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:

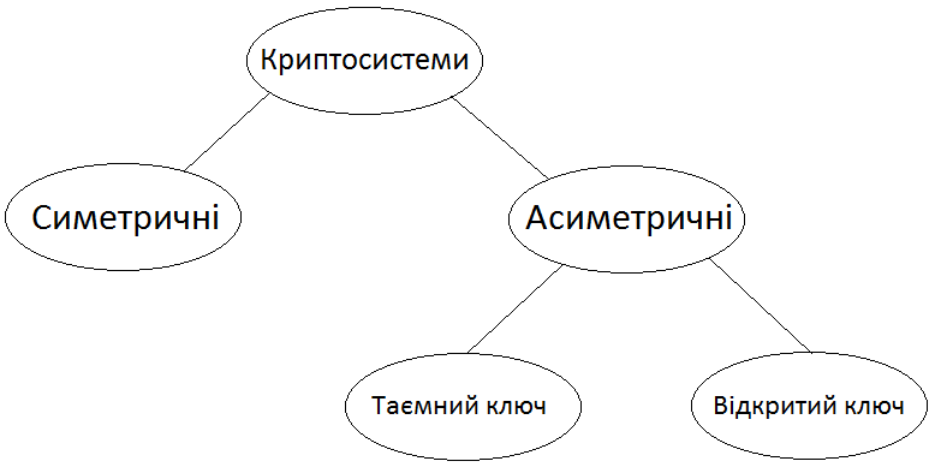

Рис. 1.1. Криптосистеми.

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

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

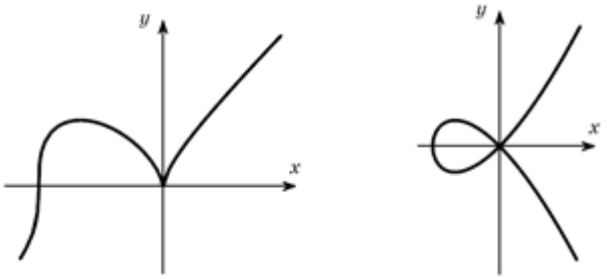

Рис. 1.1. Криві з особливими точками.

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.2.2). 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.

2.2 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 $\ll\times\gg$.

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 $a = \gamma^j(\mod p)$ 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:

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

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:

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

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.1.1.

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.

3.7 Класифікація криптографічних протоколів

- **Протоколи шифрування / розшифрування**

  В основі протоколу цього класу міститься деякий симетричний або асиметричний алгоритм шифрування / розшифрування. Алгоритм шифрування виконується на передачі відправником повідомлення, в результаті чого повідомлення перетвориться з відкритої форми в шифровану. Алгоритм розшифрування виконується на прийомі одержувачем, в результаті чого повідомлення перетвориться з шифрованого форми у відкриту. Так забезпечується властивість конфіденційності.

  Для забезпечення властивості цілісності переданих повідомлень симетричні алгоритми шифрування / розшифрування, зазвичай, поєднуються з алгоритмами

обчислення імітозахисної вставки (ІЗВ) на передачу та перевірки ІЗВ на прийомі, для чого використовується ключ шифрування. При використанні асиметричних алгоритмів шифрування / розшифрування властивість цілісності забезпечується окремо шляхом обчислення електронного цифрового підпису (ЕЦП) на передачу та перевірки ЕЦП на прийомі, ніж забезпечуються також властивості безвідмовності і автентичності прийнятого повідомлення.

- **Протоколи електронного цифрового підпису (ЕЦП)**

  В основі протоколу цього класу міститься певний алгоритм обчислення ЕЦП на передачі за допомогою секретного ключа відправника та перевірки ЕЦП на прийомі з допомогою відповідного відкритого ключа, що витягується з відкритого довідника, але захищеного від модифікацій. У разі позитивного результату перевірки протокол, зазвичай, завершується операцією архівування прийнятого повідомлення, його ЕЦП і відповідного відкритого ключа. Операція архівування може не виконуватися, якщо ЕЦП використовується тільки для забезпечення властивостей цілісності і автентичності отримане повідомлення, але не безвідмовності. У цьому випадку, після перевірки, ЕЦП може бути знищена відразу або після обмеженого проміжку часу очікування.

- **Протоколи ідентифікації / аутентифікації**

  В основі протоколу ідентифікації міститься певний алгоритм перевірки того факту, що ідентифікований об'єкт (користувач, пристрій, процес, ...), який пред'явив деякий ім'я (ідентифікатор), знає секретну інформацію, відому тільки заявленому об'єкту, причому метод перевірки є, звичайно, непрямим, то тобто без пред'явлення цієї секретної інформації.

  Зазвичай з кожним ім'ям (ідентифікатором) об'єкта пов'язується перелік його прав і повноважень у системі, записаний в захищеній базі даних. У цьому випадку протокол ідентифікації може бути розширений до протоколу аутентифікації, в якому ідентифікований об'єкт перевіряється на уповноваження до замовленої послуги.

  Якщо в протоколі ідентифікації використовується ЕЦП, то роль секретної інформації відіграє секретний ключ ЕЦП, а перевірка ЕЦП здійснюється за допомогою відкритого ключа ЕЦП, знання якого не дозволяє визначити відповідний секретний ключ, але дозволяє переконатися в тому, що він відомий автору ЕЦП.

- **Протоколи з автентифікованим розподілом ключів**

  Протоколи цього класу поєднують аутентифікацію користувачів з протоколом генерації і розподілу ключів по каналу зв'язку. Протокол має двох або трьох учасників; третім учасником є центр генерації та розподілу ключів (ЦГРК), званий для стислості сервером S.

  Протокол складається з трьох етапів, що мають назви: генерація, реєстрація і комунікація.

  На етапі генерації сервер S генерує числові значення параметрів системи, в тому числі, свій секретний і відкритий ключ.

На етапі реєстрації сервер S ідентифікує користувачів за документами (при особистій явці або через уповноважених осіб), для кожного об'єкта генерує ключову і / або ідентифікаційну інформацію і формує маркер безпеки, що містить необхідні системні константи і відкритий ключ сервера S (при необхідності).

На етапі комунікації реалізується власне протокол автентифікованим ключового обміну, який завершується формуванням спільного сеансового ключа

3.8 Різновиди атак на протоколи

- Атаки, спрямовані проти криптографічних алгоритмів
- Атаки проти криптографічних методів, що застосовуються для реалізації протоколів
- Атаки проти самих протоколів (активні або пасивні)

Доведення з нульовим знанням

Розглянемо наступну задачу, яка виникає в деяких криптографічних додатках. Знову беруть участь Аліса і Боб. Аліса знає вирішення деякої складної задачі, вона хоче переконати Боба в цьому, але так, щоб Боб не дізнався самого вирішення задачі. Тобто, в результаті Боб має переконатися в тому, що Аліса знає вирішення, але не повинен дізнатись чого-небудь про саме вирішення. Для того щоб краще зрозуміти ситуацію, розглянемо випадок з життя піратів. Нехай, наприклад, Аліса знає карту острова, де захований клад, а Боб — капітан корабля, який може доставити її на острів. Аліса хоче довести, що карта є в неї, не показуючи її Бобу (інакше Боб обійдеться без Аліси, і весь клад дістанеться йому). Така ж сама задача актуальна для комп'ютерних мереж в тих випадках , коли Боб (сервер або контроллер домену) повинен прийняти рішення про допуск Аліси до інформації, яка є в мережі, але при цьому Аліса не хоче, щоб хто-небудь, хто прослуховує канал передачі даних і сам сервер, отримали які-небудь знання про її пароль. Тобто, Боб отримує "нульове знання" про пароль (або карту) Аліси, але впевнений, що в Аліси такий пароль (або карта) є.

Тому, наша задача — побудувати протокол "доведення з нульовим знанням". При цьому ми вважаємо, що кожен з учасників може вести "нечесну" гру і намагатися обманути іншого.

В якості складної задачі, вирішення якої відомо Алісі, ми спочатку розглянемо задачу розфарбування графа трьома кольорами. Ми опишемо достатньо простий в ідейному плані протокол доведення для цієї задачі. Потім ми розглянемо задачу знаходження гамільтонового циклу в графі з більш складним в ідейному плані, але більш ефективним в плані реалізації протоколом доведення. Відзначимо, що обидві задачі — розфарбування графа трьома кольорами і знаходження гамільтонового циклу — є NP-повними. Тобто, NP-повнота задачі неформально означає, що час вирішення задачі росте експоненціально з ростом розміру задачі (об'єму вихідних даних).

4.1 Задача про розфарбування графа

В задачі про розфарбування графа розглядається граф з множиною вершин V і множиною ребер E (числа елементів в цих множинах будемо позначати через $|V|$ і $|E|$). Аліса знає правильне розфарбування цього графа трьома фарбами (червоною (R), синьою (B) і жовтою (Y)). Правильне розфарбування - це така, коли будь-які дві вершини, з'єднані одним ребром, зафарбовані різними кольорами.
Наведемо приклад (рис. 3.1).

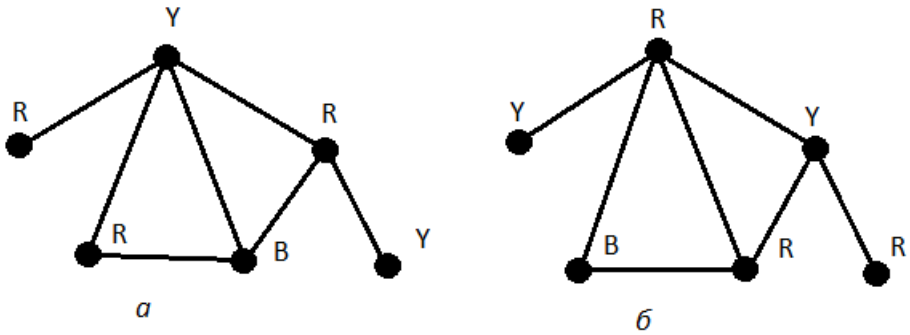

Рис. 3.1. Приклади розфарбувань: a - правильне, b - неправильне

Для отримання правильного розфарбування графа трьома фарбами відоми тільки експоненційні алгоритми, тобто такі, в яких час вирішення зростає експоненційно з ростом кількості вершин і ребер в графі. Тому у випадку великих $|V|$ і $|E|$ ця задача практично нерозв'язна.

Аліса знає (правильне) розфарбування графа з великими $|V|$ і $|E|$. Вона хоче доказати це Бобу, але так, щоб він нічого не дізнався про це розфарбування.

Протокол доведення складається з множини однакових етапів. Опишемо спочатку один етап.

Крок 1. Аліса вибирає випадкову перестановку П з трьох букв R, B, Y і перенумеровує всі вершини графа відповідно до цієї перестановки. Очевидно, що розфарбування залишається правильним. Наприклад, якщо П = (Y,R,B), то граф зліва на рис. 3.1 перетворюється в граф на рис. 3.2.

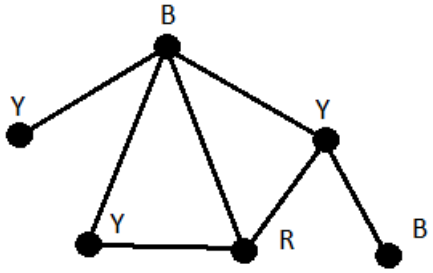

Рис. 3.2. Інший варіант розфарбування

Крок 2. Для кожної вершини v з множини V Аліса генерує велике випадкове число r і замінює в ньому два останніх біти на 00, що відповідає червоній вершині, 01 - синій, 10 - жовтій.

Крок 3. Для кожної вершини v Аліса формує дані, які використовуються в RSA, а саме, P_v, Q_v, $N_v = P_v Q_v$, c_v і d_v.

Крок 4. Аліса обчислює

$$Z_v = r_v^{d_v} \mod N_v \tag{14}$$

і посилає Бобу значення N_v, d_v і Z_v для кожної вершини графа.

Крок 5. Боб вибирає випадково одне ребро з множини E і повідомляє Алісі, яке саме ребро він вибрав. У відповідь Аліса висилає числа c_{v_1} і c_{v_2}, які відповідають вершинам цього ребра. Після цього Боб обчислює

$$\hat{Z}_{v_1} = Z_{v_1}^{c_{v_1}} \mod N_{v_1} = r_{v_1}, \quad \hat{Z}_{v_2} = Z_{v_2}^{c_{v_2}} \mod N_{v_2} = r_{v_2} \tag{15}$$

і порівнює два молодших біти в отриманих числах. При правильному розфарбуванні два молодших біти в числах $\hat{Z}_{v_1}$ і $\hat{Z}_{v_2}$ мають бути різні. Якщо значення співпали, значить, Аліса намагалась обманути Боба, і на цьому все закінчується. Якщо не співпали, то весь описаний процес повторюється $a|E|$ разів, де $a > 0$ − параметр.

Твердження 3.1. Якщо Аліса не знає правильного розфарбування графа, то ймовірність того, що вона зможе обманути Боба не перевищує e^{-a} , де $e \approx 2.718$ − число Ейлера (підстава натурального логарифма).

Зауваження. Якщо взяти велике a, то ймовірність обману можна зробити дуже малою. Наприклад, при $a = 5$ ця ймовірність менше 0.01.

Доведення. Нехай Аліса не розпоряджає правильне розфарбовування графа. Значить, хоча б для одного ребра з E вершини покрашені в один колір. Якщо Аліса буде діяти по протоколу, то ймовірність того, що Боб звернеться до такого ребра, не менше $1/|E|$ (в цьому випадку Аліса викрита). Значить, ймовірність того, що Аліса не буде викрита за час одного етапу, не перевищує $1-1/|E|$ і, тому, ймовірність того, що вона не буде викритою за $a|E|$ етапів, не перевищує $(1 - 1/|E|)^{a|E|}$. Використовуючи відому нерівність $1 - x \leq e^{-x}$, отримуємо

$$(1 - 1/|E|)^{a|E|} \leq (e^{-1/|E|})^{a|E|} = e^{-a}. \tag{16}$$

Перевіримо всі властивості, необхідні для протоколу з нульовим знанням.

1) Ми бачимо, що ймовірність можливості обману для Аліси може бути зроблена як завгодно малою.

2) Поглянемо, чому Боб не отримує жодної інформації про розфарбовування. Через те, що кольори переставляються випадково на кожному етапі, він не зможе дізнатись істинне розфабовування, перебираючи всі ребра одне за іншим, і взагалі він нічого не дізнається про правильне розфарування. Те, що на другому кроці вибирається випадкове число r_v, не дозволяє Бобу вирахувати за відомими N_v і d_v коди відповідних фарб. Він не може декодувати отримане Z_v тому, що він не знає чисел c_v, так як вони для всіх вершин не відсилаються, а вирахувати їх він не може, не знаючи P_v та Q_v.

3) Розглянемо ще одну можливість обману, яка впринципі може бути у Аліси. Здавалося б, Аліса може підмінити c_{v_1} і c_{v_2}, якщо їй це вигідно. Однак це неможливо в силу того, що число c_v, яке задовільняє рівність

$$c_v d_v \mod ((P_v - 1)(Q_v - 1)) = 1, \tag{17}$$

єдине.

Таким чином, виконані всі властивості:

1) Аліса доказує Бобу, що знає розв'язок задачі, і ймовірність того, що Боб обманутий, не більше e^{-a};

2) Боб не отримує жодних відомостей про розфарбування.

Розглянемо останню можливість обману для всіх учасників. Що буде, якщо вони будуть ухилятися від вказаного алгоритму, вибираючи параметри не випадково?

Нехай, наприклад, Боб запитує ребра графа не випадково, а по якому-небудь простому правилу (наприклад, у відповідності з їх номерами). В цьому випадку, якщо в Аліси немає правильного розфарбування, то вона зможе обманути Боба, "правильно"розфарбовуючи ті ребра, про які будуть запитувати. Таким чином, Боб зацікавлений в тому, щоб його запити були випадкові і не містили в собі якої-небудь закономірності.

Стійкість решти кроків визначається стійкістю RSA, і при великих P_v і Q_v система достатньо надійна.

4.2 Задача знаходження гамільтонового циклу в графі

Задача яку ми розглядаємо не просто представляє нам можливість описати ще одну схему побудови протоколу доведення з нульовим знанням, але і має важливе теоретичне значення. Блюм (Manuel Blum) показав, що будь-яке математичне твердження може бути представлене у вигляді графа, причому доведення цього твердження відповідає гамільтоновому циклу в цьому графі. Тому наявність протоколу доведення з нульовим знанням для гамільтонового циклу означає, що доведення будь-якого математичного твердження може бути представлено в формі доведення з нульовим знанням.

Означення 1: Гамільтоновим циклом в графі називається неперервний шлях, що проходить через усі вершини графа рівно по одному разу.

Приклад 3.2: Розглянемо граф, зображений на рис. 3.3.

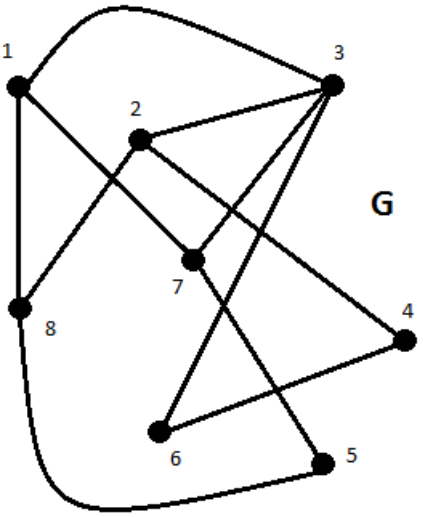

Рис. 3.3. Граф з гамільтоновим циклом (8, 2, 4, 6, 3, 5, 7, 1)

Шлях, який проходить послідовно через вершини $8, 2, 4, 6, 3, 5, 7, 1$, являє собою гамільтонів цикл. Дійсно, в цьому шляху містяться всі вершини графа, і кожна вершина відвідується лише один раз.

Ясно, що якщо в графі G з n вершинами гамільтонів цикл існує, то при деякій нумерації вершин він пройде точно через вершини з послідовними номерами $1, 2, \ldots, n$. Тому шляхом перебору всіх можливих нумерацій вершин ми обов'язково знайдемо гамільтонів цикл. Але кількість можливих нумерацій дорівнює $n!$, і тому вже при помірно великих n, наприклад, при $n = 100$, такий підхід практично неможливо реалізувати. Доведено, що задача знаходження гамільтонового циклу в графі є NP-повною. Ми вже говорили коротко про поняття NP-повноти. Неформально, NP-повнота розглянутої задачі означає, що для її вирішення не існують (точніше невідомі) алгоритми набагато швидші, ніж вказаний метод перебору.

Нашою задачею буде побудова криптографічного протоколу, з допомогою якого Аліса буде доказувати Бобу, що вона знає гамільтонів цикл в деякому графі G так, щоб Боб не отримав ніяких знань про сам цей цикл. Іншими словами, Аліса буде надавати Бобу доведення з нульовим знанням. Нагадаємо, що "нульове знання" означає, що незалежно від кількості реалізацій протоколу доведення Боб буде мати точно такі ж знання про гамільтонів цикл, які він міг би отримати, просто вивчаючи представлений йому граф G.

Припустимо, що Аліса знає гамільтонів цикл в графі G. Тепер вона може це доводити Бобу і всім, хто має граф G, з допомогою описаного нище протоколу. Аліса може використовувати це доведення, наприклад, для ідентифікації своєї особистості. Але перш ніж ми перейдемо до опису протоколу, домовимось про деякі позначення.

Ми будемо позначати графи буквами G, H, F, розуміючи під цим одночасно відповідні матриці суміжності. Елемент матриці $H_{i,j} = 1$, якщо в графі H є ребро, яке сполучає вершини i та j; $H_{i,j} = 0$ в протилежному випадку. Символом $||$ будемо позначати конкатенацію двох чисел, точніше, двійкових слів, які їм відповідають. Нам знадобиться шифр з відкритим ключем. Загалом, це може бути будь-який шифр, але для визначеності будемо використовувати шифр RSA . Будемо вважати, що Аліса сформувала систему RSA з відкритими параметрами N і d. Важливо, що зашифровані в цій системі повідомлення може розшифрувати тільки Аліса і більше ніхто.

Протокол доведення складається з наступних чотирьох кроків:

Крок 1. Аліса будує граф H, який є копією вихідного графа G, де у всіх вершин нові, випадково вибрані номера. На мові теорії графів говорять, що H ізоморфний до G. Іншими словами, H отримується шляхом деякої перестановки вершин в графі G (зі збереженням зв'язків між вершинами). Аліса кодує матрицю H, приписуючи до початкових нулів і одиниць випадкові числа r_ij по схемі $\tilde{H}_ij = r_ij||H_ij$. Потім вона шифрує елементи матриці $\tilde{H}$, отримуючи зашифровану матрицю F, $F_ij = \tilde{H}_{ij}^d \mod N$. Матрицю F Аліса передає Бобу.

Крок 2. Боб, отримавши зашифрований граф F, задає Алісі одне з двох питань.

1) Який гамільтонів цикл для графа H?
2) Чи дійсно граф H ізоморфний до G?

Крок 3. Аліса відповідає на відповідне запитання Боба.

1) Вона розшифровує в F ребра, які утворюють гамільтонів цикл.
2) Вона розшифровує F повністю (фактично передає граф $\tilde{H}$) і представляє перестановки, з допомогою яких граф H був отриманий з графа G.

Крок 4. Отримавши відповідь, Боб перевіряє правильність розшифрування шляхом повторного шифрування і порівняння з F і переконується або в тому, що показані ребра дійсно утворюють гамільтонів цикл, або в тому, що представлені перестановки дійсно переводять граф G в граф H.

Весь протокол повторюється t разів.
Обговоримо спочатку коротко декілька питань по побудові протоколу.

1) Навіщо Аліса будує ізоморфний граф? Якщо б вона цього не робила, то Боб, отримавши відповідь на своє питання номер один, дізнався би гамільтонів цикл в графі G.

2) Навіщо Аліса закодовує матрицю H? З цим прийомом ми вже зустрічались при шифрування кольорів вершин графа. Справа в тім, що неможливо зашифрувати безпосередньо нулі та одиниці (з допомогою шифру RSA вони взагалі не шифруються). Навіть якщо замінити їх на якісь довільні числа a і b, то ми отримаємо всього два різних шифротексти, і Бобу не складе труднощів зрозуміти, який з них якому числу відповідає. Тобто структура графа не буде прихованою. Тут ми стикаємось з типовою ситуацією, коли потрібно використовувати так званий рандомізований шифр. І такий шифр будується шляхом додавання випадкових чисел в матрицю H перед шифруванням. Закодована матриця $\tilde{H}$ точно так само задає граф (непарність числа означає наявність ребра, парність — його відсутність), але після шифрування $\tilde{H}$ структура графа повністю приховується (ми використовуємо відому властивість шифру RSA — він повністю приховує парність числа).

3) Навіщо Боб задає два питання? Якщо б він задавав тільки питання номер один, яке по сенсу протоколу являється основним , то Аліса, не знаючи в дійсності гамільтонового циклу в графі G, могла б представити Бобу зовсім інший граф з такою ж кількістю вершин і штучно закладеним в нього гамільтоновим циклом. Тому Боб іноді просить Алісу довести ізоморфізм графів H і G. Важливо, що Аліса не знає наперед, яке з двох питань задасть Боб.

4) Чому Боб не може задати одразу два питання? В цьому випадку він дізнався б гамільтонів цикл в G, так як йому був би показаний гамільтонів цикл в H і правило переходу від H до G.

5) Навіщо Боб перевіряє правильність розшифрування? Якщо б він цього не робив, то Аліса на четвертому кроці могла б представити йому "вигідну" для себе інформацію, а не ту, яку вона посилала йому на другому кроці.

Більш точно основні деталі протоколу обгрунтовуються в ході доведення двох основних тверджень.

Твердження 3.2. Ймовірність обману при t реалізаціях протокола не перевищує 2^{-t}.

Доведення. Спочатку покажем, що ймовірність обману в одній реалізації протоколу рівна 1/2. Зазначимо, що якщо Аліса справді знає гамільтонів цикл в графі G, то вона може правильно відповісти на будь-яке питання Боба. Якщо ж вона не знає гамільтонів цикл, то найбільше , що вона може зробити, - це підготовитись на перше або друге питання. В очікуванні першого питання, вона створює новий граф із штучно заложеним в нього гамільтоновим циклом. Але в цьому випадку вона не зможе довести його ізоморфізм графа G. В очікуванні другого питання, вона будує граф, ізоморфний графу G. Але в цьому випадку вонане зможе показати в ньому гамільтонів цикл. Таким чином, ймовірність успішності обману рівна ймовірності вгадування номера питання. Припустим, що Боб задає обидва питання з однаковими ймовірностями, ми отримуємо, що ймовірність обману рівна 1/2.

Так як Боб зупиняє гру при першій неправильній відповіді, ймовірність обману при t реалізаціях протокола не перевершує $(1/2)^t$.

Твердження 3.3. Представлений протокол реалізує доведення з нульовим знанням.

Доведення. Щоб довести, що Боб не отримує ніяких знань в ході реалізації протоколу, достатньо показати, що все, що він отримує від Аліси, він міг би отримати сам, не вступаючи з нею в жодне спілкування.

Розглянемо спочатку друге питання Боба. У відповідь на це запитання він отримує граф, ізоморфний до графа G. Але він сам міг будувати скільки завгодно ізоморфних графів, і те, що присилає йому Аліса, це просто один з них.

Випадок з першим питанням не настільки очевидний. У відповідь на перше питання Боб отримує гамільтонів цикл в графі, ізоморфному графу G. На перший погляд може здатися, що це дає Бобу якусь інформацію. Однак це не так. Зауважимо, що якщо в G є гамільтонів цикл, то при деякій нумерації вершин існує ізоморфний граф, який задається матрицею суміжності вигляду

$$\begin{pmatrix} * & 1 & * & \dots & * & * & * \\ * & * & 1 & \dots & * & * & * \\ & & & \dots & & & \\ * & * & * & \dots & * & 1 & * \\ * & * & * & \dots & * & * & 1 \\ 1 & * & * & \dots & * & * & * \end{pmatrix} \tag{18}$$

де $*$ означає невизначеність в наявності чи відсутності ребра. Тобто при такій нумерації гамільтонів цикл проходить через вершини в порядку зростання номерів. Змінюючи нумерацію вершин, Боб може отримати з (1) всеможливі ізоморфні матриці. Коли Аліса, відповідаючи на його перше питання, відкриває гамільтонів цикл, Боб бачить якраз одну з таких матриць.

Таким чином, Боб не отримує від Аліси ніякої інформації, яку він не міг би отримати сам.

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.