрита функція надмірності.

В цілому магістерська робота студента Сербина Д. В. відповідає вимогам щодо кваліфікаційних робіт магістерського рівня, зазначені недоліки не знижують якість виконаної роботи і її можна оцінити на «відмінно».

Студент Сербина Д. В. заслуговує присвоєння кваліфікації магістра з кібербезпеки за заявленою спеціальністю 125 Кібербезпека.

Рецензент, Соловська І.М.

к.н., доц.
каф. КН

UNICHECK
by Turnitin

Ім'я користувача:
Анна Серединко

Дата перевірки:
20.12.2023 10:07:12 EET

Дата звіту:
20.12.2023 11:10:20 EET

ID перевірки:
1016024117

Тип перевірки:
Doc vs Internet + Library

ID користувача:
100001433

Назва документа: Сербин Д.В. МР_125_11

Кількість сторінок: 49 Кількість слів: 11506 Кількість символів: 79065 Розмір файлу: 1.35 MB ID файлу: 1015709274

29.8%
Схожість

Найбільша схожість: 20.1% з Інтернет-джерелом (https://dut.edu.ua/firefox/l_491_94183247.pdf)

29.8% Джерела з Інтернету | 622 ..... Сторінка 51

0.33% Джерела з Бібліотеки | 4 ..... Сторінка 56

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

5.68%
Вилучень

Деякі джерела вилучено автоматично (фільтри вилучення: кількість знайдених слів є меншою за 8 слів та 0%)

5.39% Вилучення з Інтернету | 314 ..... Сторінка 57

0.72% Вилученого тексту з Бібліотеки | 40 ..... Сторінка 58

Модифікації

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

Замінені символи | 290

РЕФЕРАТ

Текстова частина магістерської роботи: 65 с., 12 рисунок, 1 таблиця, 3 додатка, 12 джерел.

ЕЛЕКТРОННИЙ ПІДПИС, КВАЛІФІКОВАНИЙ ЕЛЕКТРОННИЙ ПІДПИС, ЕЛЕКТРОННІ ДАНІ, СЕРТИФІКАТ ВІДКРИТОГО КЛЮЧА, ХЕШ–ФУНКЦІЇ, ЕЛІПТИЧНІ КРИВІ.

Об'єкт дослідження – схеми електронного підпису.

Мета роботи – дослідження методів побудови схем електронного підпису.

Метод дослідження – аналітичний з використання комп'ютерних технологій.

У магістерської роботі проведено дослідження методів побудови схем електронного підпису, приведені опис і розрахунки схем. Виконано порівняльна характеристика та аналіз схем електронного підпису.

Запропоновано модифікація електронного підпису Ніберга-Рюпеля на основі еліптичних кривих. Визначено коректність та основні переваги підпису з відновленням повідомлення.

ABSTRACT

The text part of the master's thesis: 65 pp., 12 figures, 1 table, 3 appendices, 12 sources.

ELECTRONIC SIGNATURE, QUALIFIED ELECTRONIC SIGNATURE, ELECTRONIC DATA, PUBLIC KEY CERTIFICATE, HASH FUNCTIONS, ELLIPTIC CURVES.

The object of research is electronic signature schemes.

The purpose of the work is to research the methods of constructing electronic signature schemes.

The research method is analytical with the use of computer technologies.

In the master's work, the methods of constructing electronic signature schemes were studied, the description and calculations of the schemes were given. Comparative characteristics and analysis of electronic signature schemes were performed.

A modification of the Nyrberg-Rueppel message recovery signature based on elliptic curves is proposed. The correctness and main advantages of the signature with message recovery have been determined.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ ТА УМОВНИХ ПОЗНАК

ЕП – Електронний підпис

ЕЦП – Електронний цифровий підпис

УЕП – Удосконалений електронний підпис

КЕП – Кваліфікований електронний підпис

ЕД – Електронний документ

DSA – Digital Signature Algorithm – Алгоритм цифрового підпису

DSS – Digital Signature Standards – Стандарт цифрового підпису

FIPS – Federal Information Processing Standards – Федеральні стандарти обробки інформації

ECDLP – Elliptic Curve Discrete Logarithm Problem – Задача дискретного логарифмування еліптичної кривої

DLP – Discrete Logarithm Problem – Проблема дискретного логарифмування

ПФЧ – Проблема факторизації цілих чисел

ВСТУП

Розвиток глобальних комунікацій у бізнесі та повсякденному житті породив новий аспект взаємодій – електронний обмін даними. У цьому обміні беруть участь державні органи, комерційні та некомерційні установи, а також громадяни у рамках офіційних та особистих відносин.

Проблема забезпечення недоступності електронних документів для копіювання, модифікації та підробки потребує використання специфічних засобів і методів захисту. Одним із широко використовуваних засобів захисту є електронний цифровий підпис (ЕЦП), який гарантує автентичність повідомлення та відсутність можливості використання особистого ключа (підтвердження власника цифрового підпису). За допомогою спеціального програмного забезпечення ЕЦП підтверджує достовірність інформації в документі, його реквізитів та факту підписання.

У роботі розглядаються методи створення ЕЦП та питання їх впровадження. ЕЦП є обов'язковим елементом електронного документа, який дозволяє визначити відсутність спотворення інформації в електронному документі від моменту формування ЕЦП і перевірити відповідність підпису власнику сертифіката ключа ЕЦП.

Використання електронного цифрового підпису має ряд переваг, таких як:

– заміна традиційної печатки та підпису під час безпаперового документообігу;

– покращення і зменшення вартості процедур підготовки, доставки, обліку і зберігання документів, забезпечення достовірності документації;

– суттєве зменшення часу переміщення документів, прискорення і полегшення процесу візування документів кількома особами;

– створення корпоративної системи обміну електронними документами;

– забезпечення цілісності - гарантія того, що інформація залишається в своєму початковому вигляді, тобто при її зберіганні або передачі не має несанкціонованих змін.

Об’єктом дослідження в роботі є електронний підпис і криптографічні перетворення, які застосовується для формування та перевірки підпису.

Метою магістерської роботи є дослідження методів побудови схем електронного підпису та запропонувати модифікацію електронного підпису Ніберга-Рюпеля на основі еліптичних кривих, визначити коректність підпису та основні переваги даної модифікації.

1 ЕЛЕКТРОННІ ДОВІРЧІ ПОСЛУГИ ТА ЇХ ЗАСТОСУВАННЯ

1.1 Огляд нормативно-правових документів з питань електронного підпису

Закон України «Про електронні довірчі послуги» (Відомості Верховної Ради (ВВР), 2017, № 45, ст.400) [1] визначає правові та організаційні засади надання електронних довірчих послуг, у тому числі транскордонних, права та обов'язки суб'єктів правових відносин у сфері електронних довірчих послуг, порядок здійснення державного нагляду (контролю) за дотриманням вимог законодавства у сфері електронних довірчих послуг, а також правові та організаційні засади здійснення електронної ідентифікації.

Метою закону [1] є врегулювання відносин у сферах надання електронних довірчих послуг та електронної ідентифікації.

Закон України «Про електронні довірчі послуги» [1] визначає правовий статус електронного цифрового підпису та регулює відносини, що виникають під час використання електронного цифрового підпису. У законі [1] визначено такі терміни, як:

– електронний підпис - електронні дані, які додаються підписувачем до інших електронних даних або логічно з ними пов'язуються і використовуються ним як підпис;

– кваліфікований електронний підпис - удосконалений електронний підпис, який створюється з використанням засобу кваліфікованого електронного підпису і базується на кваліфікованому сертифікаті відкритого ключа;

– перевірка - процес засвідчення справжності і підтвердження того, що електронний підпис чи печатка є дійсними;

– підписувач - фізична особа, яка створює електронний підпис;

– удосконалений електронний підпис - електронний підпис, створений за результатом криптографічного перетворення електронних даних, з якими пов'язаний цей електронний підпис, з використанням засобу удосконаленого електронного підпису та особистого ключа, однозначно пов'язаного з підписувачем, і який дає змогу здійснити електронну ідентифікацію підписувача та виявити порушення цілісності електронних даних, з якими пов'язаний цей електронний підпис.

В Україні уведено в дію та застосовується власні стандарти та гармонізовані [2, 3], які представлені на рис. 1.1:

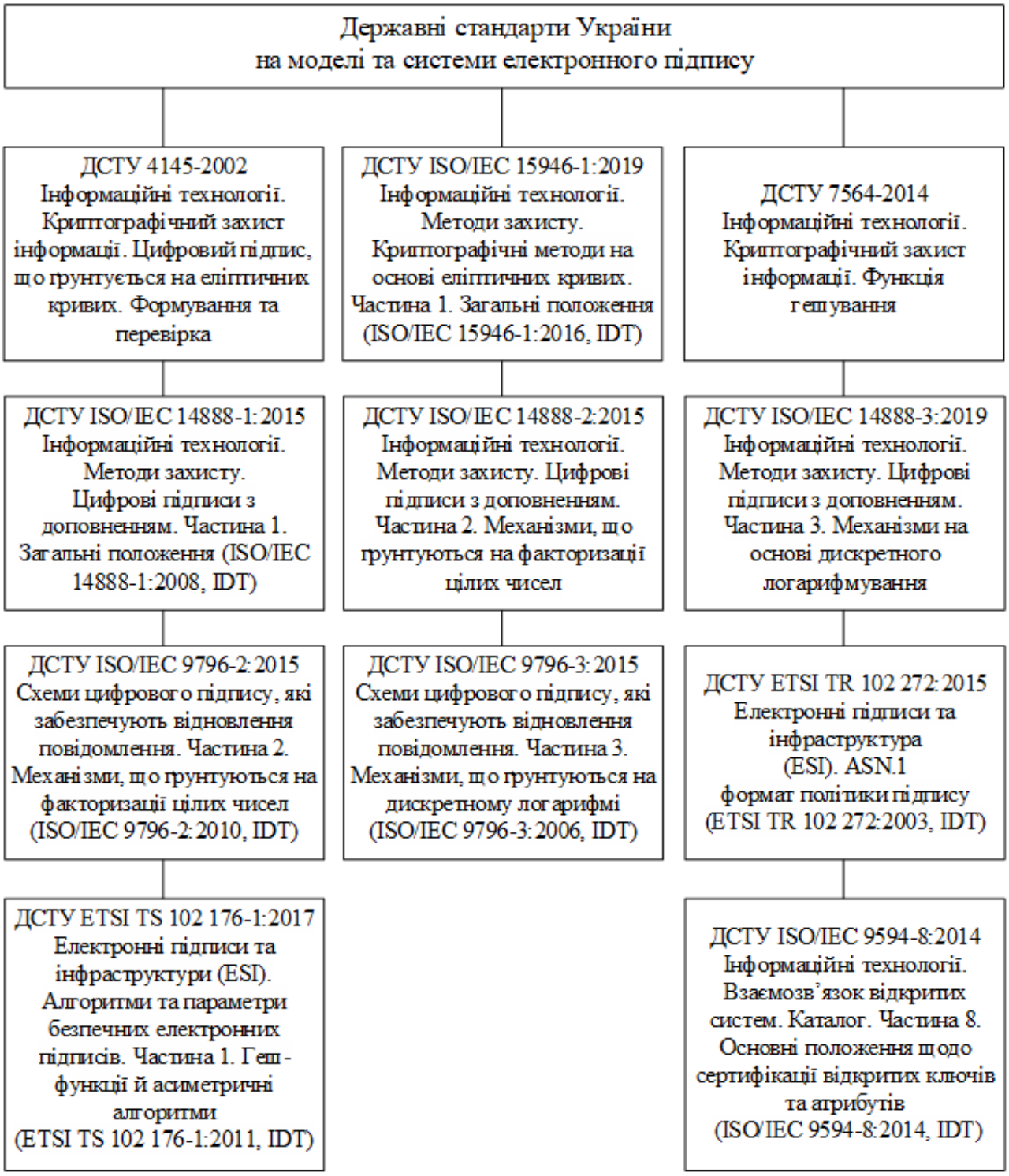

Рисунок 1.1 – Державні стандарти України на моделі та системи електронного підпису

З 2020 року звичайній електронний підпис був замінений на кваліфікований електронний підпис так як він є найбільш захищеним видом електронного підпису та є рівнозначним особистому підпису від руки.

1.2 Вимоги до системи електронного підпису України

В Україні впроваджується ієрархічна система електронного підпису. На рис. 1.2 представлена узагальнена схема інформаційної структури відкритих ключів України [2]. Основними компонентами структури системи ЕП в Україні є центральний засвідчувальний орган, засвідчувальні центри центральних органів виконавчої влади, акредитовані центри сертифікації ключів, центри сертифікації ключів (ЦСК), відокремлені пункти реєстрації ключів, заявники (юридичні та фізичні особи - користувачі), та контролюючий орган.

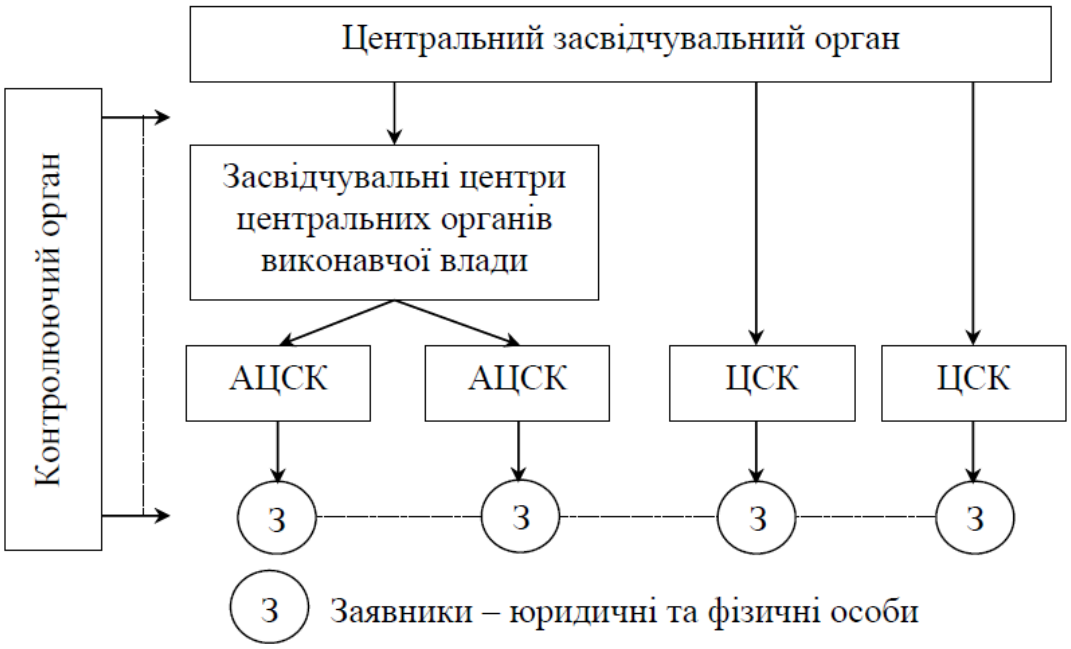

Рисунок 1.2 – Узагальнена схема інформаційної структури відкритих ключів України

Центральний засвідчувальний орган (ЦЗО) в національній системі ЕП України виступає як основний центр сертифікації відкритих ключів. Його завдання включає обслуговування посилених сертифікатів ключів центрів в Україні, акредитацію центрів сертифікації ключів та засвідчувальних центрів відповідно до законодавства України. Функції ЦЗО включають:

– акредитацію центрів, видачу, переоформлення та анулювання відповідних

свідоцтв;

– формування та видачу центрами сертифікатів ключів;

– реєстрацію центрів;

– блокування, скасування та поновлення сертифікатів ключів центрів;

– ведення реєстру суб'єктів, які надають послуги з електронним підписом;

– забезпечення цілодобового доступу до сертифікатів ключів центрів

– приймає для зберігання сертифікати ключів, їх реєстри та документовану інформацію, що підлягає обов'язковій передачі від центрів до ЦЗО у випадку припинення їх діяльності;

– приймає на зберігання сертифікати ключів, їх реєстри та документовану інформацію, яка підлягає обов’язковій передачі від центрів до ЦЗО в разі припинення їх діяльності;

– розглядає заявки та скарги на неправильне функціонування центрів та подає відповідні пропозиції контролюючому органу;

– інформує контролюючий орган про обставини, що ускладнюють діяльність ЦЗО.

Акредитований центр сертифікації ключів (АЦСК) забезпечує своїм користувачам якісні послуги у сфері електронного документообігу та використання ЕП. Його функції включають:

– обслуговування сертифікатів відкритих ключів абонентів;

– реєстрацію абонентів;

– надання абонентам засобів ЕП та шифрування даних;

– сертифікацію відкритих ключів абонентів;

– розповсюдження сертифікатів;

– управління статусом сертифікатів та розповсюдження інформації про їх стан;

– надання послуг з фіксації часу та інші послуги.

Відокремлені пункти реєстрації є відособленими підрозділами, які не мають юридичного статусу, і здійснюють функції реєстрації абонентів та їх обслуговування на відповідній території. Вони мають право укладати договори про надання послуг ЕП. Контроль за їх діяльністю здійснюється центром сертифікації ключів.

Користувачі (абоненти) ЕП мають ряд прав, включаючи отримання якісних послуг, отримання сертифіката центру, отримання списку відкликаних серти

Кабінет Міністрів України визначає порядок використання електронних підписів органами державної влади, органами місцевого самоврядування,

підприємствами, установами та організаціями державної форми власності. Порядок застосування електронних підписів у банківській сфері визначається Національним банком України.

Відокремлені пункти реєстрації заявників представляють собою самостійні підрозділи, які не мають юридичного статусу, і виконують функції центру реєстрації абонентів та їх подальшого обслуговування на відповідній території. Вони мають право укладати договори щодо надання послуг ЕП. Непряме керування цими підрозділами здійснюється центром сертифікації ключів.

Користувачі (абоненти) ЕП мають такі права:

– отримувати якісні послуги ЕП вчасно;

– отримувати сертифікат від центру;

– отримувати список відкликаних сертифікатів, сформований центром;

– використовувати сертифікат центру для перевірки автентичності ЕП сертифікатів, сформованих центром;

– використовувати список відкликаних сертифікатів для перевірки статусу свого сертифіката та сертифікатів інших абонентів;

– створювати відкриті та особисті ключі на своєму робочому місці, використовуючи надійний метод ЕП;

– отримувати інформацію щодо діяльності центру та послуг ЕП;

– вимагати скасування, блокування або відновлення свого сертифіката ключа.

Контролюючий орган, яким є Державна служба спеціального зв’язку та захисту інформації України, виконує функції перевірки відповідності законодавства центрального засвідчувального органу, засвідчувального центру центральних органів виконавчої влади, акредитованих центрів сертифікації ключів та центрів сертифікації ключів.

1.3 Основні характеристики електронного підпису

Згідно з українським законодавством [1, 2], електронні підписи можуть бути наступних видів:

а) ЕЦП – простий електронний цифровий підпис, для якого характерний низький рівень довіри. У листопаді 2020 року даний тип підпису втратив чинність та був остаточно замінений на кваліфікований електронний підпис;

б) удосконалений електронний підпис (УЕП) – створений з використанням криптографічного перетворення даних. У випадку, якщо в документ, підписаний

УЕП, відбулося втручання, це вдасться виявити;

в) кваліфікований електронний підпис (КЕП) – є аналогічним до УЕП, але додатково відповідає наступним критеріям:

– в основі такого підпису лежить сертифікат відкритого ключа, що є кваліфікованим;

– програмне забезпечення та обладнання, за допомогою якого він здійснюється, задовольняє додаткові вимоги.

Завдяки переліченим характеристикам саме КЕП є найбільш захищеним видом електронного підпису та є рівнозначним особистому підпису від руки. Наявність у контрагентів КЕП дозволяє їм повною мірою використовувати сервіси електронного документообігу під час укладання угод.

Кваліфікований електронний підпис – це електронний підпис, що створюється за допомогою засобу КЕП та має за основу кваліфікований сертифікат відкритого ключа.

Такий підпис видають на спеціальних флеш-накопичувачах, що називаються токенами (апаратними ключами). Кожен токен затверджений Держслужбою спецзв'язку та захисту інформації, має власний інвентарний номер та обмежену кількість разів введення паролю (зазвичай їх 7).

Скопіювати ключ з токена неможливо. Коли відбувається підписання документа, сервіс електронного документообігу зчитує не лише файл ключа, а й перевіряє його носій. Це гарантує 100% захищеність та унікальність електронного підпису особи.

Ефективність КЕП забезпечується двома його складовими:

– особистим ключем, який зберігається у його власника (підписувача);

– відкритим ключем, що публікується у спеціалізованому довіднику чи перебуває у загальному доступі та необхідний для того, щоб підтвердити особу підписувача.

Власник може використовувати свій КЕП, поки діє кваліфікаційний сертифікат відкритого ключа. Точний строк дії встановлює акредитований центр сертифікації ключів, в якому було отримано електронний підпис, та досягає двох років.

Одним із різновидів КЕП є Mobile ID – спосіб ідентифікації користувача за допомогою його смартфону.

2 ЗАГАЛЬНА ХАРАКТЕРИСТИКА ІСНУЮЧИХ ЕЛЕКТРОННИХ ПІДПИСІВ

2.1 Методи побудови електронних підписів

Існує кілька методів побудови ЕЦП, а саме [3]:

а) Шифрування електронного документа (ЕД) на основі симетричних алгоритмів. Ця схема передбачає наявність у системі третьої особи - арбітра, який користується довірою обох сторін. Авторизацією документа у цій схемі є факт зашифровки ЕД секретним ключем і передача його арбітру.

Переваги:

– стійкість симетричних схем випливає із стійкості використовуваних блокових шифрів, надійність яких також добре вивчена;

– якщо стійкість шифру недостатня, його легко замінити іншим.

Недоліки:

– потрібно підписувати окремо кожен біт інформації, що значно збільшує підпис (він може стати довшим за документ на порядок);

– згенеровані для підпису ключі можна використовувати лише один раз, тому що після підписування розкривається половина секретний ключ.

б) Використання асиметричних алгоритмів шифрування. Фактом підписання документа є зашифрування на секретному ключі відправника.

Вони більш поширені та широко застосовуваними у житті. Якщо в асиметричних криптосистемах шифрування виконують на відкритому ключі, а дешифрування – на закритому ключі одержувача, то в схемах ЕЦП підпис роблять за допомогою закритого ключа, а перевірку – за допомогою відкритого ключа користувача, що передає повідомлення (схема ЕЦП змінює ролі секретних та відкритих ключів). Створити легітимний цифровий підпис без володіння закритим ключем має бути обчислювально складно.

Недоліки:

– асиметричні метод побудови ЕЦП базуються, як і на асиметричне шифрування, на обчислювально складних задачах (завдання дискретного логарифмування або завдання факторизації), складність яких суворо математично не доведено. Обчислення можуть проводитись у групі точок еліптичних кривих та в полях Галуа (наприклад, DSA);

– для збільшення криптостійкості треба збільшувати довжину ключів, що

змушує переписувати програми, що реалізують схеми, і навіть перепроектувати апаратуру.

Крім цього, існують інші різновиди цифрових підписів (груповий підпис, незаперечний підпис, довірений підпис, сліпий підпис).

в) Розвитком попередньої ідеї стала найбільш поширена схема ЕЦП – шифрування остаточного результату обробки ЕД хеш-функцією за допомогою асиметричного алгоритму (рис. 2.1).

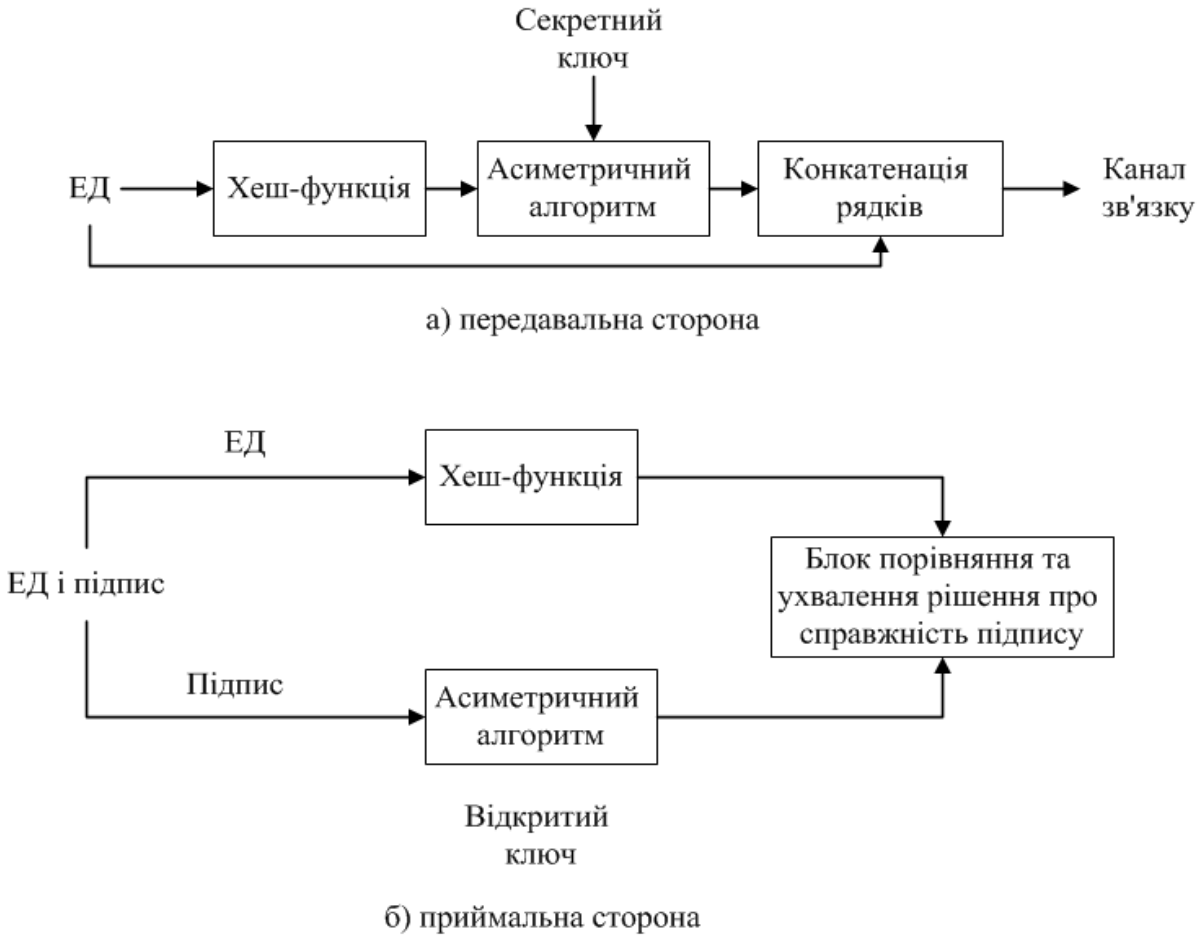

Рисунок 2.1 – Структурна схема побудови ЕП

Документи, що підписуються, мають різну, часто велику довжину, тому в схемах ЕЦП зручно використовувати не сам документ, а його хеш. Хеш обчислюють за допомогою криптографічних хеш-функцій, що гарантує виявлення змін документа під час перевірки підпису.

Використання хеш-функцій дає переваги:

– хеш документ має набагато меншу довжину, ніж сам документ, а алгоритми обчислення хеш швидше за алгоритми ЕЦП. Тому формувати хеш документа та підписувати його набагато швидше, ніж підписувати сам документ;

– хеш-функцію можна використовувати для перетворення довільного вхідного тексту на відповідний формат;

– без використання хеш-функції великий документ у деяких схемах треба ділити на менші блоки, а потім підписувати. В цьому випадку при верифікації неможливо визначити, чи всі блоки отримані і чи правильно вони порядку. Хешування знімає ці питання.

Примітка 1: хешування не є обов'язковим для цифрового підпису, а сама функція не є частиною алгоритму ЕЦП, тому хеш-функція може використовуватися будь-яка або взагалі не використовуватися.

2.2 Основні поняття та застосування хеш-функцій

Хеш-функція, або геш-функція, визначається як функція, яка змінює вхідні дані будь-якого розміру на дані фіксованого розміру, часто великого.

Хешування представляє собою процес перетворення вхідного масиву даних будь-якої довжини у бітовий рядок фіксованої довжини. Ці перетворення також називаються хеш-функціями або функціями згортання, а їх результати – хеш, хеш-код, хеш-сума або дайджест повідомлення.

Широке застосування хеш-функцій спостерігається при організації обміну документами з електронно-цифровим підписом. У цьому випадку хешується файл, який підписується, забезпечуючи отримувачеві певність щодо його автентичності.

Хоча формально хеш-функція не входить в структуру електронного ключа, вона може бути фіксована у флеш-пам'яті апаратних засобів, таких як, наприклад, eToken.

Електронний підпис включає в себе шифрування файлу за допомогою відкритого та закритого ключів.

Хеш-функція дозволяє ефективно оптимізувати алгоритми електронного підпису, шифруючи лише хеш, а не вихідний документ. Це підвищує швидкість обробки файлів та забезпечує ефективні механізми захисту електронного підпису. Також хеш-функція дозволяє підписувати різні типи даних, не обмежуючись лише текстом.

Крім того, хеш-функція використовується для електронної ідентифікації та перевірки цілісності даних. У багатьох випадках вона служить засобом забезпечення безпеки при обміні інформацією.

Згаданий Закон України "Про електронні довірчі послуги" [1] визначає

важливий правовий статус електронного цифрового підпису та регулює взаємовідносини, пов'язані з його використанням. Визначення термінів, таких як "хеш-функція", допомагає уточнити та стандартизувати термінологію у сфері електронних довірчих послуг. У контексті електронного підпису, де безпека та вірогідність грають ключову роль, хеш-функції визначаються як важливий інструмент для створення та перевірки цифрових підписів. Вони сприяють ефективній перевірці того, чи змінювалися дані під час їхнього передавання або зберігання.

Таким чином, використання хеш-функцій у сфері криптографічного захисту даних та електронних підписів є необхідним елементом для забезпечення конфіденційності, цілісності та автентичності інформації, що обмінюється в цифровому середовищі.

Алгоритми хеш-функцій будуються за принципом перетворення інформації M. При цьому, якщо $l_M > l_h$, в процесі перетворення проводиться стиснення прообразу M в образ $h(M)$. Якщо $l_M < l_h$, у процесі хешування M розтягується до довжини l_h. Таким чином, першим основним принципом обчислення $H(M)$ є перетворення M з використанням співвідношень.

Оскільки зазвичай алгоритми хешування обробляють вхідне повідомлення по блоках фіксованої довжини, вони додають деяку незначну частину до повідомлення (“розширення повідомлення”), щоб його довжина стала кратною довжиною оброблюваного блоку. При цьому в ряді випадків існує потенційна можливість отримання одних і тих же значень хеш-функції інформації, що відрізняється довжиною. Це може статися, якщо при розширенні повідомлення додається незначна частина (можливо, прогалини, нулі), яка може бути інтерпретована як частина повідомлення. Для захисту від цієї загрози до повідомлення M може бути додано значення довжини вихідної Така технологія отримала назву MD посилення. Внаслідок її застосування вихідне значення M, що хешується, замінюється перетвореним значенням M_n:

$$M_n = \{M, l_M\} = M.$$

Отже, другим важливим принципом є побудова хеш-функції як:

$$h = H(V_H, M) = H(V_H, \{M, l_M\}),$$

як функції від вихідної інформації M та її довжини l_M одночасно.

Третім основним принципом, що забезпечує виконання вимог до хеш-функції, є застосування односпрямованої (нелінійної) функції над кожним блоком вихідної інформації M. В результаті такого перетворення при $l_M > l_h$ відбувається стиснення M у h, а при $l_M < l_h$ - розтяг M до довжини l_h.

Основою функції хешування є її ядро, являє собою нелінійну функцію, яка послідовно застосовується до кожного блоку інформації (рис. 2.2). Входами функції H є блок інформації, що хешується, і значення h_{I-1} хеш-функції для M_{I-1} блоку, причому як h_0, як правило, використовується початкове значення V_H. Як випливає з наведеного, хеш-функцією h інформації M є значення h_n хеш-функції останнього блоку M_n:

$$h(V_H, M_{n-1}) = f(M_n, h_{n-1}).$$

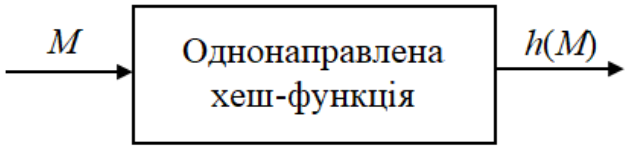

Рисунок 2.2 − Структура алгоритму хешування

Усі створені на даний момент функції хешування базуються на використанні:

1) різних бітових нелінійних функцій (наприклад: MD2, MD4, MD5, SHA);

2) блокових симетричних алгоритмів шифрування (наприклад: MDC2, 4);

3) несиметричних алгоритмів шифрування (наприклад, RSA, Ель-Гамаля).

Ідея використання симетричних блокових алгоритмів шифрування як односпрямованої функції хешування полягає в тому, що якщо блоковий алгоритм безпечний, то й односпрямована функція хешування також безпечна. На цьому базується і застосування несиметричних алгоритмів шифрування. Обмежуючим фактором їх застосування є збільшена порівняно з бітовими нелінійними функціями обчислювальна складність і, як наслідок, менша швидкість хешування.

Авжеж, що при виборі тієї чи іншої функції хешування необхідно використовувати обґрунтовані критерії оцінки ефективності та показники якості. Базуючись на, виберемо в як основні приватні показники стійкість проти криптоаналітичних атак, розуміючи під нею обчислювальну складність їх реалізації, а також швидкість хешування. У ряді випадків в якості показників ефективності функції хешування використовують і обсяг програмного забезпечення, необхідного для його реалізації.

2.3 Алгоритми електронного підпису RSA

Математична схема електронного цифрового підпису за алгоритмом RSA була запропонована в 1977 році співробітниками Массачусетського технологічного інституту США. Дана система цифрового підпису стала першим практичним рішенням задачі підпису електронних документів за допомогою криптосистем із відкритим ключем. Процедура обчислення цифрового підпису у цій системі використовує криптографічне перетворення алгоритму RSA [3, 4].

Відповідно до цієї системи цифрового підпису, суб'єкт, який бажає пересилати підписані ним документи, повинен сформувати два ключі алгоритму RSA: відкритий (визначимо K_O) та закритий K_C (визначимо K_C).

Пара значень (K_O, r), яка є відкритим ключем підпису, відправник передає всім можливим одержувачам його повідомлень. Саме ці значення будуть використовуватися для перевірки автентичності та належності відправнику отриманих від нього повідомлень.

Значення K_C зберігається відправником у секреті. Дане значення разом з модулем r є секретним ключем, який використовуватиметься відправником для встановлення підписів під своїми повідомленнями.

Схема використання алгоритму цифрового підпису з урахуванням RSA для обміну двох абонентів підписаними повідомленнями показано на рис. 2.3.

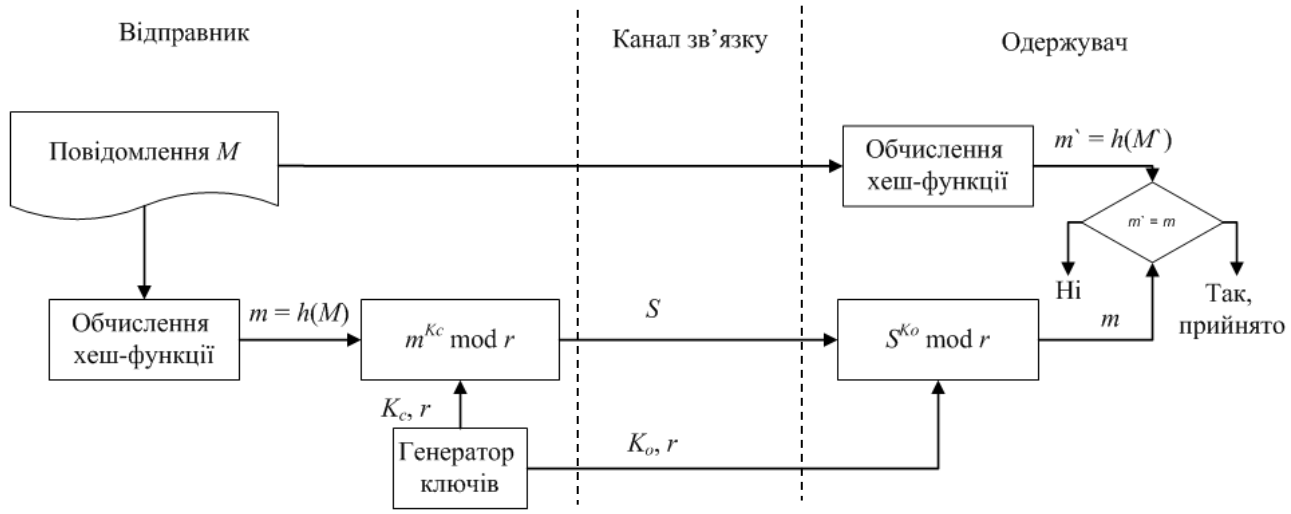

Рисунок 2.3 − Схема використання цифрового підпису на базі RSA

Припустимо, що одержувач вже має у своєму розпорядженні відкритий ключ підпису відправника. Процедура підпису відправником повідомлення M складатиметься з наступних кроків [3]:

1) відправник стискає повідомлення M за допомогою криптографічної хеш-функції h ціле число $m = h(M)$;

2) відправник визначає значення цифрового підпису S для повідомлення M на основі раніше отриманого значення хеш-образу m і значення свого закритого (секретного) ключа підпису K_C. Для цього використовується перетворення, аналогічне до перетворення, що виконується при шифруванні за алгоритмом RSA:

$$S = m^{Kc} \bmod r.$$

Пара (M, S), що є підписане відправником повідомлення, передається одержувачу. Сформувати підпис S міг лише власник закритого ключа K_C.

Процедура перевірки одержувачем справжності повідомлення та належності його відправнику складається з наступних кроків.

Отримувач стискає отримане повідомлення M' за допомогою криптографічної хеш-функції h, ідентичної тій, яка була використана відправником, ціле число m'.

Отримувач виконує розшифрування відкритим ключем K_O відправника дайджесту m оригінального повідомлення, перетворюючи значення підпису S за алгоритмом RSA:

$$m = S^{Ko} \bmod r.$$

3) одержувач порівнює отримані значення m' і m. Якщо ці значення збігаються, тобто

$$S^{Ko} \bmod r = h(M'),$$

то одержувач визнає отримане повідомлення справжнім та належним відправнику.

Фальсифікація повідомлення при його передачі каналом зв'язку можлива тільки при отриманні зловмисником секретного ключа K_C або за рахунок проведення успішної атаки проти використаного для обчислення дайджесту повідомлення хеш-функції. При використанні досить великих значень p і q визначення секретного значення K_C по відкритому ключі (K_O, r) є надзвичайно важким завданням, що відповідає за складністю розкладання модуля r на множники. Використані в реальних додатках хеш-функції мають характеристики,

що роблять атаку проти цифрового підпису практично неможливим.

Є два варіанта використання алгоритму RSA для цифрового підпису перший варіант – алгоритм підпису RSA з відновленням повідомлення.

Нехай користувач A хоче підписати повідомлення M і надіслати його користувачеві B.

Генерація ключів відправника A: збігається із генерацією ключів у алгоритмі RSA. Вибираються два простих великих числа p і q, розрахунок $n = pq$, вибирається число e, взаємно просте з числом $\phi(n) = (p–1)(q–1)$ та обчислюється $d \equiv e^{-1} \pmod{\phi(n)}$ Відкритий ключ пара (n, e) оголошується публічно, d – секретний ключ.

Формування підпису відправником A:

1) Обчислити підпис $S = M^d \pmod{n}$.

2) Передати одержувач B повідомлення та підпис S у вигляді пари (M, S).

Перевірка підпису одержувачем B :

1) На відкритому ключі відправника A знайти $M' = S^e \pmod{n}$.

2) Якщо $M' = M$, то прийняти повідомлення як правильне.

Доказ правильності процедури:

$$M' \equiv S^e \pmod{n} \equiv (M^d)^e \pmod{n} \equiv M \pmod{n}.$$

Приклад електронного підпису RSA. Нехай $p = 31$ і $q = 73$, тоді

$$n = 31 \cdot 73 = 2263;$$
$$\phi(2263) = (31–1)(73–1) = 2160.$$

Нехай задано відкритий ключ $e = 59$ і секретний ключ $d = 659$. У відкритому каналі розміщують значення (59, 2263).

Відправник хоче підписати повідомлення M, для цього використовує відкриту функцію надмірності F, яка є легко оборотною, $F(M) = 273$.

У цьому разі відправник обчислює:

$$S \equiv 273^{659} \pmod{2263} \equiv 2082$$

і формує підписане повідомлення $(M, 2082)$.

Одержувач, маючи підписане повідомлення, обчислює значення функції $F(M) = 273$

$$m' \equiv 2082^{59} \pmod{2263} = 273.$$

Значення $m' = F(M) = 273$ збіглися, тобто підпис є справжній.

Атаки цифрового підпису RSA:

1) Атака з урахуванням відомого відкритого ключа. Перехопивши пару (M, S) і знаючи відкритий ключ відправника, криптоаналітик підбирає інше повідомлення $M_1 = S^e \pmod{n}$. За складністю рішення це еквівалентно дискретному логарифмування. Таке створення противником підпису якогось можливо безглуздого повідомлення називається екзистенційною підробкою. Зазвичай вони марні.

2) Атака на основі відомих підписаних повідомлень. Нехай у руках криптоаналітика дві пари підписи повідомлень (M_1, S_1) та (M_2, S_2), отримані на одному закритому ключі. Якщо $M = M_1M_2$, то $S = S_1S_2 \pmod{n}$. Криптоаналітик посилає одержувачу нову пару (M, S), причому одержувач може вважати її, надісланою істинним власником ключів. Атака називається ще мультиплікативною. Повідомлення x зазвичай немає сенсу.

3) Атака за вибраними повідомленнями також мультиплікативна. Криптоаналітик підбирає два таких відкритих текстів M_1 та xM_2, що $M = M_1M_2$ буде необхідним йому новим документом. Далі він може отримати у законного відправника підписи (M_1, S_1) та (M_2, S_2), а потім конструювати пару (M_1M_2, S_1S_2), видаючи її за підписаний документ відправника. Така атака називається ще селективною, оскільки тут створюється підпис для заздалегідь підібраного повідомлення.

Один із способів протистояти атакам – підписувати хешоване повідомлення та вносити зашумлення.

Другий варіант – звичайний цифровий підпис за схемою RSA.

Формування підпису відправником A:

1) за допомогою криптографічної функції хешування обчислити хеш повідомлення $H(M)$;

2) обчислити підпис $S = H(M)^d \pmod{n}$;

3) передати одержувачу B пару (M, S).

Перевірка підпису одержувачем:

1) на відкритому ключі відправника обчислити $H'(M) = S^e \pmod{n}$;

2) обчислити для надісланого повідомлення M його хеш $H(M)$;

3) перевірка рівності $H(M) = H'(M) \pmod{n}$. Якщо воно правильне, то підпис законний, інакше – незаконний.

Якщо криптоаналітик підготує колізію $H(M_1) = H(M_2)$, то він може дати на підпис повідомлення M_2, а потім підмінити їм, склавши замість пари (M_1, S) пару (M_2, S). Підміна у схемі простого підпису RSA залежить від стійкості алгоритму хешування до колізій.

Недоліки ЕЦП RSA:

1) При виборі ключів слід враховувати численні додаткові умови, що ускладнює процес (невиконання будь-якої з цих умов може призвести до фальсифікації цифрового підпису, що абсолютно неприпустимо при підписанні важливих документів).

2) Для досягнення такого ж рівня криптостійкості, як при шифруванні DES (10^{18}), необхідно використовувати числа порядку 2^{512} (або навіть близько 10^{154}) для кожного ключа, що призводить до значних обчислювальних витрат.

3) ЕЦП RSA вразлива до мультиплікативних атак.

2.4 Електронні підписи на основі алгоритму Ель-Гамаля

Схема Ель-Гамаля [3, 4] – криптосистема з відкритим ключем, заснована на складності обчислення дискретних логарифмів в кінцевому полі . Криптосистема включає алгоритм шифрування і алгоритм цифрового підпису (рис. 2.4).

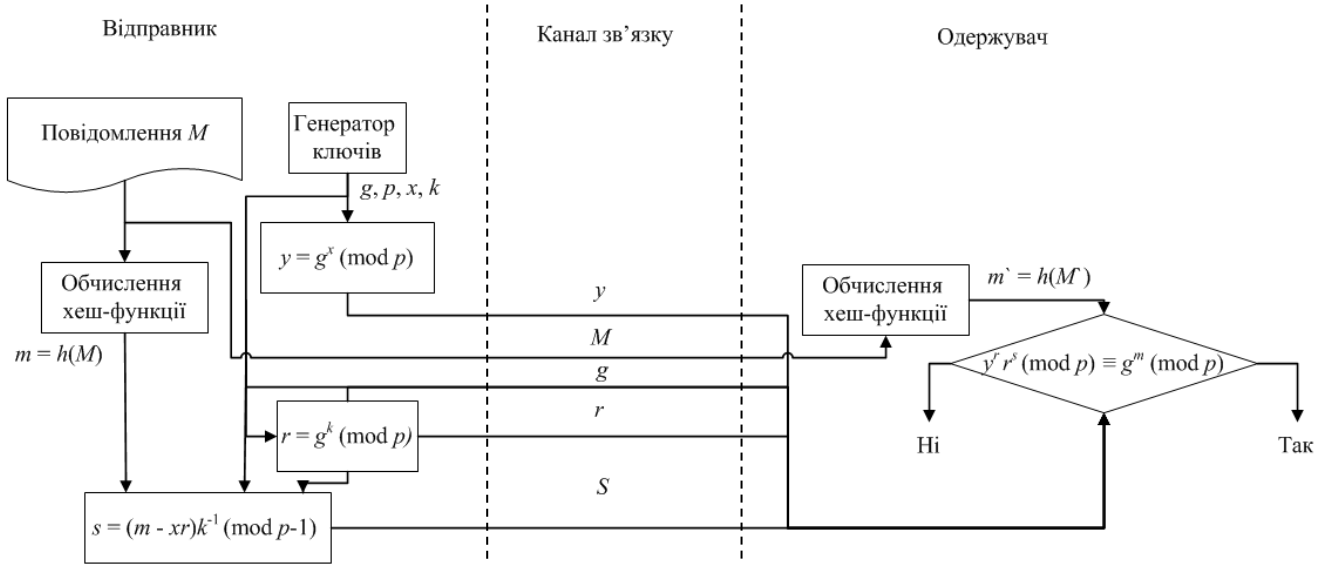

Рисунок 2.4 − Схема використання цифрового підпису на базі Ель-Гамаля

Генерація ключів:

1) генерується випадкове просте число p;

2) вибирається ціле число g - первісний корінь p;

3) вибирається випадкове ціле число x таке, що $(1 < x < p\text{-}1)$;

4) обчислюється $y = g^x \pmod p$;

5) відкритим ключем є (y, g, p), закритим ключем - число x.

Цифровий підпис служить для того, щоб можна було встановити зміни даних і щоб встановити справжність сторони, що підписалася. Отримувач підписаного повідомлення може використовувати цифровий підпис для доказу третій стороні того, що підпис дійсно зроблений стороною, що відправляє. При роботі в режимі підпису передбачається наявність фіксованої хеш-функції $h(\cdot)$, значення якої лежить в інтервалі $(1, p–1)$.

Підпис повідомлень:

Для підпису повідомлення M виконуються такі операції:

1) обчислюється дайджест повідомлення M: $m = h(M)$, (хеш-функція може бути будь яка);

2) вибирається випадкове число $1 < k < p–1$ взаємно просте $p–1$ і обчислюється $r = g^k \bmod p$;

3) обчислюється число $s = (m – xr)k^{–1} \pmod{p–1}$, де $k–1$ це мультиплікативне зворотне k за модулем $p–1$, яке можна знайти, наприклад, за допомогою розширеного алгоритму Евкліда;

4) підписом повідомлення M є пара (r, s).

Перевірка підпису:

Знаючи відкритий ключ (p, g, y), підпис (r, s) повідомлення M перевіряється так:

1) перевіряється здійсненність умов: $0 < r < p$ та $0 < s < p–1$;

2) якщо хоча б одне з них не виконується, то підпис вважається неправильним;

3) обчислюється дайджест $m = h(M)$;

4) підпис вважається вірним, якщо виконується порівняння: $y^r r^s \equiv g^m \pmod p$.

Коректність перевірки:

Розглянутий алгоритм коректний у тому сенсі, що підпис, обчислений за вказаними вище правилами, буде прийнято під час її перевірки.

Перетворюючи визначення s, маємо:

$$m \equiv xr + sk \pmod{p–1}.$$

Далі, з малої теореми Ферма випливає, що

$$g^m \bmod p \equiv (g^{xr} g^{ks}) \bmod p \equiv ((g^x)^r (g^k)^s) \bmod p \equiv (y^r r^s) \bmod p.$$

Приклад електронного підпису Ель-Гамаля. Нехай $p = 23$, $g = 5$, $k = 7$, $h(M) = 3$, $x = 5$.

Відправник обчислює відкритий ключ:

$$Y \equiv 5^7 \pmod{23} \equiv 17.$$

Відправник переходить до обчислення підпису:

$$r \equiv 5^5 \pmod{23} \equiv 20;$$
$$u \equiv (3 - 7 \cdot 20) \bmod (23 - 1) \equiv 17;$$
$$s \equiv (5^{-1} \cdot 17) \bmod (23 - 1) \equiv 21.$$

Формується підписане повідомлення як (M, 20, 21). Підписане повідомлення надсилається одержувачу.

Отримувач перевіряє справжність підпису. Спочатку він обчислює значення хеш-функції $h(M) = 3$, а потім обчислює:

$$(17^{20} \cdot 20^{21}) \pmod{23} \equiv 10;$$
$$5^3 \pmod{23} \equiv 10.$$

Одержувач робить висновок, що підпис є вірним.

Головною перевагою схеми цифрового підпису Ель-Гамаля є можливість виробляти цифрові підписи для великої кількості повідомлень, використовуючи лише один секретний ключ. Щоб зловмиснику підробити підпис, йому потрібно вирішити складні математичні завдання зі знаходженням логарифму в полі . Слід зробити кілька коментарів:

1) випадкове число k має відразу після обчислення підпису знищуватися, тому що якщо зловмисник знає випадкове число k і сам підпис, він легко може знайти секретний ключ за формулою: $x = (m - ks)r^{-1} \pmod{p-1}$ і повністю підробити підпис. Число k має бути випадковим і не повинно дублюватися для різних підписів, отриманих за однакового значення секретного ключа;

2) використання згортки $m = h(M)$ пояснюється тим, що це захищає підпис від перебору повідомлень за відомими зловмисниками значенням підпису.

Приклад: якщо вибрати випадкові числа i, j що задовольняють умовам $0 < i < p–1$, $0 < j < p–1$. НОД $(j, p–1)=1$ і припустити що

$$r = (g^i \cdot y^{-j}) \bmod p;\ s = (r \cdot j^{-1}) \bmod (p–1);$$
$$m = (r \cdot i \cdot j^{-1}) \bmod (p–1),$$

то легко переконатися в тому, що пара (r, s) є вірним цифровим підписом для повідомлення $x = M$.

3) цифровий підпис Ель-Гамалю став прикладом побудови інших підписів, схожих за своїми властивостями. У основі лежить виконання порівняння: $y^A r^B = g^C \pmod p$, у якому трійка (A, B, C) приймає значення однієї з перестановок $\pm r$, $\pm s$ і $\pm m$ за певного вибору знаків. Наприклад, вихідна схема Эль-Гамаля виходить при $A = r$, $B = s$, $C = m$. На такому принципі побудови підпису зроблено стандарти цифрового підпису навіть США. У американському стандарті DSS (Digital Signature Standard), використовується значення $A = r$, $B = –s$, $C = m$ [4];

4) ще однією з переваг є можливість зменшення довжини підпису за допомогою заміни пари чисел (s, m) на пару чисел $(s \bmod q, m \bmod q)$, де q є якимось простим дільником числа $p–1$. При цьому порівняння для перевірки підпису за модулем потрібно замінити на нове порівняння за модулем q: $(y^A r^B) \bmod g^C \pmod q$. Так в американському стандарті DSS (Digital Signature Standard) [4].

2.5 Схема електронного підпису Шнорра

Проблема схеми цифрового підпису Ель-Гамаля в тому, що p має бути дуже великим, щоб зробити складною проблему дискретного логарифму Z_p. Рекомендується довжина p щонайменше 1024 бітів. Можна зробити підпис розміром 2048 біт. Щоб зменшити розмір підпису, Шнорр запропонував нову схему на основі схемою Ель-Гамалю, але із зменшеним розміром підпису [2, 3].

Генерація ключів. Перед підписанням повідомлення A має генерувати ключі та оголосити всім доступні ключі (рис. 2.5):

1) A вибирає просте число p , яке зазвичай дорівнює довжині 1024 біт;

2) A вибирає інше просте число q , яке має той самий розмір, що і дайджест, створений функцією криптографічного хешування (нині 160 бітів, але це може змінитися у майбутньому). Просте число q має ділитися на $(p – 1)$. Іншими словами, $(p – 1) = 0 \bmod q$;

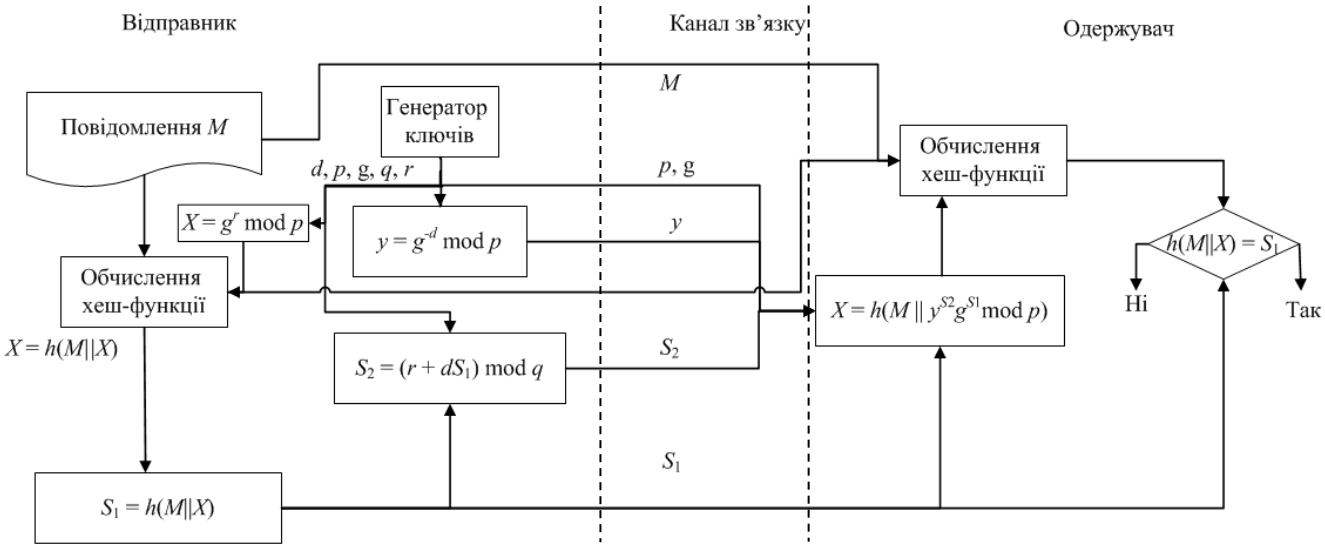

Рисунок 2.5 − Схема використання цифрового підпису Шнорра

3) *A* вибирає $g^q \equiv 1 \bmod p$.

4) *A* вибирає ціле число, *d* як свій секретний ключ;

5) *A* обчислює $y = g^{-d} \bmod p$;

6) Загальнодоступний ключ *A* - (*g*, *p*, *q*) , її секретний ключ - *d*.

Підписання:

1) *A* вибирає випадкове число *r*. Зверніть увагу, що відкриті та секретні ключі можуть використовуватися для підпису багатьох повідомлень. Але *A* повинна змінювати *r* щоразу, коли вона передає нове повідомлення. Зверніть увагу також, що *r* повинен мати значення між 1 і *q*;

2) *A* обчислює перший підпис $S_1 = h(M \parallel X) \bmod p$.

3) *A* обчислює другий підпис $S_2 = (r + dS_1) \bmod q$.

4) *A* передає *M*, S_1 і S_2.

Верифікація (перевірка) повідомлення. Приймач, наприклад *B*, отримує *M*, S_1 і S_2:

1) *B* обчислює $X = h(M \parallel y^{S2} g^{-S1} \bmod p)$;

2) Якщо S_1 дорівнює *X* по модулю *p* повідомлення прийнято; інакше воно відхиляється.

Приклад електронного підпису Шнорра. Нехай $q = 443$ та $p = 48731$, $r = 274$, $d = 357$, $g = 11444$, $M = 100$.

Вибираємо секретній ключ $d = 357$, тоді:

$$y = 11444^{-357} \bmod 48731 = 7355.$$

Відправник хоче передати повідомлення M. Він вибирає r = 274 та обчислює:

$$X = 11444^{274} \bmod 48731 = 37123.$$

Нехай $h(100||37121) = 129$, тоді $S_1 = 129$. Відправник обчислює:

$$S_2 = (274 + 129 \cdot 357) \bmod 443 = 255.$$

Відправник передає повідомлення $M = 100$, $S_1 = 129$ і $S_2 = 255$.
Отримувач перевіряє справжність підпису. Він обчислює:

$$X = (11444^{255} \cdot 7355^{129}) \bmod 48731 = 37123.$$

Одержувач робить висновок, що підпис є вірним, так як $h(100||37123) = 129 = S_1$.

2.6 Алгоритм DSA

DSA (Digital Signature Algorithm – алгоритм цифрового підпису) [2, 3, 5] – криптографічний алгоритм з використанням закритого ключа (з пари ключів: відкритий; закритий) для створення електронного підпису, але не для шифрування (на відміну від RSA та схеми Ель-Гамаля). Підпис створюється секретно (закритим ключем), але може бути публічно перевірено (відкритим ключем). Це означає, що тільки один суб'єкт може створити підпис повідомлення, але будь-хто може перевірити його коректність. Алгоритм заснований на обчислювальній складності взяття логарифмів у кінцевих полях.

Алгоритм був запропонований Національним інститутом стандартів і технологій (НІСТ) у серпні 1991 і є запатентованим, НІСТ зробив цей патент доступним для використання без ліцензійних відрахувань. DSA є частиною DSS (Digital Signature Standard – стандарт цифрового підпису), вперше опублікованого 15 грудня 1998 (документ FIPS-186 (Federal Information Processing Standards - федеральні стандарти обробки інформації)). Стандарт кілька разів оновлювався, остання версія FIPS-186-4.

DSA включає два алгоритми (*S, V*): для створення підпису повідомлення (*S*) і для її перевірки (*V*).

Обидва алгоритми спочатку обчислюють хеш повідомлення, використовуючи хеш-криптографічну функцію. Алгоритм *S* використовує хеш та секретний ключ для створення підпису, алгоритм *V* використовує хеш повідомлення, підпис та відкритий ключ для перевірки підпису (рис. 2.6).

Варто підкреслити, що фактично підписується не повідомлення (довільної довжини), а його хеш (160 – 256 біт), тому неминучі колізії і один підпис, взагалі кажучи, дійсна для кількох повідомлень з однаковим хешем. Тому вибір досить "хорошої" хеш-функції дуже важливий для всієї системи загалом. У першій версії стандарту використовувалася хеш-функція SHA-1 (Secure Hash Algorithm - безпечний алгоритм хешування), в останній версії також можна використовувати будь-який алгоритм сімейства SHA-2 . У серпні 2015 був опублікований FIPS-202, що описує нову хеш-функцію SHA-3. Але на сьогодні вона не включена до стандарту DSS [2, 3, 5, 6].

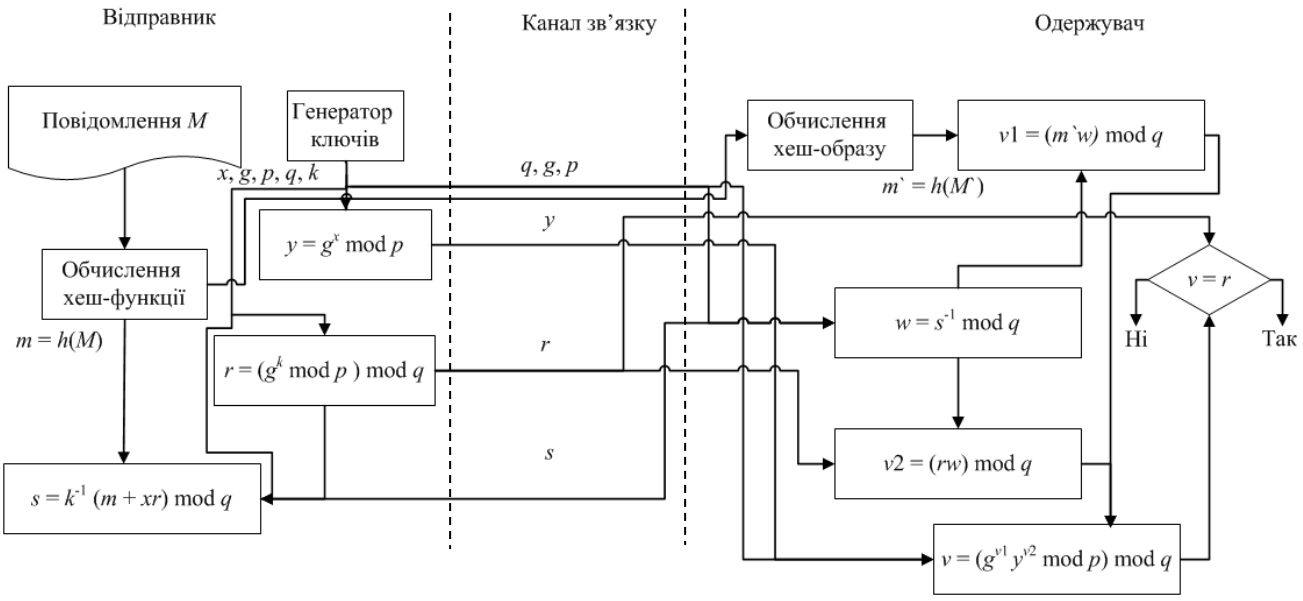

Рисунок 2.6 − Схема використання цифрового підпису DSA

Для роботи системи потрібна база відповідності між реальними реквізитами автора (це може бути як приватна особа, так і організація) і відкритими ключами, а також усіма необхідними параметрами схеми цифрового підпису (хеш-функція, прості числа). Наприклад, подібною базою може бути центр сертифікації.

Параметри схеми цифрового підпису.

Для побудови системи цифрового підпису необхідно виконати такі кроки:

1) вибір криптографічної хеш-функції $H(x)$;

2) вибір простого числа q розмірність якого N в бітах збігається з

розмірністю в бітах значень хеш-функції $H(x)$;

3) вибір простого числа p, такого щоб $(p\text{-}1)$ ділиться на q. Бітова довжина p позначається L;

4) вибір числа $g \neq 1$такого, що його мультиплікативний порядок за модулем p дорівнює q. Для обчислення можна скористатися формулою $g = h^{(p-1)/q} \bmod p$, де h – деяке довільне число h є $(1, p–1)$ таке, що $g \neq 1$. У більшості випадків значення $h = 2$ задовольняє цю вимогу.

Як згадано вище, першочерговим параметром схеми цифрового підпису є криптографічна хеш-функція, необхідна для перетворення тексту повідомлення в число, для якого і обчислюється підпис. Важливою характеристикою цієї функції є бітова довжина вихідної послідовності, що позначається далі N. У першій версії стандарту DSS рекомендована функція SHA-1 і, відповідно, бітова довжина числа 160 біт. Зараз SHA-1 вже не є досить безпечною. У стандарті вказані такі можливі пари значень чисел L і N [5]:

1) $L = 1024$, $N = 160$;

2) $L = 2048$, $N = 224$;

3) $L = 2048$, $N = 256$;

4) $L = 3072$, $N = 256$.

Відповідно до цього стандарту рекомендовані хеш-функції сімейства SHA-2. Урядові організації США повинні використовувати один із перших трьох варіантів, центри сертифікації повинні використовувати пару, яка дорівнює або перевищує пару, використовувану передплатниками. Проектуючи систему можна вибрати будь-яку допустиму хеш-функцію. Тому далі не загострюватиметься увагу на використанні конкретної хеш-функції.

Стійкість криптосистеми на основі DSA не перевищує стійкість використовуваної хеш-функції та стійкість пари (L, N), чия стійкість не більша за стійкість кожного з чисел окремо. Також важливо враховувати, як довго система має залишатися безпечною. В даний момент для систем, які повинні бути стійкими до 2010 (2030) року, рекомендується довжина в 2048 (3072) біта.

Відкритий та секретний ключі:

1) секретний ключ є числом x є $(0, q)$;

2) відкритий ключ обчислюється за формулою $y = g^x \bmod p$.

Відкритими параметрами є числа (p, q, g, y). Закритий параметр лише один - число x. При цьому числа (p, q, g) можуть бути загальними групи користувачів, а числа x і y є відповідно закритим і відкритим ключами конкретного користувача.

При підписуванні повідомлення використовуються секретні числа x і k, причому число k має вибиратися випадковим чином (на практиці псевдовипадковим) під час обчислення підпису кожного наступного повідомлення.

Оскільки (p, q, g) можуть бути використані для декількох користувачів, на практиці часто поділяють користувачів за деякими критеріями на групи з однаковими (p, q, g). Тому ці параметри називають доменними параметрами (Domain Parameters).

Підпис повідомлення виконується за наступним алгоритмом:

1) вибір випадкового числа k є (0, q);

2) обчислення $r = (g^k \bmod p) \bmod q$;

3) вибір іншого k, якщо $r = 0$;

4) обчислення $s = k^{-1} (H(M) + xr) \bmod q$;

5) вибір іншого k, якщо s=0;

6) підписом є пара (r, s) загальної довжини $2N$.

Обчислювально складні операції це зведення в ступінь за модулем (обчислення $g^k \bmod p$) для якого існують швидкі алгоритми, обчислення хеша $H(x)$, де складність залежить від обраного алгоритму хешування та розміру вхідного повідомлення, та знаходження зворотного елемента $k^{-1} \bmod q$ використовуючи, наприклад, розширений алгоритм Евкліда чи малу теорему Ферма у вигляді $k^{-1} \bmod q = k^{q-2} \bmod q$.

Перевірка підпису виконується за алгоритмом:

1) Обчислення $w = s^{-1} \bmod q$;

2) Обчислення $v_1 = (H(M)w) \bmod q$;

3) Обчислення $v_2 = (rw) \bmod q$;

4) Обчислення $v = (g^{v1} y^{v2} \bmod p) \bmod q$;

5) Підпис вірний, якщо $v = r$.

При перевірці обчислювально-складні операції це два зведення в ступінь $g^{v1} y^{v2}$, обчислення хешу $H(M)$ та знаходження зворотного елемента $s^{-1} \bmod q$.

Приклад електронного підпису DSA. Нехай $p = 1511$; $q = 151$; $g = 1024$; $k = 113$; $x = 93$; $h(M) = 100$. Відправник обчислює відкритий ключ

$$y \equiv 1024^{113} \pmod{1511} \equiv 1467.$$

Переходить до обчислення підпису. Розрахунок параметрів r, s:

$$r \equiv [1024^{97} \pmod{1511}] \bmod 151 \equiv 114;$$
$$s \equiv [97^{-1}(100 + 113 \cdot 114) \bmod 151 \equiv 56.$$

Формується підписане повідомлення у вигляді (M, 114. 56), яке передається одержувачеві. Одержувач обчислює параметри:

$$v_1 \equiv (100 \cdot 56^{-1}) \bmod 151 \equiv 142;$$
$$v_2 \equiv (114 \cdot 56^{-1}) \bmod 151 \equiv 29;$$
$$v \equiv [(1024^{142} \cdot 1467^{29}) \bmod 1511] \bmod 151 \equiv 114.$$

Далі одержувач перевіряє рівність результатів $v = r = 114$ – підпис є справжній.

Алгоритм DSA ґрунтується на труднощі обчислення дискретних логарифмів і є модифікацією класичної схеми Ель-Гамаля, де додано хешування повідомлення, а також всі логарифми обчислюються за $\bmod q$, що дозволяє зробити підпис коротшим у порівнянні з аналогами.

Така модифікація, тобто, перехід від мультиплікативної групи за модулем простого числа до групи точок еліптичної кривої існує і для DSA – ECDSA (Elliptic Curve Digital Signature Algorithm – алгоритм цифрового підпису на еліптичних кривих). Він застосовується, наприклад, у криптовалюті bitcoin для підтвердження транзакцій. Цей переклад дозволяє зменшити розмір ключів без шкоди для безпеки у системі bitcoin розмір закритого ключа 256 біт, а відповідного йому відкритого 512 біт.

Будь-яку атаку на алгоритм можна описати так: зловмисник отримує всі відкриті параметри підпису та певний набір пар (повідомлення, підпис) та намагається, використовуючи цей набір, створити дійсний підпис для нового повідомлення, не представленого в наборі.

Ці атаки можна умовно розділити на дві групи - по-перше, зловмисник може спробувати відновити секретний ключ x. І тоді він відразу отримує можливість підписати будь-яке повідомлення, по-друге, він може спробувати створити дійсний підпис для нового повідомлення без прямого відновлення секретного ключа.

3 КРИПТОСИСТЕМИ НА ЕЛІПТИЧНИХ КРИВИХ

3.1 Загальні положення

З розвитком методів і засобів криптоаналізу, а також швидкого розвитку технологій і потужностей обчислювальних комп'ютерних систем, виникає необхідність збільшувати розміри загальносистемних параметрів схем розподілу секрету, внаслідок чого збільшується ресурсомісткість і складність виконання базових операцій в полях. Однак вирішення даного питання може бути досягнуто за рахунок реалізації схем розподілу секрету на основі математичного апарату еліптичних кривих (Elliptic Curve – EC), що дозволяє зменшити розміри параметрів схем і збільшити криптографічний стійкість.

Криптосистеми на еліптичних кривих (Elliptic Curve Cryptography – ECC) [3, 6, 7] належать до класу криптосистем з відкритим ключем. Їхня безпека базується здебільшого на складності розв'язування задачі дискретного логарифмування у групі точок еліптичної кривої над скінченним полем. Цим зумовлено їхню потужну криптостійкість порівняно з іншими алгоритмами. Існують стійкі криптоалгоритми на еліптичних кривих, базовані на труднощах розкладання великих цілих чисел, коли еліптична крива задається над скінченним кільцем за складеним модулем, але вони зустрічаються дуже рідко. Проте слід зауважити, що криптостійкість є відносним поняттям, пов'язаним з поняттям найоптимальнішого відомого алгоритму зламу системи.

Еліптичні криві – математичний об'єкт, який може бути визначено над яким завгодно полем. У криптографії зазвичай використовуються скінченні поля. Для точок на еліптичній кривій вводиться операція складання, яка відіграє ту саму роль, що й операція множення у криптосистемах RSA та Ель-Гамаля [3, 8].

Іншою перевагою криптосистем на еліптичних кривих є висока швидкість опрацьовування інформації. Але й тут не все так просто. Зрозуміло, що, маючи потужну криптостійкість, криптосистеми на еліптичних кривих дозволяють використовувати ключ меншої довжини. Проте, прийнятна для роботи в мережах, швидкість обчислень досягається лише при використанні спеціалізованих обчислювачів (це цілком природно для криптосистем з відкритим ключем) та полів спеціальних характеристик.

Криптосистеми на еліптичних кривих, як і інші криптосистеми з відкритим ключем, недоцільно застосовувати для шифрування великих обсягів даних. Проте,

їх можна ефективно використовувати для систем цифрового підпису та ключового обміну. З 1998 року використовування еліптичних кривих для розв’язування криптографічних завдань, таких як цифровий підпис, було закріплено у стандартах США ANSI X9.62 та FIPS 186–2.

В Україні ухвалений стандарт цифрового підпису базується на еліптичних кривих ДСТУ 4145-2002 – "Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка".

Зазначимо, що безпека таких систем цифрового підпису спирається не лише на стійкість алгоритму на еліптичних кривих, але й на стійкість використовуваної геш-функції. Також в Україні прийняті нові стандарти ДСТУ ISO/IEC 15946-1:2019 – "Інформаційні технології. Методи захисту. Криптографічні методи на основі еліптичних кривих. Частина 1. Загальні положення", ДСТУ ISO/IEC 15946-3:2006 – "Інформаційні технології. Методи захисту. Криптографічні методи, що ґрунтуються на еліптичних кривих. Частина 3. Установлення ключів", ДСТУ ISO/IEC 15946-5:2019 – "Інформаційні технології. Методи захисту. Криптографічні методи на основі еліптичних кривих. Частина 5. Генерування еліптичних кривих".

Численні дослідження засвідчили [6, 7], що криптосистеми на підставі еліптичних кривих перевершують інші системи з відкритим ключем за двома важливими параметрами: мірою захищеності з розрахунку на кожен біт ключа та за швидкодією програмної і апаратної реалізації. Це пояснюється тим, що для обчислення обернених функцій на еліптичних кривих відомі лише алгоритми з експоненційним зростанням трудомісткості, тоді як для звичайних систем запропоновано субекспоненційні методи. Як наслідок, той рівень стійкості, який досягається, скажімо, в RSA при використанні 1024-бітових модулів, в системах на еліптичних кривих зреалізовується при розмірі модуля 160 біт, що забезпечує простішу як програмну, так і апаратну реалізацію.

Детальне вивчення еліптичних кривих потребує більше знань алгебричної геометрії, ніж вищої алгебри. Проте далі матеріал викладатиметься при можливості без залучення складних конструкцій алгебри і в обсязі, достатньому для розуміння принципів побудови та функціонування відповідних криптосистем на еліптичних кривих. Детальніше викладення теорії еліптичних кривих та їхнього використання у криптографії може бути знайдене, наприклад, в роботах [2, 3, 6, 7].

3.2 Група точок еліптичної кривої

Еліптичні криві описуються кубічними рівняннями, подібними до тих, які використовуються для обчислювання кривої еліпса. Взагалі кубічні рівняння для еліптичних кривих мають форму

$$y^2 + axy + by = x^3 + cx^2 + dx + e,$$

де a, b, c, d та e є дійсними числами, які задовольняють певним простим умовам. Означення еліптичної кривої включає також певний елемент, який позначається O й називається невласним елементом (а також нескінченним, або нульовим елементом). Такі рівняння називаються кубічними, або рівняннями третього порядку, оскільки в них найвищий показник степеня становить 3.

Розглянемо еліптичну криву E (рис. 3.1), яка відповідає рівнянню $y^2 + y = x^3 - x^2$. На цій кривій лежать лише чотири точки, координати яких є цілими числами. Це точки $A(0, 0)$, $B(1, -1)$, $C(1, 0)$, $D(0, -1)$.

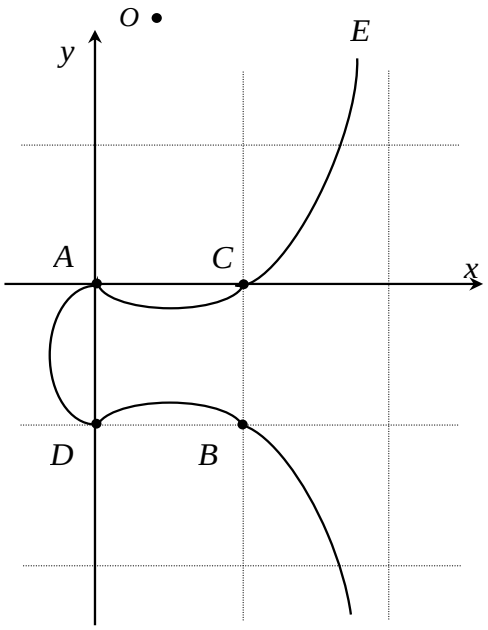

Рисунок 3.1 – Група з п’яти точок еліптичної кривої E,
O – нескінченно віддалена точка

Для визначення операції складання на групі точок еліптичної кривої вважатимемо, що:

а) на площині існує нескінченно віддалена точка $O \in E$, в якій збігаються всі вертикальні прямі;

б) дотична до кривої перетинає точку дотику P двічі.

Тепер можна сформулювати правила складання точок $P, Q \in E$ (рис. 3.2, 3.3):

а) проведемо пряму лінію через точки P та Q, знайдемо третю точку S перетинання цієї прямої з кривою E;

б) знайдемо через точку S вертикальну пряму до перетинання з кривою E у точці T;

в) шукана сума є $P + Q = T$;

г) знайдемо через точку S вертикальну пряму до перетинання з кривою E у точці T.

Застосувавши ці правила до групи точок $G = \{A, B, C, D, O\}$, знайдемо (рис. 2.3) $A + A = B$, $A + B = C$, $A + C = D$, $A + D = O$, або $2A = B$, $3A = C$, $4A = D$, $5A = O$, $6A = A$.

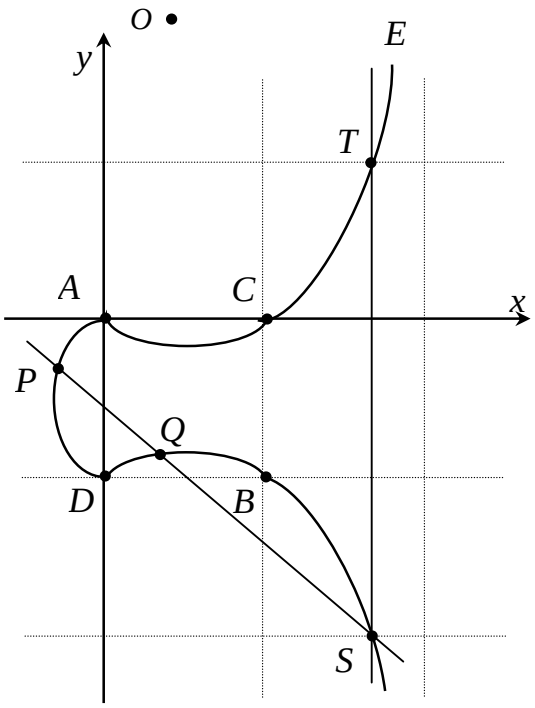

Рисунок 3.2 – Складання точок на еліптичній кривій $P + Q = T$

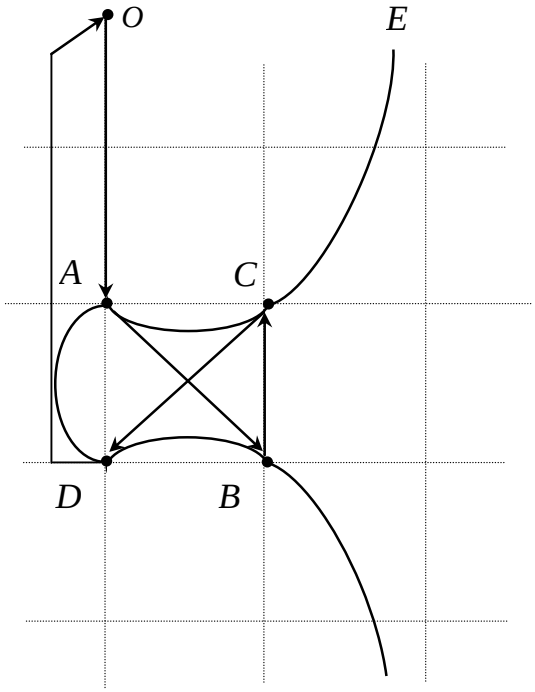

Рисунок 3.3 – Адаптивна абелева група $\{A, B, C, D, O\}$ на еліптичній кривій E

Для кожної з точок $P, Q \in G$ справедливе відношення $P + Q = Q + P$. Для кожної точки $P \in G$ справедливе є $P + O = P$; інакше кажучи, точка O – адитивний одиничний елемент групи G(O також називають – невласним елементом, нескінченним або нульовим елементом).

3.3 Еліптична крива над полем *GF*(*p*)

У реальних криптосистемах використовується рівняння $y^2 \equiv \left(x^3 + ax + b\right) \bmod p$ де $a, b \in GF(p)$; $\left(4a^3 + 27b^2\right) \bmod p \neq 0$; $p > 3$ – просте. Група $E(GF(p))$ складається з усіх точок (x, y); $x, y \in GF(p)$, які задовольняють рівнянню, і нескінченно віддаленої точки O.

Множина $E_p(a, b)$ складається з усіх точок (x, y), $x \geq 0$, $p > y$, які задовольняють рівнянню $y^2 \equiv \left(x^3 + ax + b\right) \bmod p$, й точки в нескінченності O. Кількість точок в $E_p(a, b)$ позначатимемо $\#E_p(a, b)$. Ця величина має важливе значення для криптографічних додатків еліптичних кривих.

Визначену над точками з $E(GF(p))$ операцію складання алгебрично може бути описано в такий спосіб:

а) $P + O = O + P = P$;

б) якщо $P = (x, y)$, тоді $P + (x, -y) = O$. Точка $(x, -y)$ є від'ємним значенням точки P і позначається $-P$. Зазначимо, що $(x, -y)$ лежить на еліптичній кривій і належить до $E_p(a, b)$. Наприклад, у разі $E_{59}(-3, 1)$ для $P = (30, 19)$ матимемо $-P = (30, -19)$. Але $-19 \bmod 59 \equiv 40$, отже $-P = (30, 40)$;

в) якщо $P = (x_1, y_1)$ і $Q = (x_2, y_2)$, то $P + Q = (x_3, y_3)$ визначається згідно з правилами

$$x_3 \equiv (\lambda^2 - x_1 - x_2) \bmod p;$$
$$y_3 \equiv (\lambda(x_1 - x_3) - y_1) \bmod p,$$

де $$\lambda \equiv \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} (\bmod p), & \text{за } P \neq Q; \\ \dfrac{3x_1^2 + a}{2y_1} (\bmod p), & \text{за } P = Q. \end{cases}$$

Число λ – кутовий коефіцієнт січної, проведеної через точки $P = (x_1, y_1)$ та $Q = (x_2, y_2)$. За $P = Q$ січна перетворюється на дотичну, чим і пояснюється наявність двох формул для обчислення λ.

Розглянемо криву E_7 (2, 6): $y^2 \equiv \left(x^3 + 2x + 6\right) \bmod 7$. Перевіримо умову: $\left(4 \cdot 2^3 + 27 \cdot 6^2\right) \bmod 7 \equiv 3 \neq 0$.

Отже, дана крива є несингулярна. Знайдемо певну (випадкову) точку в

$E_7(2, 6)$. Нехай $x = 5$, тоді

$$y^2 \equiv \left(5^3 + 2 \cdot 5 + 6\right) \bmod 7 \equiv (125 + 10 + 6) \bmod 7 \equiv 1 (\bmod 7),$$

і $y \equiv 1 \pmod 7$ або $y \equiv -1 \equiv 6 \pmod 7$. Маємо одразу дві точки: (5, 1) та (5, 6).

Знайдемо ще пару точок шляхом обчислення композиції. Спочатку знайдемо 2(5, 1):

$$\lambda = \frac{3 \cdot 5^2 + 2}{2 \cdot 1} = \frac{0}{2} \equiv 0 (\bmod 7);$$
$$x_3 = 0 - 2 \cdot 5 \equiv 4 (\bmod 7);$$
$$y_3 = 0(5 - 4) - 1 \equiv 6 (\bmod 7).$$

Одержали 2(5, 1) = (4, 6) (можна переконатися, що відшукану точку розташовано на кривій, підставивши її координати до рівняння). Знайдемо ще одну точку 3(5, 1) = (5, 1) + (4, 6):

$$\lambda = \frac{6 - 1}{4 - 5} = -\frac{5}{1} \equiv 2 (\bmod 7);$$
$$x_3 = 2^2 - 5 - 4 \equiv 2 (\bmod 7);$$
$$y_3 = 2(5 - 2) - 1 \equiv 5 (\bmod 7).$$

Одержали 3(5, 1) = (2, 5).

Отже, знайдено чотири точки. Для криптографічного використовування кривої важливо знати, скільки всього точок містить множина $E_7(2, 6)$.

Нехай $p = 59$. Розглянемо еліптичну криву E: $y^2 = x^3 - 3x + 1$. $E_{59}(-3, 1)$ складається з точки O, а також з точок (30, 19); (3, 45); (2, 48); (14, 15); (4, 17); (47, 16); (10, 33); (13, 34); (8, 31); (33, 47); (11, 1); (39, 47); (31, 50); (15, 33); (23, 2); (42, 53); (36, 23); (0, 1); (27, 30); (22, 50); (34, 26); (46, 12); (12, 10); (32, 39) ; (38, 19); (50, 40); (54, 3); (41, 8) та інших.

Нехай $P = (3, 10)$ і $Q = (9, 7)$. Знайдемо $P + Q$ і $2P$. Нехай $P + Q = (x_3, y_3)$, тоді

$$\lambda = \frac{7 - 10}{9 - 3} = -\frac{1}{2} \equiv 11 (\bmod 23);$$

$$x_3 = 121 - 3 - 9 = 109 \equiv 17 \pmod{23} \equiv -6 \pmod{23};$$
$$y_3 = 11(3 + 6) - 10 = 89 \equiv 20 \pmod{23}.$$

Отже, $P + Q = (17, 20)$. Знайдемо $2P = P + P = (x_3, y_3)$. Тоді

$$\lambda = \frac{3 \cdot 9 + 1}{20} = \frac{1}{4} \equiv 6 \pmod{23};$$
$$x_3 = 36 - 6 = 30 \pmod{23} \equiv 7 \pmod{23};$$
$$y_3 = 6(3 - 7) - 10 = -34 \pmod{23} \equiv 12 \pmod{23}.$$

Отже, $2P = (7, 12)$.

3.4 Вибір параметрів еліптичної кривої

Розглянемо основні рекомендації щодо вибору параметрів еліптичної кривої, призначеної для розв'язання криптографічних завдань, а саме щодо вибору коефіцієнтів *a*, *b* й модуля *p*. Фактично критерієм вибору є неможливість здійснення певного роду атак, пропонованих для певних класів кривих. Рекомендації, викладені нижче, виходять із стратегії вибору випадкової кривої. Ця стратегія вважається за найбільш надійну з точки зору забезпечення стійкості результатів криптосистеми. Альтернативний підхід, тут не розглядуваний, полягає у систематичному конструюванні кривої із заданими властивостями, що зазвичай стає ефективнішим з обчислювальної точки зору. Для реалізації цього підходу запропоновано спеціальні методи, але здобуті криві фактично обираються з відносно невеликого класу і викликають підозри щодо наявності певних специфічних властивостей, які можуть надати можливість з часом відшукати алгоритми для їхнього зламу.

Опишемо процес формування випадкової кривої [3, 6, 7]:

а) Обираємо довільно просте число *p*. Бітова довжина числа *p*, $t = \lfloor \log p \rfloor + 1$, має бути такою, щоб унеможливити вживання загальних методів знаходження логарифмів на кривій, що мають трудомісткість $T(2^{t/2})$. Величина $t = 128$ біт (чотири машинні слова на 32-бітових комп'ютерах) сьогодні є недостатня, оскільки існують повідомлення про злам відповідних кривих. Інше міркування базується на тому, що шифр на еліптичній кривій має бути не менш стійким, ніж блоковий шифр AES (Advanced Encryption Standard). Вважається, що стійкість

AES забезпечується повною довжиною його ключа, яка становить 128, 196 та 256 біт. Оскільки стійкість шифру на еліптичній кривій визначається величиною $t/2$, довжина модулів еліптичних кривих має становити відповідно 256, 392 та 512 біт;

б) Обираємо випадкові числа a та b такі, що $a, b \pmod p \neq 0$ і $(4a^3 + 27b^2) \bmod p \neq 0$. Звернімо увагу на те, що при обчисленні композиції точок параметр b ніде не фігурує. Тому для підвищення ефективності підрахунку інколи рекомендують випадково обирати лише b, а за a приймати невелике ціле число. Приміром, стандарт США FIPS 186–2 передбачає використовування кривих з параметром $a = –3$, що спрощує обчислення;

в) Визначаємо кількість точок на кривій $n = \#E_p(a, b)$ (це є найтрудомісткіший етап опису процесу). Важливо, щоб n мало великого простого дільника q, а найоптимальніше, саме було б простим числом: $n = q$. Якщо n розкладається на невеликі множники, то в $E_p(a, b)$ існує багато невеликих підмножин з власними генераторами і алгоритм Поліга–Хеллмана [6, 7] швидко обчислює логарифм на кривій через логарифми в цих невеликих підмножинах. Якщо пошук кривої з $n = q$ потребує надто багато часу, то можна припустити $n = hq$, де h – невелике число. Знову підкреслимо, що стійкість криптосистеми на еліптичній кривій визначається не модулем p, а кількістю елементів q у підмножині точок кривої. Але якщо множник h – невелике число, то q є величиною того самого порядку, що й p. Якщо n не відповідає вимогам, то слід повернутися до кроку б;

г) Перевіряємо, чи виконуються нерівності $(p^k – 1) \bmod q \neq 0$ для всіх k, $0 < k < 32$. Якщо ні, то повертаємося до кроку б. Ця перевірка запобігає можливості MOV-атаки (названої за прізвищами її авторів Menezes, Okamoto, Vanstone), а також дозволяє вилучити з розгляду так звані суперсингулярні криві та криві з $\#E_p(a, b) = p – 1$ [13]. Метод MOV і згадані особливі типи кривих дозволяють звести завдання обчислення логарифма на кривій до простіших задач;

д) Перевіряємо, чи виконується нерівність $q \neq p$. Якщо ні, то повертаємося до кроку б. Річ у тім, що для кривих з $q = p$, названих аномальними, існують ефективні методи обчислювання логарифмів [6, 7];

е) На даному кроці відповідну для криптографічних додатків криву здобуто. Маємо параметри p, a, b, кількість точок n і розмір підмножини точок q. Зазвичай ще потрібно знайти точку G – генератор цієї підмножини. Якщо $q = n$, то кожна точка (окрім O) є генератором. Якщо $q < n$, то обираємо випадкові точки G', поки не дістанемо $G = [n/q]G' \neq O$. Щоб знайти випадкову точку на кривій, обираємо випадкове число $x < p$, обчислюємо $e \equiv (x^3 + ax + b) \bmod p$ і робимо спробу

обчислити квадратний корінь $y \equiv \sqrt{e} \pmod{p}$. Якщо корінь існує, то дістанемо точку (x, y), інакше – обираємо інше число x. Алгоритми обчислювання квадратного кореня за модулем простого числа подано в роботі [6, 7].

Завдання, яке має розв'язувати криптоаналітик, використовуючи криптосистеми на базі еліптичних рівнянь, називається завданням дискретного логарифмування на еліптичній кривій і формулюється в такий спосіб. Задано точки P та Q на еліптичній кривій порядку n, де n – кількість точок на кривій. Треба визначити єдину точку x таку, що $P = xQ$.

3.5 Використання еліптичних кривих у криптографії

Обмін ключами з використанням еліптичних кривих може бути здійснено у такий спосіб. Спочатку обираються просте число p і параметри a та b для еліптичної кривої. Це задає еліптичну групу точок $E_p(a, b)$. Потім в $E_p(a, b)$ обирається генерувальна точка $G = (x, y)$. При обиранні G є важливо, щоб найменше значення n, при якому $nG = O$, було б надто великим простим числом. Параметри $E_p(a, b)$ та G криптосистеми – це параметри, відомі усім учасникам. Обмін ключами між користувачами A і B можна провести за поданою нижче схемою [3].

а) Сторона A обирає ціле число k_a, яке є менше за n. Це число буде власним ключем учасника A. Потім учасник A генерує відкритий ключ $Y_a = k_aG$. Відкритий ключ є певною точкою з $E_p(a, b)$.

б) Так само учасник B обирає власний ключ k_b і обчислює відкритий ключ $Y_b = k_bG$.

в) Учасник A генерує секретний ключ $K = k_aY_b$, а учасник B – секретний ключ $K = k_bY_a$.

Обидві подані формули дають однаковий результат, оскільки

$$k_aY_b = k_a(k_bG) = k_b(k_aG) = k_bY_a.$$

Нехай $p = 1009$, $G = (602, 971)$, $E_p(-3, 4)$, що відповідає кривій $y^2 = x^3 - 3x + 4$. Можна підрахувати, що $967G = O$. Власним ключем користувача A є $k_a = 237$, тому відкритим ключем A буде $Y_a = 237(602, 971) = (440, 208)$.

Власним ключем користувача B є $k_b = 509$, тому відкритим ключем B буде $Y_b = 509(602, 971) = (231, 605)$.

Спільний секретний ключ

$$K = 237(231, 605) = 509(440, 208) = (303, 791).$$

Зверніть увагу на те, що спільний секретний ключ є парою чисел. Якщо цей ключ передбачається використовувати як сеансовий ключ для традиційного шифрування, то з цієї пари чисел треба генерувати одне відповідне значення. Можна, наприклад, використовувати просто координату x чи певну просту функцію від x.

У літературі [2, 3, 6, 7] можна знайти аналіз кількох підходів щодо зашифровування/розшифровування, які передбачають використання еліптичних кривих. Розглянемо найпростіший з цих підходів.

Першим завданням у згаданій системі є зашифровування відкритого тексту повідомлення M, яке надсилатиметься у вигляді значення (x, y) для точки P_M. Тут точка P_M містить зашифрований текст, який згодом розшифровуватиметься.

Користувач A обирає власний ключ k_a і генерує відкритий ключ Y_a. Щоб зашифрувати й надіслати повідомлення P_M користувачеві B, користувач A обирає довільне додатне ціле число r і обчислює зашифрований текст C_M, який складається з пари точок $C_M = (rG,\ P_M + rY_b)$.

Зазначимо, що сторона A використовує відкритий ключ Y_b сторони B. Для того, щоб розшифрувати цей шифртекст, сторона B помножує першу точку в парі на секретний ключ B і віднімає результат з другої точки:

$$P_M + rY_b - k_b\,(rG) = P_M + r(k_bG) - k_b\,(rG) = P_M.$$

Користувач A замаскував повідомлення P_M за допомогою додавання до нього rY_b. Нікому, окрім цього користувача, невідоме значення r, тому, хоча Y_b й є відкритим ключем, ніхто не зможе усунути маску rY_b. Проте користувач A розмістив у повідомленні й „підказку”, якої вистачить, щоб усунути маску тому, хто має власний ключ k_b. Криптоаналітикові для відновлення повідомлення доведеться обчислити r за наведеними G та rG, що становить собою складне завдання.

Розглянемо випадок $p = 1009$, $G = (602, 971)$, $E_p(-3, 4)$, що відповідає кривій $y^2 = x^3 - 3x + 4$.

Припустімо, що користувач A збирається доправити користувачеві B повідомлення, кодоване еліптичною точкою $P_M = (532, 648)$. Для цього користувач A обирає довільне число $r = 237$ і відшукує відкритий ключ користувача $B - Y_b = (231, 605)$. Обчислює $237(602, 971) = (440, 208)$ та

(532, 648) + 237(231, 605) = (463, 525). Отже, користувач *A* повинен мати повідомлення {(440, 208), (463, 525)}.

Безпека, гарантована криптографічним підходом на базі еліптичних кривих, залежить від того, наскільки складним для розв'язання буде завдання щодо визначення *r* за даними *rP* та *P*. Це завдання зазвичай називають проблемою логарифмування на еліптичній кривій. Найбільш швидким з відомих сьогодні методів логарифмування на еліптичній кривій є так званий ρ-метод Полларда (Pollard) [13].

За допомогою описаних правил складання можна обчислити точку *kP* для будь-якого цілого числа *k* і будь-якої точки *P* еліптичної кривої. Однак рішення оберненої задачі – знаходження числа *k* по відомим точкам *P* і *kP* – є важкою проблемою – ECDLP. Складність вирішення проблеми ECDLP обумовлена ресурсомісткістю операцій додавання і дублювання точок, за допомогою яких обчислюється *kP*. Звідси випливає можливість застосування більш коротких ключів (табл. 3.1) [6, 7].

Таблиця 3.1 – Розмір ключів для ECC і RSA відповідно до NIST

ECC key, Bits	RSA key, Bits	Key ratio
163	1024	1 : 6
256	3072	1 : 12
384	7680	1 : 20
512	15360	1 : 30

4 ЕЛЕКТРОННИЙ ПІДПИС У ГРУПІ ТОЧОК ЕЛІПТИЧНИХ КРИВИХ

4.1 Стандарт електронного підпису згідно з ДСТУ 4145

ДСТУ 4145-2002 [10] (повна назва: «ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, заснований на еліптичних кривих. Формування та перевірка») — український стандарт, що описує алгоритми формування та перевірки електронного цифрового підпису , груп точок еліптичних кривих над полями $GF(2^m)$ та правила застосування цих правил до повідомлень, які пересилаються каналами зв'язку та/або обробляються в комп'ютеризованих системах загального призначення.

Прийнято та введено в дію наказом державного комітету України з питань технічного регулювання та споживчої політики від 28 грудня 2002 року № 31. Текст стандарту є у відкритому доступі [10].

Відповідно до наказу Мінцифри України від 30 вересня 2020 року № 140/614, з 1 січня 2021 року стандарт повинен використовуватись спільно з ДСТУ 7564:2014 (хеш-функція «Купіну») (рис. 4.1) [10].

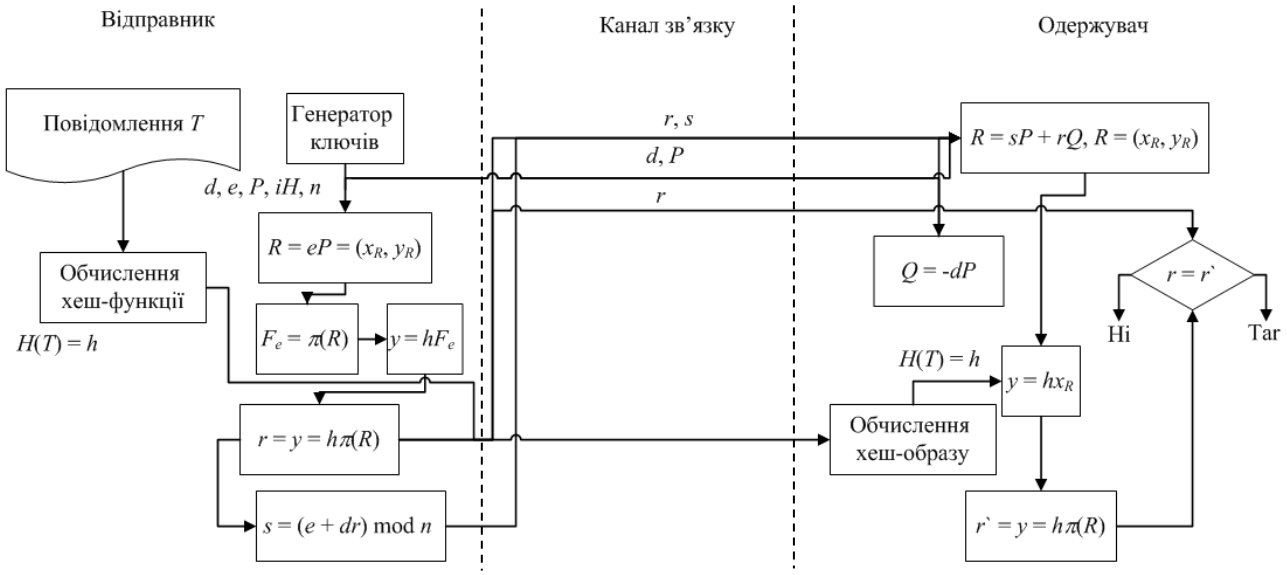

Рисунок 4.1 − Схема використання цифрового підпису ДСТУ 4145-2002

Основними процедурами алгоритму цифрового підпису, встановленими ДСТУ 4145-2002 є обчислення передпідпису, обчислення підпису та перевірка цифрового підпису.

Загальні параметри цифрового підпису:

1) ступінь розширення m - просте число (параметр поля $GF(2^m)$);

2) неприведений поліном $f(t)$ ступеня m, визначальний операції в $GF(2^m)$;

3) коефіцієнти еліптичної кривої виду $y^2 + xy = x^3 + Ax^2 + B$, де A і $B \in GF(2^m)$, $B \neq 0$, $A \in (0, 1)$. Рекомендовані для використання еліптичні криві для поліноміального базису та оптимального нормального базису наведені в додатку до стандарту;

4) базова точка еліптичної кривої P, що породжує підгрупу E_n групи E;

5) порядок n базової точки P (просте число);

6) довжина представлення числа n у двійковому вигляді $L(n)$;

7) ідентифікатор використовуваної хеш-функції iH;

8) довжина цифрового підпису L_D.

Додаткові умови на параметри:

1) порядок циклічної підгрупи n повинен задовольняти умові $n \geq \max(2160, 4[\sqrt{2^m}] + 1)$;

2) повинна виконуватися умова MOV (Менезеса-Окамото-Венстоуна): $2^{mk} \neq 1 \pmod n$ для $k = 1, 2, \ldots, 32$.

Цифровий підпис обчислюється на основі повідомлення та передпідпису.

Вхідні дані:

1) загальні параметри цифрового підпису;

2) особистий ключ цифрового підпису d;

3) повідомлення T довжини $L_T > 0$;

4) хеш-функція $H(T)$ з довжиною хеш-коду L_H та ідентифікатором iH;

5) довжина цифрового підпису L_D, яка вибирається для групи користувачів: $L_D \geq 2L(n)$, $L_D \equiv 0 \pmod{16}$.

Обчислення припису полягає у виборі першої координати секретної, випадково обраної точки з орбіти точки P. Після використання цифрового припису її відразу знищують разом із відповідним рандомізатором.

Вхідні дані: загальні параметри цифрового підпису.

Алгоритм обчислення передпідпису:

1) вибір рандомізатора e на основі криптографічного генератора псевдовипадкових чисел;

2) обчислення точки еліптичної кривої $R = eP = (x_R, y_R)$;

3) перевірка значення координати x (якщо $x_R = 0$, то повторити процедуру вибору рандомізатора);

4) інакше прийняти $F_R = x_R$ (інше позначення: $FR = n(R)$).

Результат: цифровий передпідпис $F_e \in GF(2^n)$

Алгоритм обчислення підпису:

1) перевірка коректності загальних параметрів, ключів та виконання умов та обмежень щодо значень проміжних величин відповідно до певних стандартів процедур;

2) обчислення хеш-коду $H(T)$ на основі повідомлення T;

3) одержання елемента основного поля h з хеш-коду $H(T)$ за встановленою стандартом процедурою. Якщо при цьому виходить $h = 0$, то приймають $h = 1$;

4) вибір рандомізатора e;

5) обчислення цифрового припису F_e;

6) обчислення елемента основного поля $y = hF_e$ (твір є елементом $GF(2^m)$) (фактично $r = y = hn(R)$);

7) отримання цілого числа r з елемента основного поля y за встановленою стандартом процедурою (у разі $r = 0$ вибирається новий рандомізатор);

8) обчислення цілого числа $s = (e + dr) \bmod n$ (якщо $s = 0$, вибирається новий рандомізатор);

9) на основі пари цілих чисел (r, s) записується цифровий підпис D як двійковий ряд довжини L_D: у молодших розрядах лівої половини бітів розміщується значення s, у молодших розрядах правої половини бітів розміщується значення r, що залишилися розряди заповнюються нулями.

Результат: підписане повідомлення у вигляді (iH, T, D), де D - цифровий підпис.

Перевірка цифрового підпису.

Вхідні дані:

1) загальні параметри цифрового підпису;

2) відкритий ключ цифрового підпису Q, $Q = -dP$;

3) підписане повідомлення (iH, T, D) довжини $L = L(iH) + L_T + L_D$;

4) хеш-функція $H(T)$.

Алгоритм обчислення підпису:

1) перевірка коректності загальних параметрів, ключів та виконання умов та обмежень щодо значень проміжних величин відповідно до певних стандартів процедур;

2) перевірка ідентифікатора хеш-функції iH: якщо цей ідентифікатор не використовується в заданій групі користувачів, то приймається рішення "підпис недійсний" і перевірка завершується;

3) на підставі iH визначається довжина хеш-коду L_H;

4) перевірка умов $L_D \geq 2L(n)$, $L_D = 0 \pmod{16}$. Якщо хоча б одне з них не

виконується, то приймається рішення "підпис недійсний" і перевірка завершується;

5) перевірка наявності тексту повідомлення та його довжини $L_r = L - L(iH) - L_D$. У разі відсутності тексту або при $L_T \leq 0$ приймається рішення "підпис недійсний" і перевірка завершується;

6) обчислення хеш-коду $H(T)$ на основі повідомлення T;

7) одержання елемента основного поля h з хеш-коду $H(T)$ за встановленою стандартом процедурою. Якщо при цьому виходить $h = 0$, то приймають $h = 1$;

8) виділення пари чисел (r, s) із двійкового запису цифрового підпису D;

9) перевірка умов $0 < r < n$ і $0 < s < n$. Якщо хоча б одне з них не виконується, то приймається рішення "підпис недійсний" і перевірка завершується;

10) обчислення точки еліптичної кривої $R = sP + rQ$, $R = (x_R, y_R)$;

11) обчислення елемента основного поля $y = hx_R$;

12) отримання цілого числа $\bar{r}$ з елемента основного поля y за встановленою стандартом процедурою;

13) якщо $r = \bar{r}$, то приймається рішення "підпис дійсний", інакше - "підпис недійсний".

Результат: прийняте рішення: "підпис дійсний" або "підпис недійсний".

Криптостійкість цифрового підпису ґрунтується на складності дискретного логарифмування $R = eP$, $Q = -dP$ у циклічній підгрупі групи точок еліптичної кривої.

4.2 Порівняльна характеристика та аналіз схем електронного підпису

На сучасний момент електронний цифровий підпис широко використовується як юридичними, так і фізичними особами. Активно впроваджується в державних установах і органах державної влади для підпису та підтвердження електронних документів. В рамках систем документообігу використовуються різні алгоритми ЕЦП. Незважаючи на те, що загалом всі алгоритми виконують свої функції, між ними існує значна різниця, і кожен алгоритм має свої переваги та недоліки, які потребують подальшого дослідження. Така різноманітність алгоритмів вимагає уважного вибору залежно від конкретних потреб та умов застосування.

Сучасні схеми цифрового підпису можна класифікувати залежно від математичної проблеми, на якій вони базуються та яка забезпечує їх безпеку:

1) схеми факторизації цілих чисел (ФЦ). Безпека залежить від складності розкладу на прості множники цілих чисел. Прикладами є схеми RSA та Рабіна;

2) схеми дискретного логарифму (ДЛ). Безпека ґрунтується на складності знаходження дискретного логарифму у скінченному полі. Серед таких схем можна виділити Ель-Гамаля, Шнорра та DSA;

3) схеми на еліптичних кривих (ЕК). Безпека залежить від складності розв'язання проблеми знаходження дискретного логарифму на еліптичних кривих. Прикладами є схеми підпису EC-KDSA, ECSS, ECDSA [2, 3].

Актуальність проблеми полягає в необхідності обґрунтування вибору конкретного алгоритму ЕЦП, розробці його власної реалізації для подальшого дослідження та аналізу його характеристик. Це важливо для вирішення практичних завдань та забезпечення надійності електронних підписів у різних областях застосування.

Проблеми факторизації цілих чисел та дискретного логарифму є ключовими в асиметричних схемах шифрування та підпису. Дійсно, обидві ці проблеми стоять в основі безпеки багатьох криптографічних систем. Ось коротке уточнення та доповнення до висловлення. Проблема факторизації цілих чисел (ПФЧ) полягає в розкладанні складеного числа n на прості множники. Найвідоміша асиметрична криптосистема, RSA, базується саме на цій проблемі. На сьогоднішній день найкращі класичні алгоритми для факторизації простих чисел використовують квантові комп'ютери і деякі алгоритми здатні вирішувати цю проблему швидше, ніж експоненційний час, що ставить під загрозу безпеку RSA у випадку успішного впровадження квантових обчислень.

Проблема дискретного логарифму (ПДЛ) виникає в асиметричних схемах, таких як Ель-Гамаль та схеми на еліптичних кривих. Справжній виклик полягає в тому, що, хоча існують алгоритми, що прискорюють розв'язання дискретного логарифму (такі як алгоритм Шенкса для ПДЛ у групі точок еліптичної кривої), їх ефективність залежить від конкретних параметрів криптосистеми. У той час як для деяких параметрів найкращі алгоритми можуть працювати швидше, ніж за експоненційний час, існує ймовірність, що квантові алгоритми, такі як алгоритм Шора, можуть бути застосовані для розв'язання цієї проблеми на квантовому комп'ютері. Узагальнюючи, висока складність цих проблем та поява квантових алгоритмів ризикує змінити ландшафт криптографії, вимагаючи нових методів та алгоритмів для забезпечення безпеки.

Проблема дискретного логарифму у групі точок еліптичної кривої (ПДЛЕК), визначеної над простим полем. Група точок еліптичної кривої

визначається над скінченним полем F_p, де p є простим числом. Така група містить точки, які задовольняють рівнянню еліптичної кривої над цим полем. Проблема полягає в тому, щоб знайти ціле число l, $0 \le l \le n-1$, таке що $Q = lG$ для точки Q також з групи $E(F_p)$. Відомо, що ПДЛЕК вважається більш складною за ПФЧ. За останні роки вивчення ПДЛЕК відіграє ключову роль у розвитку еліптично-криптографії, яка є часто використовуваною в криптосистемах для забезпечення безпеки в області шифрування та підпису. Збільшення обчислювальної потужності за рахунок квантових комп'ютерів може стати важливим фактором у подальшому вивченні та розвитку цієї області.

4.3 Модифікація електронного підпису Ніберга-Рюпеля з відновленням повідомлення

Підпис Ніберга-Рюпеля (Nyrberg-Rueppel message recovery signature) – схема електронного підпису з відновленням повідомлення [3] заснована на завданні дискретного логарифмування (Discrete Logarithm Problem – DLP) в кінцевому полі. Схема підпису з відновленням повідомлення має на увазі процедуру, коли повідомлення відновлюється після перевірки підпису, для цього використовують відкриту функцію надмірності F, яка є легко оборотною.

В магістерської роботі запропоновано модифікацію електронного підпису Ніберга-Рюпеля на основі еліптичних кривих над полями Галуа $GF(p)$, $GF(2^m)$ [11]. Безпека криптосистем на еліптичних кривих (Elliptic Curves – EC) [7, 8] заснована на труднощах розв’язання задачі дискретного логарифмування в групі точок еліптичної кривої (Elliptic Curve Discrete Logarithm Problem – ECDLP). Відомо, що проблема ECDLP є більш складною, ніж вирішення проблема DLP [4, 7, 8]. В даний час кращі алгоритми для вирішення проблеми ECDLP мають експоненціальний час роботи, на відміну від алгоритмів для вирішення проблеми DLP, які мають субекспоненціальний час роботи. Це означає, що в системах на EC бажаний рівень безпеки може бути досягнуто при значно меншій довжині ключа.

Модифікація схеми електронного підпису Ніберга-Рюпеля на основі еліптичних кривих над полем $GF(2^m)$ показано на рис. 4.2.

Обирається $E(a, b)$ або $E(a, b, c)$ – еліптична крива поля $GF(2^m)$; G – точка цієї кривої; n – порядок групи кривої; k – особистий ключ відправника. Відкритий ключ Y обчислюється на базі особистого ключа k: $Y = kG \pmod{f(x), 2}$.

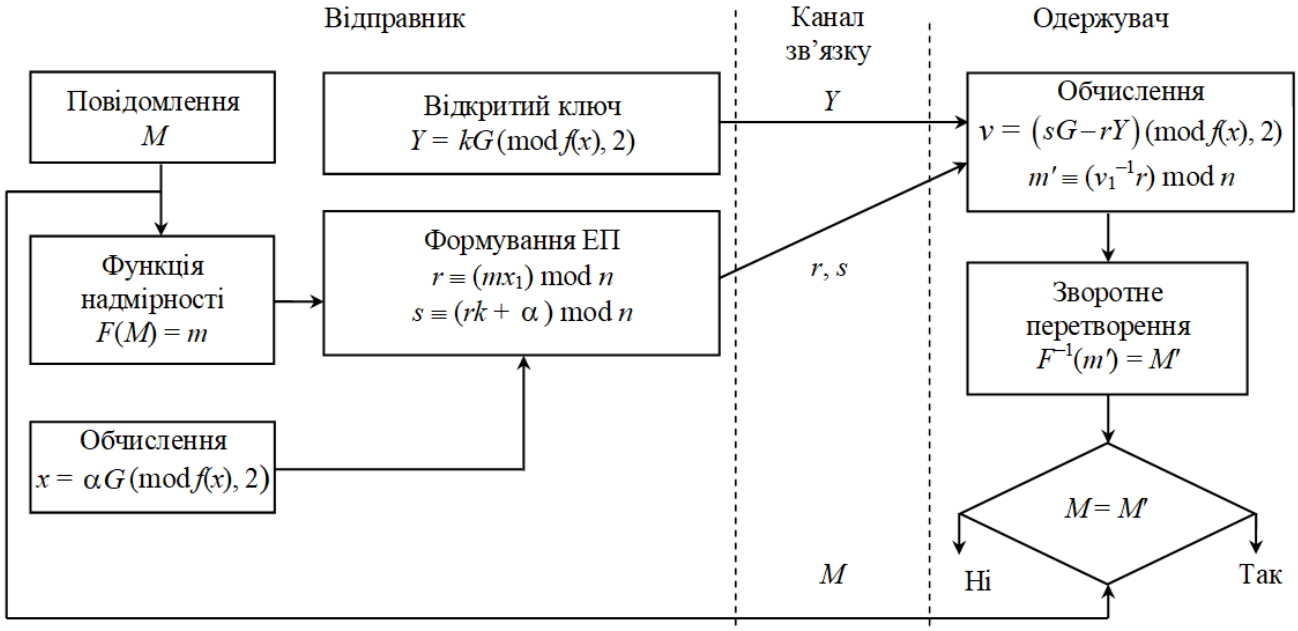

Рисунок 4.2 − Модифікація схеми електронного підпису Ніберга-Рюпеля

Для підпису повідомлення M відправник може скористатися наступним методом:

– обчислює $F(M) = m$;

– обирає випадкове число α і обчислює параметр $x = \alpha G \pmod{f(x), 2}$;

– обчислює перший параметр підпису $r \equiv (mx_1) \bmod n$;

– обчислює другий параметр підпису $s \equiv (rk + \alpha) \bmod n$.

Підписом повідомлення M є пара значень (r, s) які передається одержувачеві.

Перевірка підпису. Нехай прийнято повідомлення M і його ЕП з параметрами (r, s). Одержувач обчислюється величини v і m':

$$v = \left(sG - rY\right) \pmod{f(x), 2};$$

$$m' \equiv (v_1^{-1} r) \bmod n.$$

Одержувач виконує зворотне перетворення $F^{-1}(m') = M'$ та перевіряє рівність $M' = M$, якщо рівність виконується, то підпис є справжній.

Доказ коректності підпису Ніберга-Рюпеля:

$$v = \left(sG - rY\right) \pmod{f(x), 2} = \left[\left(rk + \alpha\right)G - rkG\right] \pmod{f(x), 2} =$$

$$= \left[rkG + \alpha G - rkG\right] \pmod{f(x), 2} = \alpha G \pmod{f(x), 2} = x;$$

$$m' \equiv (v_1^{-1} r) \bmod n \equiv (x_1^{-1} m x_1) \bmod n \equiv m.$$

Приклад електронного підпису Ніберга-Рюпеля на основі еліптичних кривих над полем $GF(p)$. Нехай $E_{1009}(-3, 63)$, що відповідає кривій $y^2 = x^3 - 3 + 63$; $p = 1009$; $n = 967$; $G = (211, 75)$; $M = 50$; $\alpha = 137$; $k = 311$; $F(M) = 450$.

Відправник обчислює Y і x:

$$Y = 311(211, 75) = (807, 900);$$
$$x = 137(211, 75) = (75, 753)/$$

Переходить до обчислення підпису. Розрахунок параметрів r і s:

$$r \equiv (450 \cdot 75) \bmod 967 \equiv 872;$$
$$s \equiv (872 \cdot 311 + 137) \bmod 967 \equiv 569.$$

Формується підписане повідомлення $M = 50$ у вигляді (872, 569), яке передається одержувачеві.

Перевірка підпису. Обчислюються величини v і m':

$$v = 569(211, 75) - 872(807, 900) = (202, 290) - (924, 772) \equiv (75, 753);$$
$$m' \equiv (75^{-1} \cdot 872) \bmod 967 \equiv (606 \cdot 872) \bmod 967 \equiv 450.$$

Одержувач виконує зворотне перетворення

$$M' = F^{-1}(450) = 450 : 9 = 50$$

та перевіряє рівність $M' = M = 50$ – підпис є справжній.

ВИСНОВКИ ТА РЕКОМЕНДАЦІЇ

Сучасний прогрес у глобальних комунікаціях в бізнесі та на повсякдень викликав виникнення нової сфери взаємодії, де відбувається електронний обмін даними. Цей обмін можуть здійснювати державні органи, комерційні та некомерційні організації, а також громадяни в рамках своїх офіційних та особистих відносин.

Однією з поширених засобів захисту електронних даних є використання електронного підпису. Цей засіб, завдяки спеціальному програмному забезпеченню, підтверджує надійність інформації в документі, його характеристик та факту підписання конкретною особою.

У магістерській роботі розглянуто методи побудови схем електронного підпису, приведені опис і розрахунки схем. Для розрахунків були обрані такі схеми електронного підпису: RSA, Ель-Гамаля, Шнорра, DSA. Для аналізу схем електронного підпису були обрані наступні схеми: RSA, Ель-Гамаля, Шнорра, DSA, ДСТУ 4145-2002, Ніберга-Рюпеля.

У роботі запропоновано модифікацію електронного підпису Ніберга-Рюпеля на основі еліптичних кривих. Визначено коректність підпису. Основними перевагами підпису є:

– набагато менша довжина ключа в порівнянні з класичною версію підпису Ніберга-Рюпеля;

– швидкодія програмної й апаратної реалізації, що дозволяє використовувати підпис на пристроях з обмеженими обчислювальними ресурсами (наприклад електронних магазинах тощо);

– дозволяє використовувати підпис в інфраструктурах з відкритими ключами.

Для впровадження запропонованого підпису можна використовувати рекомендовані еліптичні криві:

– FIPS 186-4 (Appendix D: NIST Recommended Elliptic Curves) [10];

– SEC 2: Recommended Elliptic Curve Domain Parameters [11];

– згідно ДСТУ 4145-2002.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Закон України «Про електронні довірчі послуги» від 14.01.2020 № 440-IX. – [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2155-19/print

2. Горбенко Ю.І., Горбенко І.Д. Інфраструктури відкритих ключів. Електронний цифровий підпис. Теорія та практика: монографія, Харків: Видавництво «Форт», 2020 – 608 с.

3. Йона Л. Г., Онацький О. В., Швець О. В. Системи банківської безпеки: Навч. посібник. – Одеса: ДУІТЗ, 2022. – 192 с.

4. Горбенко І. Д., Горбенко Ю. І. Прикладна криптологія. Теорія. Практика: монографія. – Харків: Видавництво «Форт», 2022. – 880 с.

5. Schneier B. Applied Cryptography: Protocols, Algorithms and Source Code in C: 20th Anniversary Edition. Wiley, 2015. – 784 p.

6. Stavroulakis P., Stamp M. Handbook of Information and Communication Security. Berlin: Springer-Verlag, 2015. – 863 p.

7. Stallings W. Cryptography and Network Security: Principles and Practice. Global Edition. 8th edition. Published by Pearson, 2023. 832 p.

8. ДСТУ 4145-2002. [Електронний ресурс]. – Режим доступу: https://uk. wikipedia.org/wiki/ДСТУ_4145-2002

9. Онацький О.В., Сербин Д.В., Жарова О.В. Модифікація електронного підпису Ніберга-Рюпеля з відновленням повідомлення // Modern research in science and education. Proceedings of the 4th International scientific and practical conference. BoScience Publisher. Chicago, USA. 2023. Pp. 299–302.

10. Federal information processing standards publication 186-4 «Digital Signature standard». National Institute of Standards and Technology issued July 2013 – [Електронний ресурс]. – Режим доступу: https://csrc.nist.gov/publications/detail/fips/186/4/final

11. SEC 2: Recommended Elliptic Curve Domain Parameters. [Електронний ресурс]. – Режим доступу: https://www.secg.org/SEC2-Ver-1.0.pdf

12. Положення про підготовку та захист кваліфікаційних робіт бакалаврів та магістрів: методичний посібник / І.В. Стрелковська, І.М. Соловська, Т.І. Григор'єва, В.І. Гура, Д.М. Розенвассер – МГУ. 2023 – 45 с.