МІНІСТЕРСТВО ОСВІТИ І НАУКИ,
МОЛОДІ ТА СПОРТУ УКРАЇНИ

Запорізький національний технічний університет

Методичні вказівки

до лабораторних робіт з дисципліни
“Криптографічні засоби захисту інформації”
для студентів спеціальностей 6.170101 "Безпека
інформаційних і комунікаційних систем " і
6.170102 "Системи технічного захисту інформації",
до лабораторних робіт з дисципліни “Методи
криптоаналізу” для магістрів спеціальності
8.160105 "Захист інформації в комп’ютерних
системах та мережах"

Частина VI

2012

Методичні вказівки до лабораторних робіт з дисципліни “Криптографічні засоби захисту інформації” для студентів спеціальностей 6.170101 "Безпека інформаційних і комунікаційних систем " і 6.170102 "Системи технічного захисту інформації", до лабораторних робіт з дисципліни “Методи криптоаналізу” для магістрів спеціальності 8.160105 "Захист інформації в комп’ютерних системах та мережах". Частина VI /Укл.: Г.Л.Козіна, Г.В. Неласа. – Запоріжжя: ЗНТУ, 2012. – 54 с.

Укладачі: Г.Л.Козіна, доцент, к.ф.-м.н.
Г.В. Неласа, доцент, к.т.н.

Рецензент: Л.М. Карпуков, проф., д.т.н.

Відповідальний
за випуск: Г.Л.Козіна, доцент, к.ф.-м.н.

Затверджено
на засіданні вченої ради
радіоприладобудівного
факультету

Протокол № 2
від 17.11.2011 р.

Затверджено
на засіданні кафедри
“Захист інформації”

Протокол № 3
від 26.10.2011 р.

ЗМІСТ

Вступ.....4

Лабораторна робота №1.
Протокол сліпого підпису 5

Лабораторна робота №2.
Протокол колективного підпису ……7

Лабораторна робота №3.
Протокол композиційного підпису ...……9

Лабораторна робота №4.
Дослідження анонімності в протоколі сліпого підпису 11

Лабораторна робота №5.
Криптографічні перетворення на гіпереліптичних кривих.....14

Лабораторна робота №6.
Протокол цифрового підпису на гіпереліптичних кривих……...16

Література……...18

Додаток А Сліпий підпис ..…….....21

Додаток Б Колективний підпис ……..26

Додаток В Композиційний підпис……...….....31

Додаток Г Приклад перевірки на анонімність схеми сліпого підпису 36

Додаток Д Елементи теорії дивізорів гіпереліптичних кривих ……...38

Додаток Е Протокол цифрового підпису на гіпереліптичних кривих..48

Додаток Ж Процедури групової операції на гіпереліптичних кривих……..51

ВСТУП

На сьогоднішній день в Україні вже є можливість довести юридичну значимість електронних документів, підписаних за допомогою цифрового ключа. Цьому, безумовно, сприяли Закон України «Про електронні документи та електронний документообіг» [1], що встановлює основні організаційно-правові положення електронного документообігу й використання електронних документів, і закон України «Про електронний цифровий підпис» [2], що визначає правовий статус електронного цифрового підпису й регулюючі відносини, які виникають при використанні електронного цифрового підпису.

По визначенню закону України [2], електронний цифровий підпис - це вид електронного підпису, отриманого в результаті певного криптографічного перетворення деякого набору даних, що додається до цього набору або логічно з ним зв'язується й дає можливість підтвердити його цілісність і ідентифікувати підписувача.

Кінцеві користувачі, для яких і створюється інформаційний сервіс, мають потреби у використанні ресурсів мереж різної приналежності для рішення своїх задач. Тому в цей час можна говорити про реальну інтеграцію відомчих, комерційних і загальнонаціональних інформаційних мереж. Необхідний рівень безпеки взаємодії мереж при збереженні доступності до їхніх ресурсів, як показує закордонний досвід, сьогодні вирішується шляхом побудови (впровадження й використання) [3,4] інфраструктури відкритих ключів (ІВК).

Розвиток цього напрямку розглядається, як одна із стратегічних задач інформатизації багатьох промислово розвинених держав. Відповідна програма розвитку Національної інфраструктури відкритих ключів, розвиток якої почався з впровадження системи електронного цифрового підпису, реалізується й в Україні. На сьогоднішній день вже зареєстровано ряд центрів сертифікації ключів таких, як УНИС [5], IVK [6], УСЦ [7], УСС [8], Masterkey [9]. Кожний із центрів пройшов акредитацію, перевірку виконання вимог безпеки й одержав посвідчення про державну акредитацію в Центральному засвідчуваному органі.

Різні схеми цифрового підпису потребують подальшого дослідження для можливості впровадження їх в існуючу ІВК.

ЛАБОРАТОРНА РОБОТА № 1
ПРОТОКОЛ СЛІПОГО ПІДПИСУ

Мета роботи: ознайомитися з протоколом сліпого підпису в групі точок еліптичної кривої над простим полем $GF(p)$ на базі алгоритму цифрового підпису ЕльГамаля.

Використовуване програмне забезпечення: пакет математичних обчислень Maple, функція хешування hash.exe.

1.1 Завдания на лабораторну роботу

Дано загальні параметри підпису:
основне поле – скінченне поле $GF(59)$;
еліптична крива над основним полем

$$y^2 = x^3 + 5x + 9 \bmod 59 .$$

Базова точка еліптичної кривої $P = (0,3)$ має порядок $n = 73$, $|n| = 7$.

Підписувач А має особистий ключ $d = 15$ та відповідний йому відкритий ключ $Q = (34,22)$.

1. Сформуйте сліпий підпис під повідомленням m у підписувача А, так щоб А у момент формування підписи не міг ознайомитися із умістом повідомлення m (див. Додаток А).

Параметр *m* взяти із таблиці згідно з номером варіанта N:

N	1	2	3	4	5	6	7	8	9	10	11	12	13
m	16	34	27	10	5	23	17	7	68	32	41	19	25
N	14	15	16	17	18	19	20	21	22	23	24	25	26
m	58	48	3	67	20	31	45	70	7	39	14	52	40

Для отримання хеш-образу використайте програму hash.exe. В якості функції хешування оберіть функцію MD5. Молодші $|n|-1=6$ розрядів 128-бітного значення функції MD5 формують параметр схеми сліпого підпису h.

2. Перевірить сліпий підпис, отриманий в п.1, з використанням відкритого ключа абонента А.

1.2 Зміст звіту

1. Титульний лист, тема і мета роботи.
2. Обрані значення параметрів.
3. Проведені обчислення.
4. Сформовані відкритий та секретний ключі.
5. Сформований сліпий підпис.
6. Результат перевірки підпису.
7. Висновки по роботі.

1.3 Контрольні питання

1. Дайте визначення поняття сліпого цифрового підпису.
2. Сформулюйте визначення поняття анонімності сліпого цифрового підпису.
3. Яке призначення сліпого підпису?
4. Опишіть властивості сліпого підпису.
5. Опишіть процедуру формування сліпого цифрового підпису.
6. Опишіть процедуру перевірки сліпого цифрового підпису.
7. Чи можливо побудова схем сліпого підпису із використанням російського та українського стандартів підпису?
8. Перевірте на анонімність сліпий підпис, схема якого наведена в Додатку А.

ЛАБОРАТОРНА РОБОТА № 2
ПРОТОКОЛ КОЛЕКТИВНОГО ПІДПИСУ

Мета роботи: ознайомлення з протоколом колективного підпису на базі російського стандарту підпису ГОСТ 34.10- 2001.

Використовуване програмне забезпечення: пакет математичних обчислень Maple.

2.1 Завдания на лабораторну роботу

Дано загальні параметри підпису:
основне поле – скінченне поле $GF(43)$;
еліптична крива над основним полем

$$y^2 = x^3 + 6x + 5 \mod 43.$$

Базова точка еліптичної кривої P має порядок $n = 37$.
Кількість підписувачів в схемі колективного підпису $t = 3$.
Допоміжне просте багаторозрядне двійкове число $\delta = 7$.

1. Згенерувати відкритий та секретний ключі для кожного підписувача за схемою ГОСТ Р 34.10 – 2001 (див. Додаток Б).

2. Обчисліть колективний цифровий підпис згідно з протоколом, наведеним в Додатку Б.

3. Перевірить колективний цифровий підпис, отриманий в п.2, з використанням відкритих ключів підписувачів (п.1).

Значення базової точки P та хеш-образу h візьміть із таблиці згідно з номером варіанта N:

N	P	h
1	(2,38)	15
2	(13,42)	4
3	(26,8)	21
4	(30,40)	10
5	(20,16)	18

N	P	h
6	(14,34)	25
7	(8,7)	12
8	(37,21)	7
9	(28,25)	22
10	(24,16)	18

N	P	h
11	(18,21)	3
12	(29,31)	16
13	(9,10)	29
14	(5,17)	27
15	(42,37)	30

N	*P*	*h*
16	(22,32)	31
17	(35,2)	14
18	(31,21)	6
19	(31,22)	9
20	(35,41)	35

N	*P*	*h*
21	(22,11)	13
22	(42,16)	16
23	(5,26)	17
24	(9,33)	3
25	(29,12)	7

N	*P*	*h*
26	(18,22)	9
27	(24,27)	11
28	(28,18)	33
29	(37,22)	35
30	(8,36)	18

2.2 Зміст звіту

1. Титульний лист, тема і мета роботи.
2. Обрані значення параметрів.
3. Проведені обчислення.
4. Сформовані відкриті та секретні ключі.
5. Сформований колективний підпис.
6. Результат перевірки підпису.
7. Висновки по роботі.

2.3 Контрольні питання

1. Дайте визначення поняття колективного цифрового підпису.
2. Назвіть властивості колективного цифрового підпису.
3. Як формується колективний відкритий ключ в наведеному протоколі?
4. Опишіть процедуру формування колективного цифрового підпису.
5. Опишіть процедуру перевірки колективного цифрового підпису.
6. Чи є обмеження по кількості підписувачів у схемах колективного цифрового підпису?
7. Чи обов'язкова перевірка коректності формування відкритих ключів в схемах колективного цифрового підпису при реєстрації цих ключів в центрі сертифікації?
8. Чи можлива побудова схем колективного цифрового підпису із використанням американських стандартів підпису?
9. У чому складається перевірка коректності роботи протоколу цифрового підпису?

ЛАБОРАТОРНА РОБОТА № 3
ПРОТОКОЛ КОМПОЗИЦІЙНОГО ПІДПИСУ

Мета роботи: ознайомлення з протоколом композиційного підпису на базі російського стандарту підпису ГОСТ 34.10- 2001.

Використовуване програмне забезпечення: пакет математичних обчислень Maple.

3.1 Завдания на лабораторну роботу

Дано загальні параметри підпису:
основне поле – скінченне поле $GF(43)$;
еліптична крива над основним полем

$$y^2 = x^3 + 6x + 5 \mod 43.$$

Базова точка еліптичної кривої $P = (8,36)$ має порядок $n = 37$.
Кількість підписувачів в схемі колективного підпису $t = 3$.
Допоміжне просте багаторозрядне двійкове число $\delta = 13$.

1. Згенерувати відкритий та секретний ключі для кожного підписувача за схемою ГОСТ Р 34.10 – 2001 (див. Додаток В).
2. Обчисліть композиційний цифровий підпис згідно з протоколом, наведеним в Додатку В.
3. Перевірить композиційний цифровий підпис, отриманий в п.2, з використанням відкритих ключів підписувачів (п.1).

Значення хеш-образів h_1, h_2, h_3 візьміть із таблиці згідно з номером варіанта N:

N	h_1, h_2, h_3
1	2,38,15
2	13,42,4
3	26,8,21
4	30,40,10

N	h_1, h_2, h_3
5	20,16,3
6	14,34,25
7	8,7,12
8	37,21,7

N	h_1, h_2, h_3
9	28,25,22
10	24,16,12
11	18,21,3
12	29,31,16

N	h_1, h_2, h_3
13	9,10,29
14	5,17,27
15	42,37,30
16	22,32,31

N	h_1, h_2, h_3
17	35,2,14
18	31,21,6
19	31,22,9
20	35,41,31

N	h_1, h_2, h_3
21	22,11,13
22	32,16,15
23	5,26,17
24	9,33,3

N	h_1, h_2, h_3
25	29,12,7
26	18,22,9
27	24,27,11
28	28,18,33

N	h_1, h_2, h_3
29	37,22,35
30	8,36,18
31	15,2,30
32	22,6,34

3.2 Зміст звіту

1. Титульний лист, тема і мета роботи.
2. Обрані значення параметрів.
3. Проведені обчислення.
4. Сформовані відкриті та секретні ключі.
5. Сформований композиційний підпис.
6. Результат перевірки підпису.
7. Висновки по роботі.

3.3 Контрольні питання

1. Дайте визначення поняття композиційного цифрового підпису.
2. Назвіть властивості композиційного цифрового підпису.
3. Чи є обмеження по кількості підписувачів у схемах композиційного цифрового підпису?
4. Чи можлива побудова схем композиційного цифрового підпису із використанням американських стандартів підпису?
5. Чім відрізняється композиційний цифровий підпис від колективного?
6. Які параметри схеми є загальносистемними ?
7. Опишіть процедуру генерації ключів у протоколі композиційного цифрового підпису.
8. Опишіть процедуру формування композиційного цифрового підпису.
9. Опишіть процедуру перевірки композиційного цифрового підпису.
10. Які параметри впливають на криптостійкість підпису?

ЛАБОРАТОРНА РОБОТА № 4

ДОСЛІДЖЕННЯ АНОНІМНОСТІ В ПРОТОКОЛІ СЛІПОГО ПІДПИСУ

Мета роботи: здійснити перевірку протоколу сліпого підпису на анонімність.

Використовуване програмне забезпечення: пакет математичних обчислень Maple, функція хешування hash.exe.

4.1 Завдания на лабораторну роботу

Дано загальні параметри підпису:
основне поле – скінченне поле $GF(59)$;
еліптична крива над основним полем

$$y^2 = x^3 + 5x + 9 \bmod 59 .$$

Базова точка еліптичної кривої $P = (0,3)$ має порядок $n = 73$, $|n| = 7$.

Підписувач А має особистий ключ $d = 15$ та відповідний йому відкритий ключ $Q = (34,22)$.

Для отримання хеш-образу підписувач А використав програму hash.exe, де в якості функції хешування обрав функцію MD5. Параметри схеми сліпого підпису h були сформовані зі молодших $|n|-1 = 6$ розрядів 128-бітного значення функції MD5.

Підписувач А здійснив наосліп декілька підписів для різних користувачів B_i, згідно з протоколом, наведеним в Додатку А. Параметри обміну k, E, h_E, $\overline{m}$, $\overline{s}$ з користувачами він зберіг в базі даних (табл.4.1).

В подальшому підписувач А ознайомився з документом m з підписом $\langle R, s \rangle$, переконався, що саме він підписав цей документ.

За допомогою бази параметрів обміну з користувачами підписувач А спробував визначити, якій зі користувачів був емітентом документа m.

Таблиця 4.1 – Параметри обміну з користувачами підписувача А

	k	E	h_E	$\overline{m}$	$\overline{s}$		k	E	h_E	$\overline{m}$	$\overline{s}$
B_1	8	(35,44)	8	60	16	B_4	66	(39,46)	16	50	36
B_2	24	(46,15)	25	21	3	B_2	30	(12,33)	7	60	7
B_{11}	19	(17,13)	23	53	38	B_1	64	(43,50)	25	8	11
B_2	29	(56,12)	23	19	20	B_3	36	(13,41)	6	33	37
B_{10}	16	(37,44)	2	54	18	B_8	13	(1,29)	22	63	54
B_3	57	(37,15)	53	15	44	B_6	3	(41,20)	9	2	68
B_1	20	(45,33)	8	8	61	B_1	55	(19,1)	45	22	60
B_5	67	(23,14)	63	60	1	B_9	44	(56,47)	14	63	62
B_7	13	(1,29)	22	36	68	B_7	50	(2,26)	50	6	28
B_2	23	(2,33)	10	7	19	B_{12}	45	(28,34)	14	19	43

Таблиця 4.2 – Варіанти завдань

N	m	R	s
1	21	(45,26)	4
2	15	(12,33)	19
3	66	(3,13)	51
4	45	(33,11)	34
5	16	(40,31)	33
6	17	(13,18)	57
7	27	(26,29)	12
8	18	(41,39)	44
9	71	(42,47)	62
10	44	(27,11)	27
11	37	(26,30)	47
12	15	(1,29)	14
13	29	(22,41)	8
14	40	(6,14)	11
15	23	(13,18)	60

N	m	R	s
16	30	(27,48)	4
17	31	(56,47)	41
18	5	(9,55)	64
19	67	(58,48)	4
20	9	(30,14)	21
21	36	(17,46)	25
22	64	(54,6)	54
23	24	(45,33)	18
24	57	(46,15)	64
25	32	(21,17)	62
26	52	(41,20)	42
27	24	(28,34)	49
28	62	(46,15)	38
29	16	(20,12)	10
30	42	(49,32)	17

1. Перевірить, чі належить сліпий підпис $\langle R, s \rangle$ під документом m підписувачу А.

2. За допомогою бази (табл. 4.1) параметрів обміну з користувачами визначити емітента документа m.

Значення документа m і підпису $\langle R, s \rangle$ візьміть із таблиці 4.2 згідно з номером варіанта N.

4.2 Зміст звіту

1. Титульний лист, тема і мета роботи.
2. Результат перевірки підпису.
3. Таблиця проведених обчислень.
4. Висновки по роботі.

4.3 Контрольні питання

1. Як перевірить приналежність сліпого підпису підписувачу А?
2. Чі можливо встановити емітента підписаного наосліп документу?
3. Опишіть алгоритм перевірки анонімності електронного документу.

ЛАБОРАТОРНА РОБОТА № 5

КРИПТОГРАФІЧНІ ПЕРЕТВОРЕННЯ НА ГІПЕРЕЛІПТИЧНИХ КРИВИХ

Мета роботи: ознайомитися з математичним апаратом гіпереліптичних кривих над простим полем Галуа. Використовуючи пакет Maple, виконати операції над дивізорами заданої кривої.

Використовуване програмне забезпечення: пакет математичних обчислень Maple.

5.1 Завдания на лабораторну роботу

Дано гіпереліптичну криву:

$$y^2 = x^5 + Nx^2 + (N-1)x + (N-2) \mod 37,$$

де N – номер варіанту.

1. Знайти усі точки кривої в полі $GF(37)$ з використанням функції **msolve** пакету Maple.
2. Побудувати випадковий дивізор D, як суму двох довільних точок. Представити його в формі Мамфорда (див. Додаток Д).
3. Побудувати підгрупу, породжену дивізором D, використовуючи процедури, що наведені в Додатку Ж.

5.2 Зміст звіту

1. Титульний лист, тема і мета роботи.
2. Точки кривої.
3. Обчислення дивізора.
4. Побудована підгрупа.
5. Порядок підгрупи.
6. Висновки по роботі.

5.3 Контрольні питання

1. Дати визначення гіпереліптичної кривої.
2. Наведіть визначення дивізора гіпереліптичної кривої.
3. Як визначити точку, обернену(протилежну) даній?
4. Дати визначення порядка групи точок гіпереліптичної кривої?
5. Дати визначення порядка дивізора гіпереліптичної кривої у визначеній точці?
6. Які дивізори є протилежними?
7. Що є степенем дивізора?
8. Який дивізор називається зведеним?
9. Як визначити базовий дивізор?
10. В чому полягає представлення дивізора у формі Мамфорда?
11. Дати визначення якобіану гіпереліптичної кривої.

ЛАБОРАТОРНА РОБОТА № 6

ПРОТОКОЛ ЦИФРОВОГО ПІДПИСУ НА ГІПЕРЕЛІПТИЧНИХ КРИВИХ

Мета роботи: ознайомитися з протоколом цифрового підпису на гіпереліптичних кривих. Використовуючи пакет Maple, виконати підписання та перевірку електронного документу.

Використовуване програмне забезпечення: пакет математичних обчислень Maple.

6.1 Завдання на лабораторну роботу

Дано гіпереліптичну криву:

$$y^2 = x^5 + Nx^2 + (N-1)x + (N-2) \mod 37,$$

де N – номер варіанту.

Нехай хеш-образ h повідомлення m визначається як сума ASCII кодів перших трьох літер Вашого Прізвища за модулем 37.

Наприклад, «Нел» $\rightarrow (8D_{16}, A5_{16}, AB_{16}) = (141_{10}, 165_{10}, 171_{10})$,

$h = (141 + 165 + 171) \bmod 37 = 33$.

1. Побудувати підгрупу дивізорів простого порядку (результат виконання лабораторної роботі №5).

2. Виконати підписання та перевірку підпису повідомлення m згідно з протоколом, наведеним в Додатку Е. Секретний ключ підписувача А визначити наступним чином: $d = N^2 \bmod 37$.

6.2 Зміст звіту

1. Титульний лист, тема і мета роботи.
2. Тексти програм.
3. Проведені обчислення.
4. Отриманий цифровий підпис.
5. Висновки по роботі.

6.3 Контрольні питання

1. Чим відрізняються криптографічні протоколи на еліптичних та гіпереліптичних кривих?
2. Які параметри гіпереліптичної кривої необхідно знати для її застосування?
3. Як Ви провели перетворення цілого числа на елемент основного поля?
4. Назвіть параметри криптографічних протоколів цифрового підпису на гіпереліптичних кривих.
5. Який вигляд може мати функція перетворення дивізора на елемент основного поля?
6. Який елемент в криптографічних протоколах цифрового підпису на гіпереліптичних кривих використовується в якості відкритого ключа?

ЛІТЕРАТУРА

1. Закон України ”Про електронні документи та електронний документообіг” [Електронний ресурс] : (Відомості Верховної Ради України (ВВР), 2003, N 36, ст.275) (Із змінами, внесеними згідно із Законом N 2599-IV (2599-15) від 31.05.2005, ВВР, 2005, N 26, ст.349), – Режим доступу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=851-15.

2. Закон України ”Про електронний цифровий підпис” [Електронний ресурс] : (Відомості Верховної Ради України (ВВР), 2003, N 36, ст.276) (Із змінами, внесеними згідно із Законом N 879-VI (879-17) від 15.01.2009, ВВР, 2009, N 24, ст.296) , – Режим доступу : http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=852-15.

3. Горбенко Ю.І. Інфраструктури відкритих ключів. Електронний цифровий підпис. Теорія та практика : монографія. / Горбенко Ю.І. Горбенко І.Д. – Харків : Видавництво «Форт», 2010. – 608 с.

4. Комп’ютерні технології криптографічного захисту інформації на спеціальних цифрових носіях. Навчальний посібник. / Задірака В.К., Кудін А.М., Людовиченко В.О., Олексюк О.С. — Київ- Тернопіль: Вид-во «Підручники і посібники», 2007. 272 с.

5. Специализированный центр сертификации ключей (СЦСК) общества с ограниченной ответственностью научно-производственной фирмы „Украинские национальные информационные системы” (УНИС) [Электронный ресурс] . – Режим доступу: www.unis.org.ua.

6. Центр сертификации ключей закрытого акционерного общества „Инфраструктура отрытых ключей” (ИВК) [Электронный ресурс] . – Режим доступу: www.ivk.org.ua.

7. Центр сертификации ключей «Украинский сертификационный центр» (УСЦ) [Электронный ресурс] . – Режим доступу: www.ukrcc.com.

8. Центр сертификации ключей „Центр автентификации национальной системы конфиденциальной связи” Государственного предприятия „Украинские специальные системы” (УСС) [Электронный ресурс] . – Режим доступу: www.uss.gov.ua.

9. Центр сертификации ключей «MASTERKEY» ООО «Арт-мастер» [Электронный ресурс] . – Режим доступу: www.masterkey.com.ua.

10. Молдовян Н.А. Теоретический минимум и алгоритмы цифровой подписи. СПб: БХВ-Петербург, 2010. – 304 с.

11. Запечников, С.В. Криптографические протоколы и их применение в финансовой и коммерческой деятельности. / С.В. Запечников. — М.: Горячая линия-телеком, 2007. – 320 с.

12. Кузнецов Г.В. Математичні основи криптографії / Г.В. Кузнецов, В.В. Фомичов, С.О. Сушко, Л.Я. Фомичова. – Дніпропетровськ: НГУ, 2006. – 391 с.

13. Смарт Н. Криптография. – М.: Техносфера, 2005. – 528 с.

14. Бессалов А.В. Криптосистемы на эллиптических кривых. Учебное пособие / А.В. Бессалов, А.Б. Тележенко. – Киев : Політехніка, 2004. – 223 с.

15. Горбенко І.Д. Захист інформації в інформаційно-телекомунікаційних системах. Част. 1. Криптографічний захист інформації. / Горбенко І.Д., Гриненко Т.О. — Харків: ХНУРЕ, 2004. – 367 с.

16. Chaum D. Blind signatures for untraceable payments / D. Chaum // Advances in Cryptology, Crypto '82. – Springer-Verlag. – 1983. – P. 199-203.

17. Ростовцев А.Г. Подпись "вслепую" на эллиптической кривой для электронных денег / А.Г. Ростовцев // Проблемы информационной безопасности. Компьютерные системы. – 2000. - № 1. – С. 40-45.

18. Молдовян Н.А. Новые протоколы слепой подписи / Н.А. Молдовян, П.А. Молдовян // Безопасность информационных технологий. – М.:МИФИ. – 2007. – № 3. – С. 17-21.

19. Информационная технология. Криптографическая защита информации. Функция хэширования: ГОСТ 34.311-95: 1995. - [Чинний від 1998-04-16]. К.: Держстандарт України, 1995. – 12 с. – (Межгосударственный стандарт).

20. Гортинская Л.В. Реализация протоколов коллективной подписи на основе стандартов ГОСТ 34.310-95 и ДСТУ 4145-2002 / Л.В. Гортинская, Н.А. Молдовян, Г.Л. Козина // Правове, нормативне та метрологичне забезпечення системи захисту інформації в Україні. – Киев : НТУУ “КПІ”. – 2008. – № 1. – С.82-86.

21. Артамонов А.В. Применение алгоритма Шнорра в протоколе коллективной подписи / А.В. Артамонов, Е.Б. Маховенко // Материалы XIV Всероссийской научной конференции «Проблемы информационной безопасности в системе высшей школы». – 2007. – С. 17-18.

22. Пат. 31105 Україна, МПК (2006) H03M 5/00, G09C 1/00, H03M 7/00. Спосіб формування і перевірки достовірності колективного електронного цифрового підпису для засвідчення електронного документа / Карпуков Л.М., Козіна Г.Л., Молдов’ян О.А., Молдов’ян М.А.; замовник і патентовласник Запорізький національний технічний університет. – № u200713254; заявл. 28.11.07; опубл. 25.03.08, Бюл. № 6.

23. Козіна Г.Л. Колективне підписання різних документів нерівноправними учасниками протоколу / Г.Л.Козіна, Л.М.Карпуков, Д.М.Піза, М.А. Молдов’ян //Захист інформації: науково-технічний журнал. – К:ДУІКТ, 2009. – № 3. – С. 74-80.

24. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи: ГОСТ Р 34.10-2001: 2001. – [Чинний від 2002-07-01]. М.: Госстандарт России, 2001. –16 с.

25. N. Koblitz. Hyperelliptic cryptosystem / N. Koblitz // Journal of Crypto. – 1989. – № 1. – P. 139-150.

26. Handbook of elliptic and hyperelliptic curve cryptography / Cohen H., Frey G., Avanzi R. et. al. . – Chapman & Hall/CRC : Taylor&Francis Group, 2005. – 808 p.

27. Menezes A. An Elementary Introduction to Hyperelliptic Curves [Электронный ресурс] / Menezes A., Wu Y., Zuccherato R. : Published as Technical Report CORR 96-19 Department of C&O University of Waterloo : Ontario : Canada,– 1996.- P. 1-35. – Режим доступу: www.cacr.math.uwaterloo.ca/techreports/1997/corr96-19.ps

28. Долгов В.И. Геометрический подход к сложению дивизоров гиперэллиптической кривой / В.И Долгов, А.В. Неласая // Радіоелектроніка. Інформатика. Управління. – 2007. – №2(18) . – С. 44-50.

29. Неласая А.В. Протокол цифровой подписи на гиперэллиптических кривых / А.В. Неласая // Радіоелектроніка. Інформатика. Управління. – 2006. - № 1(15). – С. 113-118.

30. Неласая А.В. Протоколы коллективной цифровой подписи на эллиптических и гиперэллиптических кривых / А.В. Неласая, Г.Л. Козина, Н.А. Молдовян // Радіоелектроніка. Інформатика. Управління. – 2008. – №1(19). - С.127-133.

31. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння: ДСТУ 4145: 2002. – [Чинний від 2002-03-13]. К.: Держстандарт України, 2002. – 38 с.: табл. – (Національний стандарт України).

Додаток А
Сліпий підпис

Розвиток інфраструктури відкритих ключів в Україні, створення регіональних центрів сертифікації ключів [5-9] дозволяє клієнтам отримати та надавати послуги електронного цифрового підпису. Крім класичної схеми [10-15] однократного цифрового підпису існують інші схеми, зокрема сліпий цифровий підпис [16-18].

Сліпий підпис лежить в основі криптосистем, у яких вирішується проблема забезпечення анонімності – системах таємного електронного голосування й системах електронних грошей.

Сліпим називається підпис, який сформовано під замаскованим повідомленням. В процесі підписання підписувач не має можливості ознайомиться зі змістом відкритого (незамаскованого) повідомлення.

Схеми сліпого підпису призначені для розв'язання задачі забезпечення анонімності (невідстежуваності) користувачів у системах електронної готівки й системах таємного електронного голосування.

Відомі протоколи сліпого підпису реалізуються на основі алгоритмів електронного цифрового підпису, що використають три обчислювальне складні задачі: факторизація натурального числа, знаходження дискретного логарифма по простому модулі, знаходження дискретного логарифма на еліптичній кривій.

В розглянутому протоколі використається в якості математичної структури група точок еліптичної кривої над скінченним полем. Протокол побудовано на базі відомого протоколу цифрового підпису ЕльГамаля. Стійкість протоколу заснована на складності задачі знаходження дискретного логарифма на еліптичній кривій.

Для хешування електронного документу може бути запропоновано використання стандарту [19] та інших.

Протокол сліпого підпису на базі алгоритму ЕльГамаля

Цей протокол [17] є модифікацією алгоритму ЕльГамаля для еліптичних кривих. Стійкість протоколу засновано на складності задачі знаходження дискретного логарифма на еліптичній кривій.

Користувач В підписує в підписувача А деяке повідомлення m, $0 < m < n$, так щоб А у момент формування підписи не міг ознайомитися із умістом повідомлення m.

Загальні параметри:

основне поле – скінченне поле $GF(p)$;

еліптична крива над основним полем

$$y^2 = x^3 + Ax + B \mod p,$$

де $A, B \in GF(p), B \neq 0,$ разом із приєднаною нескінченно віддаленою точкою O;

базова точка еліптичної кривої $P \neq \mathrm{O}$ простого порядку n, така що $nP = \mathrm{O}$ і $kP \neq \mathrm{O}, 0 < k < n$;

H – функція хешування.

Генерація ключів

Підписувач А має асиметричну пару ключів:

особистий $d : 1 < d < n$ та

відкритий $Q = d \cdot P$.

Формування сліпого підпису

Підписувач А обирає одноразовий випадковий секретний ключ k, $1 < k < n$, обчислює координати точки $E = k \cdot P$ та $H(E)$. Молодші $|n|-1$ розряди хеш-образу $H(E)$ формують десяткове число h_E. Далі підписувач А перевіряє умову $h_E \neq 0$ та надає точку E користувачу В. Якщо $h_E = 0$, підписувач А обирає інше значення k.

Користувач В перевіряє приналежність точки E еліптичній кривій, обирає випадкове число α, $1 < \alpha < n$, обчислює координати точки $R = \alpha \cdot E$ та $H(R)$. Молодші $|n|-1$ розряди хеш-образу $H(R)$ формують десяткове число h_R. Далі користувач В перевіряє умову $h_R \neq 0$ (якщо $h_R = 0$, користувач В обирає інше значення α), обчислює коефіцієнт $\beta = \dfrac{h_R}{h_E} \bmod n$, осліпляє повідомлення m:

$\overline{m} = \frac{\alpha}{\beta} m \bmod n$ та надає $\overline{m}$ підписувачу А. Якщо α співпадає з β користувач В має обрати інше значення α.

Підписувач А перевіряє умову $\overline{m} \neq 0$, обчислює підпис $\overline{s} = (h_E \cdot d + k \cdot \overline{m}) \bmod n$ та надає його користувачу В.

Користувач В перевіряє сформований підписувачем А підпис $\overline{s}$. Якщо $\overline{s}P = h_E \cdot Q + \overline{m} \cdot E$, сліпий цифровий підпис документу $\overline{m}$ признається справжнім. Далі користувач В обчислює підпис для документа m: $s = \beta \cdot \overline{s} \bmod n$.

Сліпим підписом є пара $\langle R, s \rangle$.

Перевірка сліпого підпису

Перевірка підпису $\langle R, s \rangle$ під електронним документом m здійснюється за допомогою відкритого ключа Q підписувача А.

Якщо $sP = h_R \cdot Q + m \cdot R$, де h_R – молодші $|n|-1$ розряди хеш-образу $H(R)$, сліпий цифровий підпис документу m признається справжнім.

Покажемо коректність пропонованого алгоритму формування і перевірки сліпого підпису:

$$sP = \beta \cdot \overline{s} \cdot P = \beta \cdot (d \cdot h_E + \overline{m} \cdot k) \cdot P = \beta \cdot h_E \cdot Q + m \cdot \alpha \cdot E =$$
$$= h_R \cdot Q + m \cdot R.$$

Приклад.

Оберемо загальні параметри:

основне поле – скінченне поле $GF(17)$;

еліптична крива над основним полем

$$y^2 = x^3 + 6x + 8 \bmod 17.$$

Дана еліптична крива містить 13 точок, тобто будь-яка її точка має порядок $n = 13$, $|n| = 4$.

Базова точка еліптичної кривої $P = (1,7)$.

Нехай користувач B бажає підписати у підписувача A повідомлення $m = 10$.

Генерація ключів

Нехай підписувач A має особистий ключ $d = 8$ та відповідний йому відкритий ключ $Q = (9,3)$.

Формування сліпого підпису

Підписувач A обирає одноразовий випадковий секретний ключ $k = 4$, обчислює координати точки $E = (3,6)$ та

$$H(E) = MD5("(3,6)") =$$

$$='4A9F50245A33E4429DD7B31E9C1F6240'.$$

Звідси $h_E = 0$. Оскільки $h_E = 0$, підписувач A має обрати інше значення k: $k = 5$. Далі підписувач A обчислює координати новій точки $E = (9,14)$ та

$$H(E) = MD5("(9,14)") =$$

$$='33BC083E4ED53C83903460C66655BBAD'.$$

Звідси $h_E = 5$ (молодші $|n| - 1 = 3$ розряди хеш-образу $H(E)$ становлять 101).

Підписувач A надає точку $E = (9,14)$ користувачу B.

Користувач B перевіряє приналежність точки E еліптичній кривій, обирає випадкове число $\alpha = 9$, обчислює координати точки $R = (16,16)$ та

$$H(R) = MD5("(16,16)") =$$

$$='C6F039988A718433AB1D5367484E9453'.$$

Звідси $h_R = 3$.

Далі користувач B обчислює коефіцієнт $\beta = 11$, осліпляє повідомлення m: $\overline{m} = 7$ та надає $\overline{m}$ підписувачу A.

Підписувач A обчислює підпис $\overline{s} = 10$ та надає його користувачу B.

Користувач B перевіряє сформований підписувачем A підпис $\overline{s}$: обчислює $\overline{s}P = (0,12)$ і $h_E \cdot Q + \overline{m} \cdot E = (1,7) + (3,11) = (0,12)$. Оскільки $\overline{s}P = h_E \cdot Q + \overline{m} \cdot E$, сліпий цифровий підпис документу $\overline{m}$ признається справжнім. Далі користувач B обчислює підпис для документа m: $s = 6$.

Сліпим підписом є пара $\langle R, s \rangle = \langle (16,16),6 \rangle$.

Перевірка сліпого підпису

Перевірка підпису $\langle R, s \rangle = \langle (16,16),6 \rangle$ під електронним документом $m = 10$ здійснюється за допомогою відкритого ключа $Q = (9,3)$ підписувача A.

Обчислюється хеш-образ $H(R)$ точки R та відповідне число $h_R = 3$. Далі обчислюються $sP = (16,16)$,

$h_R \cdot Q + m \cdot R = (7,6) + (9,3) = (16,16)$.

Оскільки $sP = h_R \cdot Q + m \cdot R$, сліпий цифровий підпис документу m признається справжнім.

Додаток Б
Колективний підпис

При формуванні електронних документів у ряді випадків виникає необхідність підписування документів декількома учасниками. Підпис, сформований колективом рівноправних учасників підписання під спільним документом, називається *колективним*.

Схеми колективного підпису призначені для розв’язання задачі одночасного підписання контрактів і скорочення розміру підписів до документів, що підписуються двома й більше суб'єктами. Особливо актуальним є питання про скорочення розміру підпису у випадках, коли електронний цифровий підпис вноситься в шрих-код або іншу машиночитаєму мітку, що наноситься на матеріальний об'єкт, наприклад паперовий документ.

В протоколі колективного підпису здійснюється обмін відкритими параметрами по мережах зв’язку, причому кожен учасник створює свою частину підпису, після чого формується колективний підпис. Для перевірки колективного підпису формується колективний відкритий ключ, який залежить від відкритих ключів учасників підписання електронного документа.

На сьогодні з'явилися нові схеми колективного цифрового підпису в різних постановах [20-23]. В розглянутому протоколі використається в якості математичної структури група точок еліптичної кривої над скінченним полем. Протокол побудовано на базі російського стандарту цифрового підпису ГОСТ Р34.10-2001 [24]. Стійкість протоколу заснована на складності задачі знаходження дискретного логарифма на еліптичній кривій. Для хешування електронного документу може бути запропоновано використання стандарту [19] та інших.

Важливою особливістю протоколу є те, що при компрометації секретних ключів частини учасників складність задачі формування підробленого підпису й обчислення секретних ключів останніх учасників не знижується.

Протокол колективного цифрового підпису електронного документу на еліптичної кривої над простим полем

Цей протокол [22] заснований на російському стандарті цифрового підпису ГОСТ Р34.10-2001. Введення допоміжного числа δ дозволяє скоротити першу частину цифрового підпису.

Загальні параметри:

основне поле – скінченне поле $GF(p)$;

еліптична крива над основним полем

$$y^2 = x^3 + Ax + B \mod p,$$

де $A, B \in GF(p), B \neq 0,$ разом із приєднаною нескінченно віддаленою точкою O;

базова точка еліптичної кривої $P \neq \mathrm{O}$ простого порядку n, така що $nP = \mathrm{O}$ і $kP \neq \mathrm{O}, 0 < k < n$;

H – функція хешування;

δ – допоміжне просте багаторозрядне двійкове число.

Генерація ключів

Кожний i-ий ($i = 1,2,...,t$) користувач має асиметричну пару ключів:

особистий $d_i : 1 < d_i < n$ та

відкритий $Q_i = d_i P$.

Формування колективного підпису

Нехай колектив користувачів, $i = 1,2,...,t$, має підписати електронний документ M з хеш-образом $H(M)$. Молодші $|n|-1$ розряди хеш-образу $H(M)$ формують десяткове число h, яке використається при обчисленні цифрового підпису.

Кожний підписувач обирає одноразовий випадковий секретний ключ k_i, $1 < k_i < n$, обчислює координати точки

$$R_i = k_i P$$

та надає їх для колективного використання.

Далі обчислюється сума всіх точок R_i, $i = 1,2,...,t$:

$$R = \sum_{i=1}^{t} R_i = (xR, yR),$$

після чого формується число

$$r = h \cdot xR \bmod \delta.$$

При $r = 0$ обираються нові випадкові секретні ключі k_i.

Потім кожний користувач i за допомогою свого особистого ключа d_i та значення k_i обчислює свою долю підпису

$$s_i = k_i - d_i \cdot r \bmod n,$$

після чого генерується підпис s:

$$s = \sum_{i=1}^{t} s_i \bmod n.$$

Число s не може бути рівним 0. При $s = 0$ процедура підпису повторюється.

Колективним підписом є пара чисел $\langle r, s \rangle$.

Перевірка колективного підпису

Перевірка підпису $\langle r, s \rangle$ під електронним документом M здійснюється за допомогою додаткової точки еліптичної кривої

$$Q = \sum_{i=1}^{t} Q_i,$$

яка залежить від відкритих ключів Q_i учасників підписання.

Обчислюється точка $\widetilde{R}$ еліптичної кривої

$$\widetilde{R} = sP + rQ = (x\widetilde{R}, y\widetilde{R})$$

після чого обчислюються хеш-образ документу $H(M)$, відповідне десяткове число h та формується число

$$\tilde{r} = h \cdot x\tilde{R} \bmod \delta .$$

Якщо $\tilde{r} = r$, колективний цифровий підпис електронного документу M признається справжнім.

Покажемо коректність пропонованого алгоритму формування і перевірки колективного підпису:

$$\tilde{R} = sP + rQ = \left(\sum_{i=1}^{t} s_i\right)P + r\left(\sum_{i=1}^{t} Q_i\right) = \left(\sum_{i=1}^{t} k_i - d_i r\right)P + r\left(\sum_{i=1}^{t} d_i P\right) =$$

$$= \left(\sum_{i=1}^{t} k_i\right)P = \sum_{i=1}^{t} R_i = R.$$

Оскільки $\tilde{R} = R$, то і $\tilde{r} = r$.

Приклад.

Оберемо загальні параметри:

основне поле – скінченне поле $GF(17)$;

еліптична крива над основним полем $y^2 = x^3 + 2x + 6 \mod 17$.

Базова точка еліптичної кривої $P = (2,1)$ має порядок $n = 11$.

Допоміжне просте багаторозрядне двійкове число $\delta = 7$.

Генерація ключів

Нехай число користувачів $t = 2$.

Відповідні особисті ключі є $d_1 = 8$, $d_2 = 5$.

Тоді відкрити ключі $Q_1 = (6,8)$, $Q_2 = (1,3)$.

Формування колективного підпису

Нехай хеш-образ електронного документу M дорівнює $h = 9$.

Кожний підписувач обирає одноразовий випадковий секретний ключ k_i: $k_1 = 3$, $k_2 = 4$, та обчислює координати точки R_i: $R_1 = (6,9)$, $R_2 = (13,11)$.

Далі обчислюється R – сума всіх точок R_i: $R = (13,6)$, після чого формується число r:

$$r = 9 \cdot 13 \bmod 7 = 5,\ r = 5.$$

Потім кожний користувач i за допомогою свого особистого ключа d_i та значення k_i обчислює свою долю підпису:

$$s_1 = 3 - 8 \cdot 5 \bmod 11 = 7,\ s_1 = 7,$$

$$s_2 = 4 - 5 \cdot 5 \bmod 11 = 1,\ s_2 = 1,$$

після чого генерується підпис s: $s = 8$.

Колективним підписом є пара чисел $\langle r, s \rangle = \langle 5,8 \rangle$.

Перевірка колективного підпису

Перевірка підпису $\langle r, s \rangle = \langle 5,8 \rangle$ під електронним документом M здійснюється за допомогою додаткової точки еліптичної кривої Q, яка залежить від відкритих ключів Q_i учасників підписання: $Q = (11,4)$.

Обчислюється точка $\widetilde{R}$ еліптичної кривої:

$$sP = (6,8),\ rQ = (2,16),$$

$$\widetilde{R} = (13,6).$$

Далі обчислюються хеш-образ документу $H(M)$, відповідне десяткове число $h = 9$ та формується число

$$\widetilde{r} = 9 \cdot 13 \bmod 7 = 5,\ \widetilde{r} = 5.$$

Оскільки $\widetilde{r} = r$, колективний цифровий підпис електронного документу M признається справжнім.

Додаток В
Композиційний підпис

Якщо учасники підписання не є рівноправними, може виникнути необхідність підписання різних документів групою осіб, кожна із котрих має право підписувати тільки свій документ. Наприклад, директор, бухгалтер, завідувач відділу кадрів, технолог підписують кожний свій електронний документ с використанням свого особистого ключа. С метою зменшення довжини підпису пропонується формування єдиного, *композиційного*, підпису різних документів на базі елементів особистих підписів [22,23]. Перевірка такого композиційного підпису потребує знання відкритих ключів кожного із учасників підписання і відповідних кожному електронних документів.

Схеми композиційного підпису мають призначення, аналогічне призначенню колективних підписів, але надають розширені можливості: одночасне підписання пакета контрактів і підписання різних документів різними підмножинами користувачів, що брали участь у формуванні єдиного пакета документів.

В розглянутому протоколі використається в якості математичної структури група точок еліптичної кривої над скінченним полем. Протокол побудовано на базі російського стандарту цифрового підпису ГОСТ Р34.10-2001 [24]. Стійкість протоколу заснована на складності задачі знаходження дискретного логарифма на еліптичній кривій. Для хешування електронного документу може бути запропоновано використання стандарту [19] та інших.

Протокол композиційного цифрового підпису різних документів на еліптичної кривої над простим полем

Цей протокол [22] є модифікацією російського стандарту цифрового підпису ГОСТ Р34.10-2001. Введення допоміжного числа δ дозволяє скоротити першу частину цифрового підпису.

Загальні параметри:

основне поле – скінченне поле $GF(p)$;

еліптична крива над основним полем

$$y^2 = x^3 + Ax + B \mod p,$$

де $A, B \in GF(p), B \neq 0,$ разом із приєднаною нескінченно віддаленою точкою O;

базова точка еліптичної кривої $P \neq O$ простого порядку n, така що $nP = O$ і $kP \neq O, 0 < k < n$;

H – функція хешування;

δ – допоміжне просте багаторозрядне двійкове число.

Генерація ключів

Кожний i-ий ($i = 1,2,...,t$) користувач має асиметричну пару ключів:

особистий $d_i : 1 < d_i < n$ та

відкритий $Q_i = d_i P$.

Формування композиційного підпису

Нехай колектив із t користувачів має створити композиційний підпис під набором електронних документів $\{M_1, M_2, ..., M_t\}$, причому кожен користувач i, $i = 1,2,...,t$, має підписати свій електронний документ M_i з хеш-образом $H(M_i)$. Молодші $|n|-1$ розряди хеш-образу $H(M_i)$ формують десяткове число h_i, яке використається при обчисленні цифрового підпису.

Кожний підписувач обирає одноразовий випадковий секретний ключ k_i, $1 < k_i < n$, обчислює координати точки

$$R_i = k_i P$$

та надає їх для подальшого використання.

Далі обчислюється сума всіх точок R_i, $i = 1,2,...,t$:

$$R = \sum_{i=1}^{t} R_i = (xR, yR),$$

після чого формується число

$$r = xR \bmod \delta.$$

При $r = 0$ обираються нові випадкові секретні ключі k_i.

Потім кожний користувач i за допомогою свого особистого ключа d_i, значення k_i, хеш-образу h_i та числа r обчислює свою долю підпису

$$s_i = k_i - d_i \cdot h_i \cdot r \bmod n,$$

після чого генерується підпис s:

$$s = \sum_{i=1}^{t} s_i \bmod n.$$

Параметр підпису s не може бути рівним 0. При $s = 0$ процедура підпису повторюється.

Композиційним підписом є пара чисел $\langle r, s \rangle$.

Перевірка композиційного підпису

Перевірка підпису $\langle r, s \rangle$ під електронними документами $\{M_1, M_2, ..., M_t\}$ з відповідними хеш-образами $\{h_1, h_2, ..., h_t\}$ здійснюється за допомогою додаткової точки еліптичної кривої

$$Q = \sum_{i=1}^{t} h_i \cdot Q_i,$$

яка залежить від відкритих ключів Q_i учасників підписання та хеш-образів електронних документів h_i.

Обчислюється точка $\widetilde{R}$ еліптичної кривої

$$\widetilde{R} = sP + rQ = (x\widetilde{R}, y\widetilde{R})$$

після чого формується число

$$\widetilde{r} = x\widetilde{R} \bmod \delta.$$

Якщо $\widetilde{r} = r$, композиційний цифровий підпис під набором електронних документів $\{M_1, M_2, ..., M_t\}$ признається справжнім.

Покажемо коректність пропонованого алгоритму формування і перевірки композиційного підпису:

$$\widetilde{R} = sP + rQ = \left(\sum_{i=1}^{t} s_i\right)P + r\left(\sum_{i=1}^{t} h_i \cdot Q_i\right) =$$

$$= \left(\sum_{i=1}^{t} k_i - d_i h_i r\right)P + r\left(\sum_{i=1}^{t} h_i d_i P\right) = \left(\sum_{i=1}^{t} k_i\right)P = \sum_{i=1}^{t} R_i = R.$$

Оскільки $\widetilde{R} = R$, то і $\widetilde{r} = r$.

Приклад.

Оберемо загальні параметри:

основне поле – скінченне поле $GF(13)$;

еліптична крива над основним полем

$$y^2 = x^3 + 2x + 4 \mod 13.$$

Базова точка еліптичної кривої $P = (7,6)$ має порядок $n = 17$.

Допоміжне просте багаторозрядне двійкове число $\delta = 7$.

Генерація ключів

Нехай число користувачів $t = 3$.

Відповідні особисті ключі є $d_1 = 8$, $d_2 = 5$, $d_3 = 15$.

Тоді відкрити ключі $Q_1 = (5,10)$, $Q_2 = (8,8)$, $Q_3 = (9,7)$.

Формування композиційного підпису

Нехай хеш-образи електронних документів M_1, M_2, M_3 дорівнюють відповідно $h_1 = 9$, $h_2 = 10$, $h_3 = 13$.

Кожний підписувач обирає одноразовий випадковий секретний ключ k_i: $k_1 = 5$, $k_2 = 10$, $k_3 = 9$ та обчислює координати точки R_i: $R_1 = (8,8)$, $R_2 = (0,11)$, $R_3 = (5,3)$.

Далі обчислюється R – сума всіх точок R_i: $R = (0,2)$, після чого формується число r:

$$r = 0 \bmod 7 = 0.$$

Оскільки $r = 0$, необхідно обрати нові випадкові секретні ключі k_i: $k_1 = 3$, $k_2 = 4$, $k_3 = 12$. Відповідно $R_1 = (10,7)$, $R_2 = (12,1)$, $R_3 = (8,5)$. Тоді $R = (9,6)$, і число $r = 9 \bmod 7 = 2$, $r = 2$.

Далі кожний користувач i за допомогою свого особистого ключа d_i, значення k_i, хеш-образу h_i та числа r обчислює свою долю підпису:

$$s_1 = 3 - 8 \cdot 9 \cdot 2 \bmod 17 = 12,\ s_1 = 12,$$

$$s_2 = 4 - 5 \cdot 10 \cdot 2 \bmod 17 = 6,\ s_2 = 6,$$

$$s_3 = 12 - 15 \cdot 13 \cdot 2 \bmod 17 = 13,\ s_3 = 13,$$

після чого генерується підпис s: $s = 14$.

Композиційним підписом є пара чисел $\langle r, s \rangle = \langle 2,14 \rangle$.

Перевірка композиційного підпису

Перевірка підпису $\langle r, s \rangle = \langle 2,14 \rangle$ під набором електронних документів $\{M_1, M_2, M_3\}$ з відповідними хеш-образами $h_1 = 9$, $h_2 = 10$, $h_3 = 13$ здійснюється за допомогою додаткової точки еліптичної кривої

$$Q = 9Q_1 + 10Q_2 + 13Q_3 = (2,9),\ Q = (2,9).$$

Обчислюється точка $\widetilde{R}$ еліптичної кривої:

$$sP = (10,6),\ rQ = (8,8),$$

$$\widetilde{R} = (9,6).$$

Звідси $\widetilde{r} = 9 \bmod 7 = 2$, $\widetilde{r} = 2$.

Оскільки $\widetilde{r} = r$, композиційний цифровий підпис під набором електронних документів $\{M_1, M_2, M_3\}$ признається справжнім.

Додаток Г
Приклад перевірки на анонімність схеми сліпого підпису

Нехай загальні параметри підпису: еліптична крива $y^2 = x^3 + 5x + 9 \bmod 59$, базова точка еліптичної кривої $P = (0,3)$ з простим порядком $n = 73$, $|n| = 7$. Підписувач А має особистий ключ $d = 15$ та відповідний йому відкритий ключ $Q = (34,22)$.

Нехай підписувач А отримав електронний документ $m = 5$ з підписом $\langle R, s \rangle = \langle (1,29), 30 \rangle$, згідно з протоколом, наведеним в Додатку А.

Обчислимо h_R. Для отримання хеш-образу $H(R)$ підписувач А використав програму hash.exe, де в якості функції хешування обрав функцію MD5. Значення h_R сформовано зі молодших $|n| - 1 = 6$ розрядів 128-бітного значення функції MD5.

Хеш-функція

MD5("(1,29)") = 3729424dd8272d04deea8aefe33242d6=….11010110.

Звідси $h_R = 010110_2 = 22_{10}$.

Перевіримо приналежність підпису $R = (1,29)$, $s = 30$ підписувачу А – $sP = h_R \cdot Q + m \cdot R$:

$$sP = 30 \cdot (0,3) = (12,33),$$
$$h_R \cdot Q + m \cdot R = 22 \cdot (34,22) + 5 \cdot (1,29) = (12,33).$$

Підписувач А переконався, що саме він підписав документ m з підписом $\langle R, s \rangle$.

За допомогою бази параметрів обміну з користувачами (наборів даних k, E, h_E, $\overline{m}$, $\overline{s}$) підписувач А спробував визначити, якій із користувачів був емітентом документа m.

Для цього він обчислив значення $\beta = \frac{s}{\overline{s}} \bmod n$, $\alpha = \frac{\beta \cdot \overline{m}}{m} \bmod n$ та точки $\alpha \cdot E$ по усіх наборах даних.

Результати обчислень зведені в таблицю Г.1.

Таблиця Г.1 – Результати обчислень підписувача А

	k	E	h_E	$\overline{m}$	$\overline{s}$	$\beta = \frac{s}{\overline{s}}$	$\alpha = \frac{\beta \cdot \overline{m}}{m}$	$\alpha \cdot E$
B_1	8	(35,44)	8	60	16	11	59	(24,18)
B_2	24	(46,15)	25	21	3	10	42	(26,30)
B_{11}	**19**	**(17,13)**	**23**	**53**	**38**	**20**	**66**	**(1,29)**
B_2	29	(56,12)	23	19	20	38	13	(20,12)
B_{10}	16	(37,44)	2	54	18	26	18	(30,14)
B_3	57	(37,15)	53	15	44	4	12	(32,30)
B_1	20	(45,33)	8	8	61	34	69	(39,46)
B_5	67	(23,14)	63	60	1	30	68	(12,33)

Оскільки $\alpha \cdot E = R$ для користувача B_{11}, то саме він надав документ m для підпису.

Додаток Д
Елементи теорії дивізорів гіпереліптичних кривих

Гіпереліптична крива – це узагальнення поняття еліптичної кривої [25-27]. Вона також може бути визначена над будь-яким полем, зокрема над полем дійсних чисел або над простим чи розширенним полем Галуа.

Гіпереліптичною кривою C роду g ($g \geq 1$) над полем $GF(q)$, $q = p^m$, (p – просте число) є рівняння виду

$$C: y^2 + h(x)y = f(x),$$

де $f(x)$ – нормований многочлен ступеня $2g+1$ над полем $GF(q)$, $x, y \in \overline{GF(q)}$, $\overline{GF(q)}$ – алгебраїчне замикання поля $GF(q)$ і не існує рішень $(x, y) \in \overline{GF(q)} \times \overline{GF(q)}$, які одночасно задовольняли б рівнянню $y^2 + h(x)y = f(x)$ та рівнянням часткових похідних $2y + h(x) = 0$ і $f'(x) - h'(x)y = 0$.

На рис. Д.1 подано приклад гіпереліптичної кривої над полем дійсних чисел *R*.

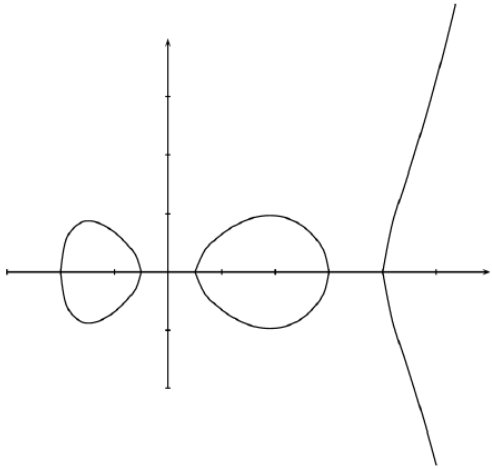

Рисунок Д.1. – Гіпереліптична крива над полем дійсних чисел *R*

Точки гіпереліптичної кривої $P=(x,y)$ і $\widetilde{P}=(x,-y-h(x))$ визначимо як протилежні: $\widetilde{P}=-P$.

По аналогії з еліптичними кривими визначемо точку на нескінченності P_∞, причому $P_\infty=-P_\infty$.

Для простого поля $GF(p)$ заміною змінних $x\to x$, $y\to(y-h(x)/2)$ криву $y^2+h(x)y=f(x)$ можна перетворити на криву

$$C: y^2=f(x).$$

Отже, в подальшому будемо розглядати гіпереліптичні криві в такому вигляді.

На відміну від еліптичної кривої, точки гіпереліптичної кривої не утворюють адитивну групу. Однак адитивну групу можна побудувати за допомогою дивізорів.

Дивізором гіпереліптичної кривої C називається формальна сума скінченної кількості точок кривої:

$$D=\sum_{P_i\in C} m_iP_i\ ,\ \ m_i\in Z\ .$$

Дивізори $D=\sum_{P_i\in C} m_iP_i$ і $-D=\sum_{P_i\in C} m_i(-P_i)$ називаються протилежними.

Введемо правило додавання дивізорів [28]:

$$\sum_{P_i\in C} m_iP_i+\sum_{P_i\in C} n_iP_i=\sum_{P_i\in C}(m_i+n_i)P_i\ .$$

Порядком $ord_{P_i}(D)$ дивізора $D=\sum_{P_i\in C} m_iP_i$ в точці P_i є коефіцієнт m_i: $ord_{P_i}(D)=m_i$.

Степенем дивізора $D=\sum_{P_i\in C} m_iP_i$ називається сума $\sum_{P_i\in C} m_i$ порядків дивізора в точках P_i.

Будемо розглядати дивізори степеня 0, представлені у вигляді

$$D = \sum_{P_i \in C} m_i P_i - \sum_{P_i \in C} m_i P_\infty ,$$

де $\sum_{P_i \in C} m_i \le g$, причому в сумі не можуть бути одночасно P_i і $-P_i$.

Такі дивізори називаються *зведеними* і є унікальними елементами *якобіану* кривої, що являє собою адитивну групу з наведеним вище правилом додавання дивізорів.

Для практичних додатків більш ефективно представлення зведених дивізорів в *формі Мамфорда* – у вигляді пар многочленів $D = \langle u(x), v(x) \rangle$. Для дивізора $D = \langle u(x), v(x) \rangle$ протилежним є дивізор $-D = \langle u(x), -v(x) \rangle$.

Твердження. Якщо $D = \sum_{P_i \in C} m_i P_i - \sum_{P_i \in C} m_i P_\infty$, де $P_i = (X_i, Y_i)$ – точки гіпереліптичної кривої, то многочлени $u(x)$, $v(x)$, такі що $D = \langle u(x), v(x) \rangle$, обчислюються за правилами: $u(x) = \prod_i (x - X_i)^{m_i}$, $\deg v(x) < \deg u(x)$, $v(X_i) = Y_i$.

Введемо операцію додавання двох дивізорів $D_1 = \langle u_1, v_1 \rangle$ і $D_2 = \langle u_2, v_2 \rangle$: $D = D_1 + D_2 = \langle u_3, v_3 \rangle$.

Якщо $D_1 \ne D_2$, то

1 обчислимо найбільш спільний дільник многочленів u_1, u_2 і $(v_1 + v_2)$: $d = \gcd(u_1, u_2, v_1 + v_2) = s_1 u_1 + s_2 u_2 + s_3 (v_1 + v_2)$;

2 обчислимо $u_0' = \dfrac{u_1 u_2}{d^2}$;

3 обчислимо $v_0' = \dfrac{s_1 u_1 v_2 + s_2 u_2 v_1 + s_3 (v_1 v_2 + f)}{d} \bmod u_0'$;

4 обчислимо в циклі (u_k', v_k'), $k = 1,2...$, до виконанні умови $\deg u_k' \le g$

4.1 $u'_k = \dfrac{f - (v'_{k-1})^2}{u'_{k-1}}$,

4.2 $v'_k = -v'_{k-1} \bmod u'_k$;

5 якщо умова $\deg u'_k \le g$ виконана, то обчислено сума дивізорів $D = D_1 + D_2 = \langle u_3, v_3 \rangle = \langle u'_k, v'_k \rangle$.

Якщо $D_1 = D_2 = \langle u, v \rangle$, то кроки 1-3 замінюються на таки:

1 обчислимо найбільш спільний дільник многочленів u і $2v$: $d = \gcd(u, 2v) = s_1 u + s_3 (2v)$;

2 обчислимо $u'_0 = \left(\dfrac{u}{d}\right)^2$;

3 обчислимо $v'_0 = \dfrac{s_1 uv + s_3 (v^2 + f)}{d} \bmod u'_0$.

Дивізор $D0 = \langle 1, 0 \rangle$ є нейтральним елементом (нулем) якобіану.

Для отримання елементів якобіану необхідно обчислити кратні базового дивізора до отримання нуля групи, тобто дивізора $D0 = \langle 1, 0 \rangle$.

Порядок якобіану гіпереліптичної кривої роду g над полем $GF(q)$ обмежено інтервалом Хассе-Вейля

$$\left| (\sqrt{q} - 1)^{2g} \right| \le \#J / GF(q) \le \left\lfloor (\sqrt{q} + 1)^{2g} \right\rfloor.$$

Таким чином, отримано групова структура на гіпереліптичній кривій. Наявність групової структури дозволяє будувати криптографічні протоколи (див. лаб. роб. №6) на основі арифметики якобіанів гіпереліптичних кривих.

Приклад. Розглянемо гіпереліптичну криву другого роду над полем $GF(7)$:

$$y^2 = x^5 + 2x^2 + x + 3 \mod 7.$$

В формуванні якобіану приймають участь точки кривої в $GF(7)$ и $GF(7^2)$. В цьому прикладі для визначення поля $GF(7^2)$ оберемо незвідний поліном $f(t) = t^2 + 6t + 6$.

В прикладі порядок якобіану кривої обмежено інтервалом Хассе-Вейля:

$$8 \le \#J / GF(7) \le 176.$$

Точками кривої в $GF(7)$ є $P_1 = (1,0)$, $P_2 = (3,1)$, $P_3 = (3,6)$.

Точки $P_2 = (3,1)$ і $P_3 = (3,6)$ є протилежними.

Точками кривої в $GF(7^2)$ серед інших є $(2t,3t)$, $(4t,5+3t)$, $(2+5t,3+4t)$, $(2t,4t)$, $(5+3t,4+6t)$, $(1+3t,2+3t)$.

Для отримання, наприклад, точки $(2t,3t)$ необхідно розв'язати в полі $GF(7^2)$ рівняння

$$y^2 = (2t)^5 + 2\cdot(2t)^2 + (2t) + 3 \bmod(7,\ t^2 + 6t + 6),$$

тобто

$$y^2 = 2t + 2 \bmod(7,\ t^2 + 6t + 6)$$

Отримуємо $y = 3t$.

Побудуємо дивізори

$d1 = (1,0) + (3,1) - 2P_\infty$,

$d2 = (3,1) - P_\infty$,

$d3 = 2\cdot(3,1) - 2P_\infty$,

$d4 = (3,1) - 2\cdot(1,0)$,

$d5 = 6\cdot(3,1) - 4\cdot(3,6)$,

$d6 = 8\cdot(3,1) - 2\cdot(5+3t, 4+6t)$,

$d7 = 4\cdot(4t, 5+3t) + 5\cdot(1+3t, 2+3t)$,

$d8 = (3,6) - P_\infty$,

$d9 = 7\cdot(3,1) - 2\cdot(1,0) - 4\cdot(3,6)$.

Порядок дивізора $d6$ в точці (3,1) дорівнює 8.

Дивізори $d2$ і $d8$ є протилежними.

Згідно з правилом додавання дивізорів

$$d4 + d5 = (3,\ 1) - 2\cdot(1,0) + 6\cdot(3,\ 1) - 4\cdot(3,6) =$$
$$= 7\cdot(3,1) - 2\cdot(1,0) - 4\cdot(3,6) = d9.$$

Степінь дивізора $d7$ дорівнює 9.

Дивізори $d1,\ d2,\ d3, d8$ є зведеними.

З використанням точок $P_1 = (1,0)$, $P_2 = (3,1)$, $P_3 = (3,6)$ кривої $y^2 = x^5 + 2x^2 + x + 3 \pmod 7$ сформуємо наступні зведені дивізори у формі Мамфорда:

$$D1 = (1,0) + (3,1) - 2P_\infty =< x^2 + 3x + 3,\ 4x + 3 >,$$
$$D2 = (1,0) + (3,6) - 2P_\infty =< x^2 + 3x + 3,\ 3x + 4 >,$$
$$D3 = (1,0) - P_\infty = (x - 1,\ 0) =< x + 6,\ 0 >,$$
$$D4 = (3,\ 1) - P_\infty = (x - 3,1) =< x + 4,1 >,$$
$$D5 = (3,6) - P_\infty = (x - 3,\ 6) =< x + 4,\ 6 >,$$
$$D6 = 2\cdot(3,\ 1) - 2P_\infty =< x^2 + x + 2,6x + 4 >,$$
$$D7 = 2\cdot(3,6) - 2P_\infty =< x^2 + x + 2, x + 3 >.$$

Представимо дивізор $D1$ в формі Мамфорда.

Для дивізора $D1 = (1,0) + (3,1) - 2P_\infty$ обчислимо многочлен

$$u(x) = (x - 1)\cdot(x - 3) = (x^2 - 4x + 3) \bmod 7 = x^2 + 3x + 3.$$

Многочлен $v(x)$ має вигляд $v(x) = b_1 \cdot x + b_0$ і задовольняє умовам:

$$v(1) = b_1 \cdot 1 + b_0 = 0 \bmod 7,$$
$$v(3) = b_1 \cdot 3 + b_0 = 1 \bmod 7.$$

Звідси отримуємо $b_1 = 4$, $b_0 = 3$, тобто $v(x) = 4x + 3$.

Таким чином, представлення дивізора $D1$ в формі Мамфорда є $D1 =< x^2 + 3x + 3,\ 4x + 3 >$.

Представимо в формі Мамфорда дивізор $-D1$, протилежний дивізору $D1$: $-D1 = -(1,0) - (3,1) - 2P_\infty = (1,0) + (3,6) - 2P_\infty$.

Многочлен $u(x) = (x-1)\cdot(x-3) \bmod 7 = x^2 + 3x + 3$ має той же вигляд, як для дивізора $D1$.

Многочлен $v(x)$ задовольняє умовам:

$v(1) = b_1 \cdot 1 + b_0 = 0 \bmod 7$,

$v(3) = b_1 \cdot 3 + b_0 = 6 \bmod 7$.

Звідси отримуємо $b_1 = 3$, $b_0 = 4$, тобто $v(x) = 3x + 4$,

$-D1 =< x^2 + 3x + 3,\ 3x + 4 >$.

Для дивізора $D1 =< x^2 + 3x + 3,\ 4x + 3 >$ знайдємо суму $D1 + D1 = 2 \cdot D1$.

Згідно з правилом додавання дивізорів,

1 обчислимо найбільшій спільний дільник многочленів $u = x^2 + 3x + 3$ і $2v = x + 6$ ($v = 4x + 3$):

$$d = \gcd(u, 2v) = s_1 u + s_3 (2v) = 0 \cdot (x^2 + 3x + 3) + 1 \cdot (x + 6) = x + 6,$$

$d = x + 6$, $s_1 = 0$, $s_3 = 1$;

2 обчислимо

$$u_0' = \left(\frac{u}{d}\right)^2 = \left(\frac{x^2 + 3x + 3}{x + 6}\right)^2 = (x + 4)^2 = x^2 + x + 2;$$

3 обчислимо

$$v_0' = \frac{s_1 uv + s_3 (v^2 + f)}{d} \bmod u_0' =$$

$$= \frac{(4x + 3)^2 + x^5 + 2x^2 + x + 3}{x + 6} \bmod (x^2 + x + 2) =$$

$$= \frac{x^5 + 4x^2 + 4x + 5}{x + 6} = (x^4 + x^3 + x^2 + 5x + 2) \bmod (x^2 + x + 2) =$$

$$= 6x + 4,$$

$v_0' = 6x + 4$.

Звідси $2D1 = \left\langle x^2 + x + 2, 6x + 4 \right\rangle$.

Знайдемо суму $D1 + 2D1 = 3D1$.

$$u_1 = x^2 + 3x + 3,\ v_1 = 4x + 3,\ u_2 = x^2 + x + 2,\ v_2 = 6x + 4.$$

Згідно з правилом додавання дивізорів,

1 обчислимо найбільшій спільний дільник многочленів u_1, u_2 і $v_1 + v_2 = 3x$:

$$d = \gcd(u_1, u_2, v_1 + v_2) = s_1 u_1 + s_2 u_2 + s_3 (v_1 + v_2) =$$

$$= 1 \cdot (x^2 + 3x + 3) + 6 \cdot (x^2 + x + 2) + 4 \cdot 3x = 1,$$

$d = 1$, $s_1 = 1$, $s_2 = 6$, $s_3 = 4$;

2 обчислимо

$$u_0' = \frac{u_1 u_2}{d^2} = (x^2 + 3x + 3)(x^2 + x + 2) = x^4 + 4x^3 + x^2 + 2x + 6;$$

3 обчислимо

$$v_0' = \frac{s_1 u_1 v_2 + s_2 u_2 v_1 + s_3 (v_1 v_2 + f)}{d} \bmod u_0' =$$

$$= (x^2 + 3x + 3)(6x + 4) + 6(x^2 + x + 2)(4x + 3) + 4((4x + 3)(6x + 4) +$$

$$+ x^5 + 2x^2 + x + 3) \bmod (x^4 + 4x^3 + x^2 + 2x + 6) =$$

$$= (4x^5 + 2x^3 + 5x + 3) \bmod (x^4 + 4x^3 + x^2 + 2x + 6) = 6x^3 + x^2 + 6x + 1,$$

$v_0' = 6x^3 + x^2 + 6x + 1$.

4 обчислимо в циклі $(u_k', v_k'), k = 1,2\ldots$, до виконанні умови $\deg u_k' \le g$

$$u_1' = \frac{f - (v_0')^2}{u_0'} =$$

$$= \frac{x^5 + 2x^2 + x + 3 - (6x^3 + x^2 + 6x + 1)^2}{x^4 + 4x^3 + x^2 + 2x + 6} = x^2 + 2;$$

$$v_1' = -v_0' \bmod u_1' =$$

$$= -(6x^3 + x^2 + 6x + 1) \bmod (x^2 + 2) = 6x + 1.$$

Звідси $3D1 = \left\langle x^2 + 2{,}6x + 1 \right\rangle$.

Знайдемо суму двох протилежних дивізорів $D1$ і $-D1$.

$u_1 = x^2 + 3x + 3$, $v_1 = 4x + 3$, $u_2 = x^2 + 3x + 3$, $v_2 = 3x + 4$.

Згідно з правилом додавання дивізорів,

1 обчислимо найбільшій спільний дільник многочленів u_1, u_2 і $v_1 + v_2 = 0$:

$$d = \gcd(u_1, u_2, v_1 + v_2) = s_1 u_1 + s_2 u_2 + s_3 (v_1 + v_2) =$$

$$= 1 \cdot (x^2 + 3x + 3) + 0 \cdot (x^2 + 3x + 3) + 0 \cdot 0 = x^2 + 3x + 3,$$

$d = x^2 + 3x + 3$, $s_1 = 1$, $s_2 = 0$, $s_3 = 0$;

2 обчислимо $u'_0 = \dfrac{u_1 u_2}{d^2} = 1$;

3 обчислимо $v'_0 = \dfrac{s_1 u_1 v_2 + s_2 u_2 v_1 + s_3 (v_1 v_2 + f)}{d} \bmod u'_0 = 0$.

Звідси $D1 + (-D1) = \langle 1{,}0 \rangle$.

В наведеному прикладі дивізор $D =< x^2 + 3x + 3,\ 4x + 3 >$ породжує групу порядку 34, яка містить нуль групи $\langle 1{,}0 \rangle$, один дивізор $< x + 6,\ 0 >$ порядку 2, 16 дивізорів порядку 17 и 16 дивізорів порядку 34.

Елементи якобіану кривої $y^2 = x^5 + 2x^2 + x + 3 \mod 7$ представлені в таблиці Д.1 як кратні базового дивізора.

Таблиця Д.1 – Елементи якобіану кривої $y^2 = x^5 + 2x^2 + x + 3 \mod 7$

Дивізор	Представлення у формі Мамфорда	Представлення у вигляді суми точок
D	<x^2+3x+3, 4x+3>	(1,0)+(3,1)
2D	<x^2+x+2, 6x+4>	(3,1)+(3,1)
3D	<x^2+2, 6x+1>	(1+5t, 2t)+(6+2t, 2+5t)
4D	<x^2+5x+3, 5x>	(2t, 3t)+(2+5t, 3+4t)
5D	<x^2+6x+3, 3x+5>	(2+4t, 4+5t)+(6+3t, 2+2t)
6D	<x^2+4x+6, 6x+3>	(6+5t, 4+2t)+(4+2t, 6+5t)
7D	<x^2+x+4, 5x+5>	(2+2t, 1+3t)+(4+5t, 4+4t)
8D	<x^2+3x+5, x+2>	(4+3t, 6+3t)+(4t, 2+4t)
9D	<x^2+x+3, 5x+6>	(1+4t, 4+6t)+(5+3t, 3+t)
10D	<x^2+5x+5, 2>	(4+t, 2)+(5+6t, 2)
11D	<x^2+2x+3, 5x+5>	(5t, 5+4t)+(5+2t, 2+3t)
12D	<x^2+5x+2, 5x>	(3+3t, 1+t)+(6+4t, 2+6t)
13D	<x^2+2x+2, x+1>	(4+4t, 5+4t)+(1+3t, 2+3t)
14D	<x^2+x+6, 6x+1>	(6+t, 2+6t)+(6t, 1+t)
15D	<x^2+6x+6, x>	(t, t)+(1+6t, 1+6t)
16D	<x+4, 6>	(3,6)
17D	<x+6, 0>	(1,0)
18D	<x+4, 1>	(3,1)
19D	<x^2+6x+6, 6x>	(1+6t, 6+t)+(t, 6t)
20D	<x^2+x+6, x+6>	(6+t, 5+t)+(6t, 6+6t)
21D	<x^2+2x+2, 6x+6>	(1+3t, 5+4t)+(4+4t, 2+3t)
22D	<x^2+5x+2, 2x>	(3+3t, 6+6t)+(6+4t, 5+t)
23D	<x^2+2x+3, 2x+2>	(5+2t, 5+4t)+(5t, 2+3t)
24D	<x^2+5x+5, 5>	(4+t, 5)+(5+6t, 5)
25D	<x^2+x+3, 2x+1>	(1+4t, 3+t)+(5+3t, 4+6t)
26D	<x^2+3x+5, 6x+5>	(4t, 5+3t)+(4+3t, 1+4t)
27D	<x^2+x+4, 2x+2>	(2+2t, 6+4t)+(4+5t, 3+3t>
28D	<x^2+4x+6, x+4>	(4+2t, 1+2t)+(6+5t, 3+5t)
29D	<x^2+6x+3, 4x+2>	(6+3t, 5+5t)+(2+4t, 3+2t)
30D	<x^2+5x+3, 2x>	(2t, 4t)+(2+5t,4+3t)
31D	<x^2+2, x+6>	(6+2t, 5+2t)+(1+5t, 5t)
32D	<x^2+x+2, x+3>	(3,6)+(3,6)
33D	<x^2+3x+3, 3x+4>	(1,0)+(3,6)
34D	<1, 0>	

Додаток Е
Протокол цифрового підпису на гіпереліптичних кривих

Для побудови протоколів [29,30] цифрового підпису на гіпереліптичних кривих можна модифікувати протоколи цифрового підпису на еліптичних кривих. При цьому операції з точками еліптичної кривої замінюються на операції з дивізорами гіпереліптичної кривої.

У розглянутому протоколі формування й перевірки цифрового підпису група точок еліптичної кривої була замінена на групу дивізорів (якобіан) гіпереліптичної кривої.

Функцію $\psi(D)$ перетворення на ціле число дивізора $D = \langle u(x), v(x) \rangle$ гіпереліптичної кривої над простим полем $GF(p)$, представленого в формі Мамфорда, визначимо формулою

$$\psi(D) = u(p).$$

Протокол цифрового підпису на гіпереліптичної кривої над простим полем

Цей протокол [29] є модифікацією сучасного українського стандарту ДСТУ 4145-2002 [31].

Загальні параметри:

основне поле – скінченне поле $GF(p)$;

гіпереліптична крива роду g ($g \geq 1$) над основним полем $y^2 = f(x)$, де $f(x)$ – нормований многочлен ступеня $2g+1$ над полем $GF(p)$;

базовий дивізор D простого порядку n, такий що $nD = \langle 1,0 \rangle$ і $kD \neq \langle 1,0 \rangle$, $0 < k < n$;

H – функція хешування.

Генерація ключів

Підписувач А має асиметричну пару ключів: особистий $d : 1 < d < n$, та відкритий $Q = -dD$.

Формування підпису

Нехай підписувач А має підписати електронний документ M з хеш-образом $H(M)$. Молодші $|n|-1$ розряди хеш-образу $H(M)$ формують десяткове число h, яке використається при обчисленні цифрового підпису.

Підписувач А обирає одноразовий випадковий секретний ключ k, $1 < k < n$, обчислює дивізор $R = kD = \langle u(x), v(x) \rangle$, після чого формуються складові цифрового підпису

$$r = h \cdot \psi(R) \bmod n = h \cdot u(p) \bmod n,$$

$$s = (k + d \cdot r) \bmod n.$$

Параметр підпису s не може бути рівним 0. При $s = 0$ процедура підпису повторюється.

Цифровим підписом є пара чисел $\langle r, s \rangle$.

Перевірка підпису

Перевірка підпису $\langle r, s \rangle$ під електронним документом M здійснюється за допомогою відкритого ключа Q підписувача А.

Обчислюється дивізор гіпереліптичної кривої

$$\widetilde{R} = sD + rQ$$

після чого обчислюються хеш-образ документу $H(M)$, відповідне десяткове число h та формується число

$$\widetilde{r} = h \cdot \psi(\widetilde{R}) \bmod n.$$

Якщо $\widetilde{r} = r$, цифровий підпис електронного документу M признається справжнім.

Покажемо коректність алгоритму формування і перевірки підпису:

$$\widetilde{R} = sD + rQ = (k + d \cdot r)D + r(-d \cdot D) = kD = R.$$

Оскільки $\widetilde{R} = R$, то і $\widetilde{r} = r$.

Приклад. Оберемо загальні параметри:
основне поле – скінченне поле $GF(7)$;
гіпереліптична крива над основним полем

$$y^2 = x^5 + 2x^2 + x + 3,\ p = 7;$$

базовий дивізор $D = \langle x + 4,1 \rangle$ простого порядку $n = 17$.

Генерація ключів

Нехай підписувач А має особистий ключ $d = 3$ та відповідний йому відкритий ключ

$$Q = -dD = -3\langle x + 4,\ 1 \rangle = -\left\langle x^2 + x + 6,\ x + 6 \right\rangle = \left\langle x^2 + x + 6,\ 6x + 1 \right\rangle.$$

Формування підпису

Нехай хеш-образ електронного документу M дорівнює $h = 2$.

Підписувач А обирає одноразовий випадковий секретний ключ $k = 4$, обчислює дивізор $R = 4D = \left\langle x^2 + 5x + 3,5x \right\rangle$, після чого формує складові цифрового підпису

$$r = h \cdot \psi(R) \bmod n = 2 \cdot (7^2 + 5 \cdot 7 + 3) \bmod 17 = 4,$$
$$s = (k + d \cdot r) \bmod n = (4 + 3 \cdot 4) \bmod 17 = 16.$$

Цифровим підписом є пара чисел $\langle r, s \rangle = \langle 4,16 \rangle$.

Перевірка підпису

Перевірка підпису $\langle r, s \rangle = \langle 4,16 \rangle$ під електронним документом M здійснюється за допомогою відкритого ключа $Q = \left\langle x^2 + x + 6,\ 6x + 1 \right\rangle$ підписувача А.

Обчислюється дивізор гіпереліптичної кривої

$$\widetilde{R} = 16D + 4Q = \langle x + 4,6 \rangle + \left\langle x^2 + 5x + 2 \right\rangle = \left\langle x^2 + 5x + 3,5x \right\rangle,$$

після чого обчислюються хеш-образ документу $H(M)$, відповідне десяткове число $h = 2$ та формується число

$$\widetilde{r} = h \cdot \psi(\widetilde{R}) \bmod n = 2 \cdot (7^2 + 5 \cdot 7 + 3) \bmod 17 = 4.$$

Оскільки $\widetilde{r} = r$, цифровий підпис електронного документу M признається справжнім.

Додаток Ж
Процедури групової операції на гіпереліптичних кривих

Ж.1 Процедура додавання двох різних дивізорів

```
p_SumD:=proc(D1,D2,f,h,g,m) global aa22;
   local a1,b1,a2,b2,bb,d,e1,e2,d1,c1,c2,s1,s2,s3,bb1,bb2,bb3,bb4,bb5,
   d0_1,d0,h11,h12,d_1,h22,h1,h2,h3,a,b,b3,rr,q1,q2,aa1,aa2,aa3,aa4,deg;
   description "Sum D1 & D2";

a1:=D1[0]; b1:=D1[1];a2:=D2[0]; b2:=D2[1];
bb:=modp1(Add(b1,b2,h),m);
d1:=modp1(Gcdex(a1,a2,'e1','e2'), m);
d:=modp1(Gcdex(d1,bb,'c1','c2'), m);
s1:=modp1(Multiply(c1,e1),m);
s2:=modp1(Multiply(c1,e2),m);
s3:=c2;
modp1(Divide(Multiply(a1,a2),Multiply(d,d),'a'),m);
bb1:=modp1(Multiply(s1,Multiply(a1,b2)),m);
bb2:=modp1(Multiply(s2,Multiply(a2,b1)),m);
bb3:=modp1(Multiply(s3,Add(Multiply(b1,b2),f)),m);
bb4:=modp1(Add(bb1,bb2,bb3),m);
modp1(Divide(bb4,d,'bb5'),m); b:=modp1(Powmod(bb5,1,a),m);

while modp1(Degree(a),m)>g do
  a1:=a;   b1:=b;
  aa1:=modp1(Multiply(h,b1),m);
  aa2:=modp1(Multiply(b1,b1),m);
  aa3:=modp1(Subtract(f,aa1),m);
  aa4:=modp1(Subtract(aa3,aa2),m);
  modp1(Divide(aa4,a1,'a'),m);a;
  bb1:=modp1(Subtract(ConvertIn(0,x),h),m);
  bb2:=modp1(Subtract(bb1,b1),m);   a2:=a;
  aa1:=modp1(ConvertOut(a,x),m);
  deg:=degree(aa1);   aa2:=coeff(aa1,x^deg);
  if aa2>1
```

```
    then
    unassign('u');     aa3:=msolve(aa2*u=1,m);   assign(aa3);aa3:=u;
    aa4:=modp1(ConvertIn(aa3,x),m);  a2:=modp1(Multiply(a,aa4),m);
   end if;
   a:=a2;   b:=modp1(Powmod(bb2,1,a),m);
end do;
rr:=array(0..1,[a,b]);
end proc:
```

Ж.2 Процедура подвоєння дивізора

```
p_DubD:=proc(D,f,h,g,m)  local deg,a,b,a2,b2,h1,h2,d,d_1,a1,b1,rr,bb,
       bb1,bb2,bb3,bb4,q1,q2,aa1,aa2,aa3,aa4;  description "2*D";
a1:=D[0]; b1:=D[1];
bb:=modp1(Add(b1,b1,h),m);
d:=modp1(Gcdex(a1,bb,'s1','s3'), m);
modp1(Divide(Multiply(a1,a1),Multiply(d,d),'a'),m);
bb1:=modp1(Multiply(s1,Multiply(a1,b1)),m);
bb2:=modp1(Multiply(s3,Add(Multiply(b1,b1),f)),m);
bb4:=modp1(Add(bb1,bb2),m);
modp1(Divide(bb4,d,'bb5'),m);
b:=modp1(Powmod(bb5,1,a),m);
while modp1(Degree(a),m)>g do
   a1:=a;   b1:=b;
   aa1:=modp1(Multiply(h,b1),m);
   aa2:=modp1(Multiply(b1,b1),m);
   aa3:=modp1(Subtract(f,aa1),m);
   aa4:=modp1(Subtract(aa3,aa2),m);
   modp1(Divide(aa4,a1,'a'),m);a;
   bb1:=modp1(Subtract(ConvertIn(0,x),h),m);
   bb2:=modp1(Subtract(bb1,b1),m);
   a2:=a;
   aa1:=modp1(ConvertOut(a,x),m);
   deg:=degree(aa1);   aa2:=coeff(aa1,x^deg);
   if aa2>1
     then
     unassign('u');  aa3:=msolve(aa2*u=1,m);  assign(aa3);aa3:=u;
     aa4:=modp1(ConvertIn(aa3,x),m); a2:=modp1(Multiply(a,aa4),m);
```

```
  end if;
  a:=a2;   b:=modp1(Powmod(bb2,1,a),m);
end do;
rr:=array(0..1,[a,b]);
end proc:
```

Ж.3 Процедура множення дивізора на ціле число

```
p_MulD:=proc(P,d,f,h,g,m)   local dd,k,Q,bit,i,rr;   description "d*P";
Q:=P;
if d>1
  then k:=0;
       dd:=d; bit[k]:=dd mod 2; dd:=iquo(dd,2);
       while dd<>0 do
            k:=k+1; bit[k]:=dd mod 2; dd:=iquo(dd,2);
       end do;
       k:=k-1;
       for i from k by -1 to 0 do
            Q:=p_DubD(Q,f,h,g,m);
            if bit[i]=1 then Q:=p_SumD(Q,P,f,h,g,m); end if;
       end do;
end if;
rr:=array(0..1,[Q[0],Q[1]]);
end proc:
```

Ж.4 Приклад основної програми

```
g:=2; f:=x^5+2*x^2+x+3; m:=7;h:=0; d:=17;
h:=modp1(ConvertIn(h,x),m);
f:=modp1(ConvertIn(f,x),m);
u1:=x^2+3*x+3: v1:=4*x+3:     u2:=x+4: v2:=1:
u1:=modp1(ConvertIn(u1,x),m);
v1:=modp1(ConvertIn(v1,x),m);
u2:=modp1(ConvertIn(u2,x),m);
v2:=modp1(ConvertIn(v2,x),m);
```

$g := 2 \quad m := 7 \quad d := 17$

$h := 0$

$f := 3 + x + 2x^2 + x^5$

$u1 := 3 + 3x + x^2$

$v1 := 3 + 4x$

$u2 := 4 + x$

$v2 := 1$

```
dd1:=array(0..1,[u1,v1]);
```

$$dd1 := \text{array}(0 .. 1, [(0) = 3 + 3x + x^2 (1) = 3 + 4x])$$

```
dd2:=array(0..1,[u2,v2]);
```

$$dd2 := \text{array}(0 .. 1, [(0) = 4 + x (1) = 1])$$

```
print("Summa dd1+dd2=");
```

"Summa dd1+dd2="

```
p_SumD(dd1,dd2,f,h,g,m);
```

$$\text{array}(0 .. 1, [(0) = 6 + 6x + x^2 (1) = 6x])$$

```
print("Doubling 2*dd1=");
```

"Doubling 2*dd1="

```
p_DubD(dd1,f,h,g,m);
```

$$\text{array}(0 .. 1, [(0) = 2 + x + x^2 (1) = 4 + 6x])$$

```
print("Mult d*dd1=");
```

"Mult d*dd1="

```
p_MulD(dd1,d,f,h,g,m);
```

$$\text{array}(0 .. 1, [(0) = 6 + x (1) = 0])$$