

Львівський національний університет
імені Івана Франка
кафедра обчислювальної математики

Курсова робота

на тему:

Криптографічні протоколи, що базуються на доведенні з нульовим знанням

Студента 3-го курсу групи ПМп-31
напрямку підготовки.
6.040301 "Прикладна математика"
Тернового В.М.

Керівник:

доц. Остудін Б.А.

Національна шкала _____

Кількість балів: _____ Оцінка ECTS _____

Члени комісії

_____	_____
_____	_____
_____	_____

Львів 2015

Зміст

1. Вступ	3
2. Математичні основи	4
2.1. Еліптичні криві	4
2.1.1. Порядок еліптичної кривої і точок еліптичної кривої	5
2.2. Скінченні поля (Галуа)	5
2.2.1. Існування скінченного поля $F(p)$	5
2.2.2. Зворотний елемент групи $F(p)^*$	5
2.2.3. Ділення в полі $F(p)$	5
2.2.4. Квадрати і неквадрати в полі $F(p)$	5
2.2.5. Пошук квадратного кореня в полі $F(p)$	6
3. Груповий закон для еліптичних кривих $E(F(p))$	7
3.1. Огляд систем координат	7
3.2. Груповий закон в афінних координатах	7
3.3. Груповий закон у проєктивних координатах	8
3.4. Груповий закон у проєктивних координатах Якобі	9
3.5. Груповий закон у модифікованих координатах Якобі	10
3.6. Змішані координати	10
4. Еліптична криптографія	12
4.1. Принципи еліптичної криптографії	12
4.2. Електронний цифровий підпис на еліптичних кривих	12
4.2.1. Вимоги до еліптичних кривих згідно стандарту X9.62	12
4.2.2. Вибір параметрів ЕЦП	13
4.2.3. Генерація ключів ЕЦП	13
4.2.4. Формування цифрового підпису	13
4.2.5. Перевірка цифрового підпису	14
5. Приклади застосування	15
5.1. Визначення порядку канонічних еліптичних кривих	15
6. Висновок	16
Список літератури	17

Вступ

Сьогодні багато конфіденційної інформації передається між комп'ютерами відкритими мережами, що потребує її захисту та автентифікації. В останній чверті минулого століття з'явилась і зараз інтенсивно розвивається криптографія з відкритими ключами на еліптичних кривих, яка дозволяє розв'язувати різноманітні задачі захисту інформації в комп'ютерних мережах.

Особливе зацікавлення в еліптичній криптографії зумовлено високою швидкістю і порівняно невеликою довжиною ключа. Наприклад, побудовані на принципах еліптичної криптографії системи з довжиною ключа 160 - 210 біт забезпечують таку саму криптостійкість, як традиційні системи при довжині ключа 1024 - 2048 біт.

В роботі розглянуто еліптичні криві та їх використання в сучасній криптографії, принципи побудови криптографічних систем на еліптичних кривих і їх застосування для систем електронного цифрового підпису.

Математичні основи

2.1 Еліптичні криві

Кубічна крива на площині (x, y) (над полем дійсних чисел) називається кривою в формі Веєрштрасса, якщо вона описується рівнянням:

$$y^2 = x^3 + ax + b. \quad (1)$$

Ця форма представлення кривої вважається канонічною. Для прикладу на рис. 1.1 наведені кубічні криві

$$y^2 = x^3 - x \quad \text{та} \quad y^2 = x^3 - x + 1.$$

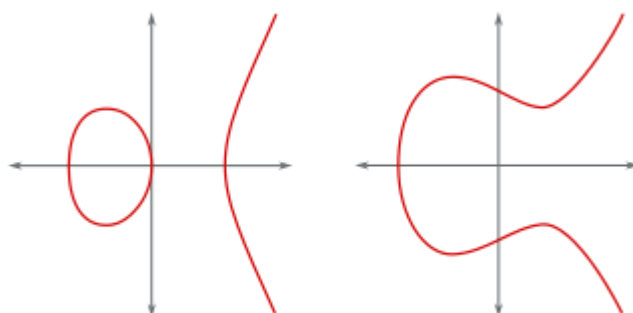


Рис. 1.1. Еліптичні криві.

Кубічні криві, які не мають особливих точок називають еліптичними кривими. Особливими точками називають точки, в яких функція невизначена або має нерегулярну поведінку. Наприклад, точки повернення або самоперетину кубічних кривих (рис.1.2).

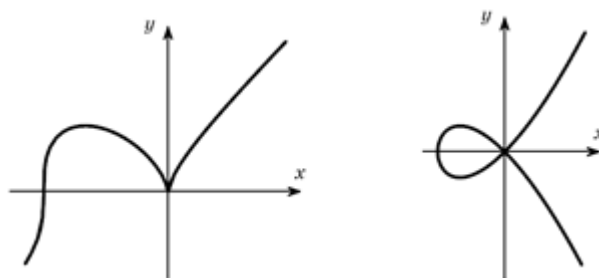


Рис. 1.2. Криві з особливими точками.

Для того, щоб криві в формі Веєрштрасса не мали особливих точок, дискримінант рівняння (1)

$$\Delta = 4a^3 + 27b^2 \quad (2)$$

не має дорівнювати 0. Еліптична крива має дві частини, якщо $\Delta < 0$ і одну частину, якщо $\Delta > 0$. Наприклад, перша крива на рис.1 має $\Delta = -4$, а друга $\Delta = 23$. Ще одною характеристикою еліптичної кривої є j -інваріант $j = \frac{1728(4a^3)}{\Delta}$. Криві з нульовим j -інваріантом називаються суперсингулярними, а з ненульовим - несуперсингулярними.

2.1.1 Порядок еліптичної кривої і точок еліптичної кривої

Порядком еліптичної кривої N_E над кінцевим полем F_q називається загальна кількість точок еліптичної кривої $(x, y) \in F_q$. Порядком точки P еліптичної кривої називається мінімальне число $m \geq 1$ таке, що $mP = O$. Якщо такого числа не існує, то точка має нескінченний порядок. Порядок точки завжди ділить порядок еліптичної кривої. Точка з визначеним порядком називається точкою кручення (або точкою кінцевого порядку). З цього випливає, що точка O є точкою невизначеного порядку.

2.2 Скінченні поля (Галуа)

2.2.1 Існування скінченного поля $F(p)$

Для будь-якого простого p існує скінченне поле, що складається точно з p елементів. Це поле унікально визначається з точністю до ізоморфізму і називається скінченим простим полем $F(p)$.

Елементи скінченного простого поля $F(p)$ можуть бути ідентифіковані за допомогою безлічі $[0, p-1]$ усіх позитивних цілих чисел, тобто менших за p . Для $F(p)$ визначено дві операції — складання і множення, що мають такі властивості:

- 1) $F(p)$ — абелева група відносно операції складання $\ll + \gg$.

Для $a, b \in F(p)$ сума $a + b$ задається як $a + b := r$, де $r \in F(p)$ — залишок від ділення суми цілих $a + b$ на p ;

- 2) $F(p) \setminus \{0\}$ позначається як $F(p)^*$ — абелева група відносно операції множення $\ll \times \gg$.

Для $a, b \in F(p)$ результат множення $a \times b$ отримується як $a \times b := r$, де $r \in F(p)$ є залишком від ділення цілого $a \times b$ на p . Операція множення $\ll \times \gg$, як правило, упускається і використовується позначення ab або $a \cdot b$.

2.2.2 Зворотний елемент групи $F(p)^*$

Нехай $a = \gamma^j \pmod{p}$ буде елементом групи $F(p)^*$. Тоді для кожного $a \in F(p)^*$ існує $b \in F(p)^*$ такий, що $a \cdot b = b \cdot a = 1$. Елемент b називається мультиплікативно зворотним до елемента a (інверсією), позначається як a^{-1} і може бути обчислений як $a^{-1} = \gamma^{p-1-j} \pmod{p}$.

2.2.3 Ділення в полі $F(p)$

Значення b/a в полі $F(p)$ існує, якщо знаменник не нульовий. В такому разі частка $b/a = b \cdot (a^{-1}) \pmod{p}$.

2.2.4 Квадрати і неквадрати в полі $F(p)$

Припустимо, що $p > 2$. Елемент $a \in F(p)^*$ називається квадратом у полі $F(p)^*$, якщо існує елемент $b \in F(p)^*$ такий, що $a = b^2 \pmod{p}$. Факт існування квадратного кореня визначається за умови, що a є квадратом у полі $F(p)^*$, якщо $a^{(p-1)/2} = 1$.

2.2.5 Пошук квадратного кореня в полі $F(p)$

Для знаходження квадратних коренів у полі $F(p)$ існують різні методи. Їх застосування дозволяє для кожного $a \in F(p)^*$ знайти $b \in F(p)^*$ таке, що $a = b^2 \pmod{p}$, де a є квадратом числа $b \in F(p)^*$.

Груповий закон для еліптичних кривих $E(F(p))$

3.1 Огляд систем координат

Зазвичай еліптична крива визначається в афінних координатах. Тому базова точка або відкритий ключ користувача задається в афінних координатах. Головним недоліком афінних координат є складність операції ділення в полі $F(Q)$ при виконанні як складання, так і подвоєння. Зменшення складності в цілому при складанні та подвоєнні точок може досягатись засобом уникнення операції ділення, причому якомога більше. Це досягається використанням при множенні (складанні та подвоєнні точок) інших координат, таких як проєктивні координати, координати Якобі та модифіковані координати Якобі тощо, які є трьохмірними. Причому має забезпечуватись вимога, щоб усі системи координат, що використовуються, були сумісними.

3.2 Груповий закон в афінних координатах

Нехай $F(q)$ є скінченним полем Галуа з $p > 3$. Нехай E є еліптичною кривою над $F(Q)$, що задається «коротким рівнянням Веєрштрасса»

$$Y^2 = X^3 + aX + b, \quad a, b \in F(q), \quad (3)$$

а також $4a^3 + 27b^2 \neq 0_F$ у полі $F(q)$. Тоді в афінних координатах груповий закон складання і подвоєння на еліптичній кривій (3) задається таким чином:

- 1) точка на нескінченності O_E є одиничним елементом до операції додавання «+»;
- 2) усі точки $R = (x, y)$ є такими, що $R \neq O_E$;
- 3) якщо $R_1 = (x_1, y_1)$ і $R_2 = (x_2, y_2)$ є дві різні точки на E — такі, що $R_1 \neq \pm R_2$ і $R_1, R_2 \neq O_E$, то сумою точок R_1 та R_2 є точка $R_3 = (x_3, y_3)$, координати якої визначаються як:

$$\begin{aligned} x_3 &= r^2 - x_1 - x_2; \\ y_3 &= r(x_1 - x_3) - y_1, \\ r &= (y_2 - y_1)/(x_2 - x_1); \end{aligned} \quad (4)$$

якщо $R = (x, y)$ є точка на E — така, що $R \neq O_E$ і $Y \neq O_F$, то її подвоєнням є точка $2R = (x_3, y_3)$, координати якої визначаються як:

$$\begin{aligned} x_3 &= r^2 - 2x; \\ y_3 &= r(x - x_3) - y, \\ r &= (3x^2 + a)/(2y); \end{aligned} \quad (5)$$

У разі якщо $R = (x, O_F)$, подвоєнням цієї точки є точка $2R = O_E$.

Геометрична інтерпретація складання двох точок з координатами (x_1, y_1) та (x_2, y_2) на еліптичній кривій наведена на рис.2.1.

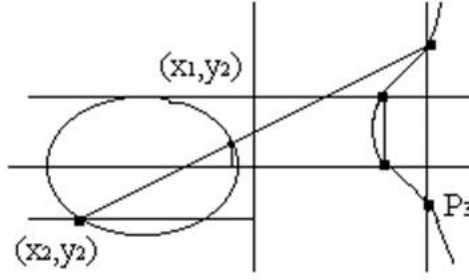


Рис. 2.1. Додавання точок еліптичної кривої.

3.3 Груповий закон у проєктивних координатах

Особливістю проєктивного базису є те, що при використанні проєктивних координат необхідно виконувати більше операцій множення, але немає операції ділення за модулем (інверсії). Після виконання скалярного множення в проєктивному базисі необхідно зробити зворотне перетворення на афінні координати. Але при виконанні перетворення з проєктивних координат на афінні, необхідне одне ділення в полі.

Проективний аналог короткого афінного рівняння Веєрштрасса (3) визначається однорідним кубічним рівнянням:

$$Y^2Z = X^3 + aXZ^2 + bZ^3, \quad a, b \in F(Q). \quad (6)$$

Безліч усіх трійок еквівалентна (X, Y, Z) і позначається як $(X, Y, Z) / \sim$.

Еліптична крива, що задається в проєктивних координатах, складається з усіх точок $R = (X, Y, Z)$ рівняння (6) так, що трійка (X, Y, Z) є розв'язком рівняння.

Існує співвідношення між точками Q кривої E , коли крива задана в афінних координатах, а точка R — у проєктивних координатах. В такому разі справедливі твердження:

- 1) Якщо $Q = (X_Q, Y_Q)$ є точка в афінних координатах, то $R = (X_Q, Y_Q, 1_F)$ є відповідною точкою в проєктивних координатах.
- 2) Якщо $R = (X, Y, Z)$ і $Z \neq 0_F$ є розв'язком (6), то $Q = (X/Z, Y/Z)$ є відповідною точкою в афінних координатах кривої E .
- 3) Існує тільки один розв'язок (6) із $Z = 0$, а саме: точка $(0_F, 1_F, 0_F)$, яка відповідає O_E .

У проєктивних координатах груповий закон задається таким чином:

- 1) точка $(0_F, 1_F, 0_F)$ є одиничним елементом O_E відносно операції «+»;
- 2) точка $R_1 = (X, Y, Z) \neq (0_F, 1_F, 0_F)$ є точкою на E , що задана в проєктивних координатах, тоді точка $-R = (X, -Y, Z)$
- 3) нехай $R_1 = (X_1, Y_1, Z_1)$ і $R_2 = (X_2, Y_2, Z_2)$ є дві відмінні точки на E — такі, що $R_1 \neq R_2$ і $R_1, R_2 \neq (0_F, 1_F, 0_F)$, тоді сума R_1 та $R_2 \in R_3 = (X_3, Y_3, Z_3)$ Координати X_3, Y_3 і Z_3 можуть бути обчислені за допомогою таких формул:

$$\begin{aligned} X_3 &= -su, \\ Y_3 &= t(u + s^2X_1Z_2) - s^3Y_1Z_2, \\ Z_3 &= s^3Z_1Z_2, \end{aligned} \quad (7)$$

де $s = X_2Z_1 - X_1Z_2$, $t = Y_2Z_1 - Y_1Z_2$, та $u = s^2(X_1Z_2 + X_2Z_1) - t^2Z_1Z_2$;

- 4) якщо $R = (X, Y, Z) \neq (0_F, 1_F, 0_F) \in$ точкою на E , тоді її подвоєння є $2R = (X_3, Y_3, Z_3)$.

Координати точки $2R = (X_3, Y_3, Z_3)$ можуть бути обчислені за допомогою таких формул:

$$\begin{aligned} X_3 &= -su, \\ Y_3 &= t(u + s^2X) - s^3Y, \\ Z_3 &= s^3Z, \end{aligned} \quad (8)$$

де $t = 3X^2 + aZ^2$, $s = 2YZ$, та $u = 2s^2X - t^2Z$.

3.4 Груповий закон у проєктивних координатах Якобі

Особливістю групового закону в проєктивних координатах Якобі є те, що скалярне множення вимагає більше мнужень, але не вимагає обчислення інверсій.

Аналогом рівняння Якобі в проєктивних координатах відносно короткого рівняння Веєрштрасса (4) є кубічне рівняння:

$$(Jac)Y^2 = X^3 + aXZ^4 + bZ^6, \quad a, b \in F(Q). \quad (9)$$

Безліч усіх трійок еквівалентна (X, Y, Z) і позначається як $(X, Y, Z)/\sim$.

Існує відношення між точками Q кривої E , коли крива задана в афінних координатах, а точки R — у проєктивних координатах. Так, справедливими є твердження:

- 1) Якщо $Q = (X_Q, Y_Q) \in$ точкою в афінних координатах E , то $R = (X_Q, Y_Q, 1_F) \in$ відповідною точкою в координатах Якобі.
- 2) Якщо $R = (X, Y, Z) (Z \neq 0_F) \in$ розв'язком (9), тобто в координатах Якобі, то $Q = (X/Z^2, Y/Z^3) \in$ відповідною точкою в афінних координатах точки E .
- 3) Існує тільки один розв'язок (9) зі значенням $Z = 0_F$, а саме точка $(1_F, 1_F, 0_F)$, яка відповідає O_E .

У проєктивних координатах Якобі груповий закон для (9) задається таким чином:

- 1) точка $(1_F, 1_F, 0_F) \in$ одиничним елементом 0_E відносно «+»;
- 2) якщо $R = (X, Y, Z) \neq (1_F, 1_F, 0_F) \in$ точкою на E , заданою в координатах Якобі, тоді точка $-R = (X, -Y, Z)$
- 3) якщо $R_1 = (X_1, Y_1, Z_1)$ і $R_2 = (X_2, Y_2, Z_2) \in$ дві відмінні точки на E , але такі, що $R_1 \neq R_2$ і $R_1, R_2 \neq (1_F, 1_F, 0_F)$, тоді сумою точок R_1 та R_2 є точка $R_3 = (X_3, Y_3, Z_3)$.

Координати X_3, Y_3 і Z_3 можуть бути обчислені за допомогою таких формул:

$$\begin{aligned} X_3 &= -h^3 - 2u_1h^2 + R^2, \\ Y_3 &= -s_1h^3 + R(u_1h^2 - X_3), \\ Z_3 &= Z_1Z_2h, \end{aligned} \quad (10)$$

де $u_1 = X_1Z_1^2$, $u_2 = X_2Z_1^2$, $s_1 = Y_1Z_2^3$, $s_2 = Y_2Z_1^3$, $h = u_2 - u_1$, і $R = s_2 - s_1$;

- 4) якщо $R = (X, Y, Z) \neq (1_F, 1_F, 0_F) \in$ точкою на E , тоді її подвоєння є $2R = (X_3, Y_3, Z_3)$.
Координати X_3, Y_3 і Z_3 можуть бути обчислені за допомогою таких формул:

$$\begin{aligned} X_3 &= t, \\ Y_3 &= -8Y^4 + m(s - t), \\ Z_3 &= 2YZ, \end{aligned} \tag{11}$$

де $s = 4XY^2$, $m = 3X^2 + aZ^4$, і $t = -2s + m^2$.

3.5 Груповий закон у модифікованих координатах Якобі

Згідно з тим же кубічним рівнянням (9), груповий закон у модифікованих координатах Якобі задається шляхом подання координат Якобі четвіркою координат (X, Y, Z, aZ^4) . Таке подання забезпечує найменшу складність операції подвоєння для еліптичної кривої $E(F(Q))$.

У модифікованих координатах Якобі груповий закон на еліптичній кривій задається таким чином:

- 1) якщо $R_1 = (X_1, Y_1, Z_1, aZ_1^4)$ і $R_2 = (X_2, Y_2, Z_2, aZ_2^4)$ є дві відмінні точки на E — такі, що $R_1 \neq R_2$ і $R_1, R_2 \neq (1_F, 1_F, 0_F, 0_F)$, тоді сумою є точка $R_3 = (X_3, Y_3, Z_3, aZ_3^4)$.

Координати X_3, Y_3 і Z_3 можуть бути обчислені за допомогою таких формул:

$$\begin{aligned} X_3 &= -h^3 - 2u_1h^2 + R^2, \\ Y_3 &= -s_1h^3 + R(u_1h^2 - X_3), \\ Z_3 &= Z_1Z_2h, \\ aZ_3^4 &= aZ_3^4, \end{aligned} \tag{12}$$

де $u_1 = X_1Z_2^2$, $u_2 = X_2Z_1^2$, $s_1 = Y_1Z_2^3$, $s_2 = Y_2Z_1^3$, $h = u_2 - u_1$, і $R = s_2 - s_1$;

- 2) якщо $R = (X, Y, Z, aZ^4) \neq (1_F, 1_F, 0_F, 0_F) \in$ точкою на E , тоді її подвоєння є $2R = (X_3, Y_3, Z_3, aZ_3^4)$.

Координати X_3, Y_3 і Z_3 можуть бути обчислені за допомогою таких формул:

$$\begin{aligned} X_3 &= t, \\ Y_3 &= m(s - t) - u, \\ Z_3 &= 2YZ, \\ aZ_3^4 &= 2u(aZ^4), \end{aligned} \tag{13}$$

де $s = 4XY^2$, $u = 8Y^4$, $m = 3X^2 + (aZ^4)$, і $t = -2s + m^2$.

3.6 Змішані координати

Подання точок еліптичної кривої в афінних координатах, проєктивних координатах, координатах Якобі або модифікованих координатах Якобі має обчислювальні переваги й недоліки. Немає ніякої системи координат, яка забезпечує обидва як швидкі складання, так і швидкі подвоєння. Можливе змішування різних координат, тобто

додавання двох точок, де перша задається в деякій одній системі координат, а друга — в деякій іншій системі координат. Ми можемо також вибрати систему координат результату. Оскільки ми маємо чотири різні види систем координат, це надає велике число можливостей. Змішані координати дають кращу комбінацію систем координат для подвоєнь або складань з мінімізацією часу для піднесення до степеня еліптичної кривої. Змішані координати діють найефективніше в алгоритмі попереднього обчислення.

Еліптична криптографія

4.1 Принципи еліптичної криптографії

Криптосистеми типу RSA засновані на складності задачі обчислення дискретних логарифмів і розкладання великих чисел на прості множники. Але такі ж принципи можуть бути застосовані для будь-якої множини чисел, де є схожа на множення (піднесення до степеня) операція (наприклад, операція додавання) і свої закони. Суть еліптичної криптографії полягає в тому, що в ній використовуються групи точок еліптичних кривих з визначеними для них груповими операціями. Еліптичний аналог традиційної криптографії з відкритим ключем виглядає таким чином:

- Абоненти обирають і повідомляють всім форму еліптичної кривої та цілу точку G на цій кривій, яка є генеруючою точкою.
- Абонент A обирає ціле число k і знаходить точку $PA = k \cdot G$ (додає точку G до самої себе k разів).
- Абонент B обирає число m і обчислює точку $PB = m \cdot G$. Потім вони обмінюються отриманими результатами і їх спільним секретним ключем стає точка $k \cdot m \cdot G$.

Щоб розкрити такий шифр, потрібно навчитися за відомими $k \cdot G$ і G обчислювати $k < p$, що і є аналогом дискретного логарифмування для систем RSA. Досить легко обчислити P за відомими k і G , але важко обчислити k за відомими P і G .

4.2 Електронний цифровий підпис на еліптичних кривих

Алгоритм ЕЦП на еліптичних кривих ECDSA (Elliptic Curve Digest Signature Algorithm) використовується в різних стандартах, серед яких ANSI X9.62, FIPS-186-2, IEEE 1363-2000 та інші. Розглянемо систему ЕЦП згідно стандарту ANSI X9.62.

4.2.1 Вимоги до еліптичних кривих згідно стандарту X9.62

Для практичного застосування алгоритму ECDSA накладаються обмеження на поля, в яких визначені еліптичні криві, рівняння еліптичних кривих і на порядок генеруючих точок. Для забезпечення високого рівня захищеності криптографічних систем на еліптичних кривих необхідно, щоб порядок кривої NE ділився на достатньо велике просте число q . Стандарт ANSI X9.62 вимагає $q > 2^{160}$. Криптографічні еліптичні криві мають задовольняти наступним умовам:

- 1) Криві розглядаються над простими полями F_p , де p є простим числом (або над полями характеристики два: F_2^m).
- 2) Крива $E_p(a, b)$ задається в формі Веєрштраса $y^2 = x^3 + ax + b$, де $a, b \in F_p$ і $(4a^3 + 27b^2) \neq 0 \pmod{p}$.
- 3) На кривій має бути обрана генеруюча точка $G = (xG, yG)$ (xG і $yG \in F_p$) простого порядку q , де $q > 2^{160}$ і $q > 4\sqrt{p}$.
- 4) Порядок кривої N_E має ділитися на q . Результат ділення N_E/q називається кофактором.

4.2.2 Вибір параметрів ЕЦП

Алгоритм вибору параметрів ЕЦП виглядає наступним чином:

- 1) Обрати хеш-функцію $h = H(M)$, де M — повідомлення.
- 2) Обрати просте число p (характеристика поля F_p).
- 3) Обрати форму еліптичної кривої згідно описаних вище вимог, яка задає групу точок еліптичної кривої $E_p(a, b)$ і генеруючу точку $G = (x_G, y_G)$.

4.2.3 Генерація ключів ЕЦП

Для ЕЦП необхідна пара ключів — відкритий і секретний. При цьому секретний ключ відомий тільки тому, хто підписує повідомлення, а відкритий — будь-кому, хто хоче перевірити його автентичність і цілісність. Також загальновідомими є параметри самого алгоритма ЕЦП, форма еліптичної кривої, генеруюча точка і хеш-функція $H(M)$. Ключі для ЕЦП формуються наступним чином:

- 1) Абонент A обирає ціле число $d_A < p$. Це є секретним ключем абонента для його підписів. Потім він обчислює відкритий ключ $P_A = d_A G$, який є точкою кривої $E_q(a, b)$.
- 2) Абонент B аналогічним чином обирає свій секретний ключ d_B та знаходить відкритий ключ для підписів P_B .
- 3) Абоненти обмінюються відкритими ключами.

4.2.4 Формування цифрового підпису

Для того, щоб підписати повідомлення M , абонент A повинен зробити наступне:

- 1) Обчислити значення хеш-функції повідомлення M : $h = H(M)$, $h < p$;
- 2) Обрати довільне ціле число k_A з інтервалу $[1, p - 1]$ (разовий ключ);
- 3) Обчислити точку $R = k_A G = (x_1, y_1)$
- 4) Обчислити значення $r = x_1 \bmod p$. При цьому перевіряється, щоб $r \neq 0$, бо в цьому випадку підпис s не буде залежати від закритого ключа k_A . Якщо $r = 0$, то пара чисел (r, s) не може бути використана для цифрового підпису і вибирають інше значення k_A , тобто повертаються до кроку 2.
- 5) Обчислити зворотній елемент k_A^{-1} в полі F_p
- 6) Обчислити $s = k_A^{-1}(h + d_A r) \bmod p$. Якщо $s = 0$, то значення $s^{-1} \bmod p$, необхідне для перевірки підпису, не існує. Тобто, у випадку $s = 0$ потрібно повернутися до кроку 2.

Цифровим підписом для повідомлення M є пара цілих чисел $DS = (r, s)$. Для цієї схеми можна визначити ключове рівняння

$$sk_A = (h + d_A r) \bmod p, \quad (14)$$

яке пов'язує параметри s і r з разовим і секретним ключами k_A і d_A . Воно використовується при формуванні і перевірці цифрового підпису.

4.2.5 Перевірка цифрового підпису

Абонент перевіряє цифровий підпис абонента, маючи у розпорядженні: відкритий ключ P_A абонента, параметри кривої, хеш-функцію $H(M)$ та підписане повідомлення (M, r, s) . Суть перевірки полягає в обчисленні на основі цих даних значення r' і порівнянні його з отриманим r . Помноживши (14) на інверсію s^{-1} другого параметру підпису і враховуючи, що $P_A = d_A G$, для точок криптосистеми в результаті експоненціювання (скалярного множення) отримаємо рівність

$$\begin{aligned} k_A G &= s^{-1} h G + s^{-1} r d_A G = u G + v P_A, \\ u &= s^{-1} h \bmod p, \\ v &= s^{-1} r \bmod p. \end{aligned} \quad (15)$$

Згідно пп.3 і 4 протоколу формування підпису ліва частина цього рівняння визначає точку $R = (x_1, y_1)$ і, відповідно, параметр $r = x_1 \bmod p$. Права частина рівняння включає відомі отримувачу дані, які він використовує для обчислення параметру r' . Таким чином, щоб перевірити підпис абонента (r, s) на повідомленні M , абонент B повинен зробити наступне:

- 1) Отримати цифровий підпис (r, s) абонента для повідомлення M ;
- 2) Обчислити значення хеш-функції повідомлення $h = H(M)$;
- 3) Обчислити зворотній елемент s^{-1} в полі F_p ;
- 4) Обчислити $u = s^{-1} h \bmod n$, $v = s^{-1} r \bmod p$;
- 5) Обчислити точку $R' = uG + vP_A = (x'_1, y'_1)$;
- 6) Обчислити $r' = x'_1 \bmod p$;
- 7) Підпис вірний, якщо $r' = r$.

Приклади застосування

5.1 Визначення порядку канонічних еліптичних кривих

Розглянемо канонічну еліптичну криву E_p над простим полем Галуа. Нехай $\chi(z)$ — квадратичний характер елемента z поля F_p , такий що

$$\chi(z) = \begin{cases} 1, & z = a^2 \\ -1, & z \neq a^2, \\ 0, & z = 0. \end{cases} \quad a \in F_p \quad (16)$$

Тобто, якщо z має квадратний корінь в полі F_p , то $\chi(z) = 1$, якщо ні, то $\chi(z) = -1$. В першому випадку кажуть, що z є квадратичним залишком, у другому — квадратичним незалишком. З урахуванням (1) порядок кривої можливо розрахувати перебором всіх елементів поля F_p як суму

$$N_E = 1 + \sum_{x \in F_p} \chi\{(x^3 + ax + b) + 1\} = p + 1 + \sum_{x \in F_p} \chi\{(x^3 + ax + b)\} = p + 1 - t, \quad (17)$$

де $t = - \sum_{x \in F_p} \chi\{(x^3 + ax + b)\}$

Перша одиниця в формулі (17) враховує точку O , а під знаком суми кожен розв'язок рівняння (1) дає по дві точки кривої. Винятком є точки другого порядку з координатою $y = 0$, які згідно з (16), (17) враховуються по одному разу.

Приклад 1. Розглянемо криву $y^2 = x^3 + 1$ над полем F_5 . Перебором значень x отримаємо всі рішення рівняння, які зведені в Таблиці 1.

Таблиця 1. Визначення координат точок кривої $y^2 = x^3 + 1$ над полем F_5

x	0	1	2	3	4
x^2	0	1	4	4	1
y^2	1	2	4	3	0
y_1	1	—	2	—	0
y_2	—1	—	—2	—	

У цій таблиці для наочності використано додатні та від'ємні значення y координати. Значення $y = -1$ порівнюється з додатнім залишком $p - 1 = 4$, а $y = -2 \equiv 3 \pmod{5}$. Разом з точкою O порядок кривої дорівнює 6.

Висновок

У роботі ми розглянули криптографічні протоколи, що базуються на доведенні з нульовим знанням. Розглянули типи протоколів, їхні завдання, функції, вимоги до безпеки і види атак на них. Також було розглянуто криптографічні протоколи, що базуються на доведенні з нульовим знанням для задач про розфарбування графа і знаходження гамільтонового циклу. Розглянуто питання по побудові протоколів. Доведено твердження про неможливість обману будь-якою з сторін, та твердження, що представлений протокол реалізує доведення з нульовим знанням.

Було програмно реалізовано протокол доведення з нульовим знанням для задачі відшукування гамільтонового циклу в графі. Розглянуто приклад на якому при t повтореннях протоколу ми бачимо істинність доведення і неможливість його обходу будь-якою з сторін чи взламу третьою особою.

Отже, як бачимо з даної роботи, актуальність криптології росте з кожним роком, без методів шифрування/дешифрування, електронного цифрового підпису, ідентифікації / аутентифікації, неможливий захист інформації. Яка на сьогодні є основою всього і її об'єми збільшуються дуже швидко. Головну роль в реалізації цих методів відіграють протоколи доведення з нульовим знанням.

Література

- [1] *О.В.Вербіцький* Вступ до криптології, - Львів: Видавництво наукової технічної літератури, 1998. - 247 с.
- [2] *Рябко Б.Я., Фионов А.Н.* Основы современной криптографии и стеганографии, - М.: Научный мир, 2004 г. - 173с.
- [3] *Анатолий Малюк* Теория защиты информации. - М.: Телеком, 2012. - 186 с.
- [4] *Шнайер Брюс, Фергюсон Нильс* Практическая криптография, 2-е изд. - М: ООО "И.Д.Вильямс 2005. — 424 с.