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

Вступ

Питання безпечного передавання інформації виникли ще за часів Римської Імперії і набувають по сьогоднішній день все більшої актуальності. Ці питання розглядаються в криптології.

Криптологія — розділ науки, що вивчає методи шифрування і дешифрування інформації. Вона включає в себе два розділи: криптографію та криптоаналіз.

Криптографія займається розробкою методів шифрування даних, у той час як криптоаналіз займається оцінкою сильних і слабких сторін методів шифрування, а також розробкою методів, які дозволяють зламувати криптосистеми.

Слово «криптологія» (англ. cryptology) зустрічається в англійській мові з XVII століття, і спочатку означало «скритність в мові»; в сучасному значенні було введено американським вченим Вільямом Фрідманом і популяризована письменником Девідом Каном.

Розглянемо схему поділу поділу криптосистем:

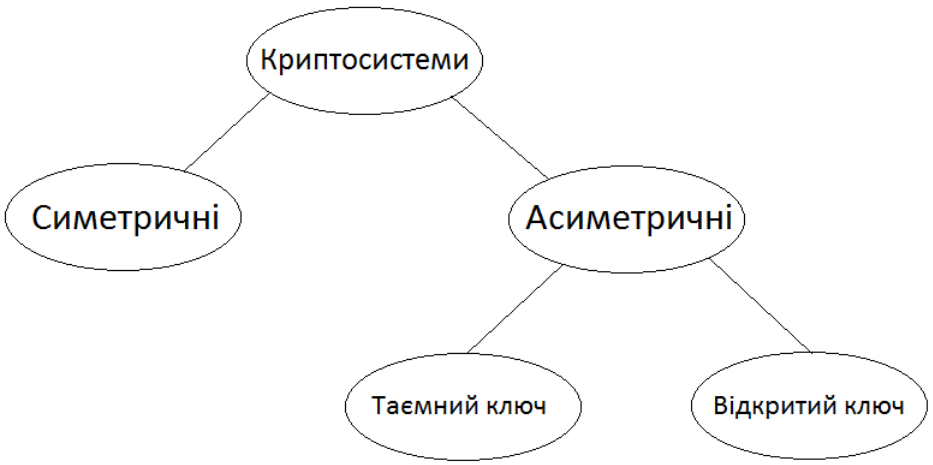

Рис. 1.1. Криптосистеми.

1976 рік відкрив сучасний етап у криптографії. Для новітньої криптогафії характерною рисою є поява принципово нових криптографічних задач, а також принципово нових розв'язків задач класичних. Тому часто говорять про революцію у галузі криптографії. Поступ,що відбувся у 1976 році, пов'язаний з іменами американських математиків Вайтфілда Діффі та Мартіна Хелмана, які розвинули ідеологію відкритого ключа.

У криптосистемі з відкритим ключем процедура шифрування є загальнодоступною. Це однак не означає як у традиційних криптосистемах, що загальнодоступним є також дешифрування.

Метою цієї курсової є вивчення криптографічних протоколів доведення з нульовим знанням.

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:

$$y^2 = x^3 + ax + b. \tag{1}$$

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

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

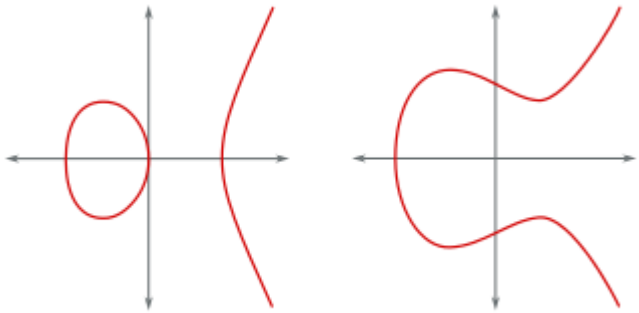

Рис. 1.1. Еліптичні криві.

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).

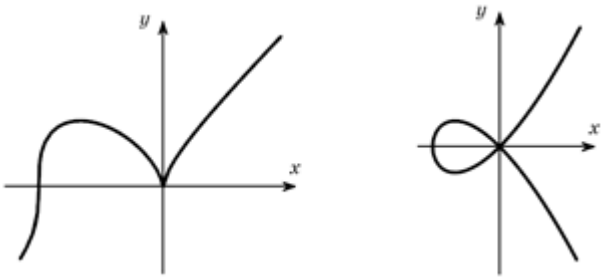

Рис. 1.2. Криві з особливими точками.

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

$$\Delta = 4a^3 + 27b^2 \tag{2}$$

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 скінченним 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 «+».
   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 «×».

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 «×», як правило, упускається і використовується позначення ab або $a \cdot b$.

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

Нехай $a = \gamma^j (\mod p)$ 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 $a^{-1} = \gamma^{p-1-j} (\mod p)$.

2.2.3 Ділення в полі $F(p)$

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

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 $a = b^2 (\mod p)$. 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 $a = b^2(\mod p)$, 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 проективні 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»

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

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:

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

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:

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

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.

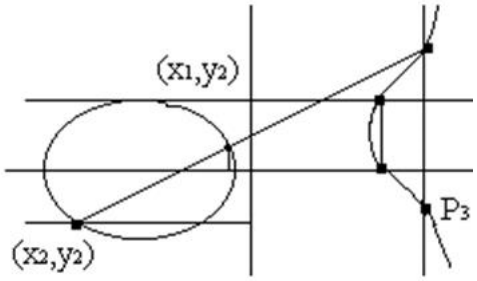

Рис. 2.1. Додавання точок еліптичної кривої.

3.3 Груповий закон у проективних координатах

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

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

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

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

Еліптична крива, що задається в проективних 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 проективних 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 проективних координатах.

2) Якщо $R = (X, Y, Z)$ і $Z \neq O_F$ 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 проективних 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 проективних 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 є $R_3 = (X_3, Y_3, Z_3)$ Координати X_3, Y_3 і Z_3 можуть бути обчислені за допомогою таких формул:

$$\begin{aligned} X_3 &= -su, \\ Y_3 &= t(u + s^2 X_1 Z_2) - s^3 Y_1 Z_2, \\ Z_3 &= s^3 Z_1 Z_2, \end{aligned} \tag{7}$$

де $s = X_2 Z_1 - X_1 Z_2,\ t = Y_2 Z_1 - Y_1 Z_2,$ та $u = s^2(X_1 Z_2 + X_2 Z_1) - t^2 Z_1 Z_2$;

4) якщо $R = (X, Y, Z) \neq (0_F, 1_F, 0_F)$ є 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:

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

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

3.4 Груповий закон у проективних координатах Якобі

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

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

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

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 проективних координатах. Так, справедливими є твердження:

1) Якщо $Q = (X_Q, Y_Q)$ є точкою в афінних координатах E, то $R = (X_Q, Y_Q, 1_F)$ є відповідною точкою в координатах Якобі.

2) Якщо $R = (X, Y, Z)(Z \neq 0_F)$ є розв'язком (9), тобто в координатах Якобі, то $Q = (X/Z^2, Y/Z^3)$ є 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 проективних координатах Якобі груповий закон для (9) задається таким чином:

1) точка $(1_F, 1_F, 0_F)$ є одиничним елементом 0_E відносно «+»;

2) якщо $R = (X, Y, Z) \neq (1_F, 1_F, 0_F)$ є точкою на E, заданою в координатах Якобі, тоді точка $-R = (X, -Y, Z)$

3) якщо $R_1 = (X_1, Y_1, Z_1)$ і $R_2 = (X_2, Y_2, Z_2)$ є 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:

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

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 $R = (X, Y, Z) \neq (1_F, 1_F, 0_F)$ є 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 $R = (X, Y, Z, aZ^4) \neq (1_F, 1_F, 0_F, 0_F)$ є 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, проективних 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.

Висновок

У роботі ми розлянули 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 відшукання 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.