

Методи обчислення композиції точок еліптичної кривої без використання інверсії

Терновий Володимир

Львівський національний університет ім. І.Франка

Постановка задачі

- Розглянути типи, завдання, функції, вимоги до безпеки криптографічних протоколів
- Дослідити криптографічні протоколи, що базуються на доведенні з нульовим знанням.
- Програмно реалізувати приклад протоколу доведення з нульовим знанням для задачі відшукування гамільтонового циклу в графі.

Еліптичні криві

Кубічна крива у формі Веєрштрасса:

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

Для прикладу на рис. 1.1 наведені кубічні криві

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

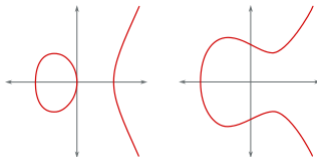


Рис. 1.1. Еліптичні криві.

Кубічні криві, які не мають особливих точок називають еліптичними кривими.

Груповий закон в афінних координатах

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

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

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

- точка на нескінченності O_E є одиничним елементом до операції додавання « $+$ »;
- усі точки $R = (x, y)$ є такими, що $R \neq O_E$;

Груповий закон в афінних координатах

- якщо $R_1 = (x_1, y_1)$ і $R_2 = (x_2, y_2)$ $R_1 \neq \pm R_2$ 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:

$$\begin{aligned}x_3 &= r^2 - x_1 - x_2; \\y_3 &= r(x_1 - x_3) - y_1, \\r &= (y_2 - y_1)/(x_2 - x_1); \end{aligned} \tag{3}$$

- 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:

$$\begin{aligned}x_3 &= r^2 - 2x; \\y_3 &= r(x - x_3) - y, \\r &= (3x^2 + a)/(2y); \end{aligned} \tag{4}$$

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

Геометрична інтерпретація складання двох точок

Геометрична інтерпретація складання двох точок з координатами (x_1, y_1) та (x_2, y_2) на еліптичній кривій;

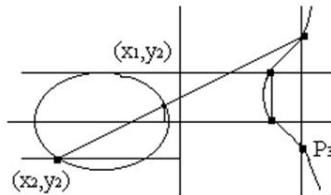


Рис. 2.1. Додавання точок еліптичної кривої.

Груповий закон у проєктивних координатах

Проективний аналог короткого афінного рівняння Веєрштрасса:

$$Y^2Z = X^3 + aXZ^2 + bZ^3, \quad a, b \in F(Q). \quad (5)$$

Еліптична крива, що задається в проєктивних координатах, складається з усіх точок $R = (X, Y, Z)$ рівняння (5) так, що трійка (X, Y, Z) є розв'язком рівняння.

Груповий закон у проєктивних координатах

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 $Z \neq O_F$ є розв'язком (5), то $Q = (X/Z, Y/Z)$ є відповідною точкою в афінних координатах кривої E .
- 3 Існує тільки один розв'язок (5) із $Z = 0$, а саме: точка $(0_F, 1_F, 0_F)$, яка відповідає O_E .

Еліптична криптографія

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 $k \cdot m \cdot G$.

Вимоги до еліптичних кривих

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.

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 $G = (x_G, y_G)$.

Генерація ключів ЕЦП

- 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.

Формування цифрового підпису

- 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 $r = x_1 \bmod p$. Перевірити, 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 то 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.

Перевірка цифрового підпису

- 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 $r' = r$.

Результати виконання програми

Вхідні дані:

$p = 6277101735386680763835789423207666416083908700390324961279;$

$a = -3;$

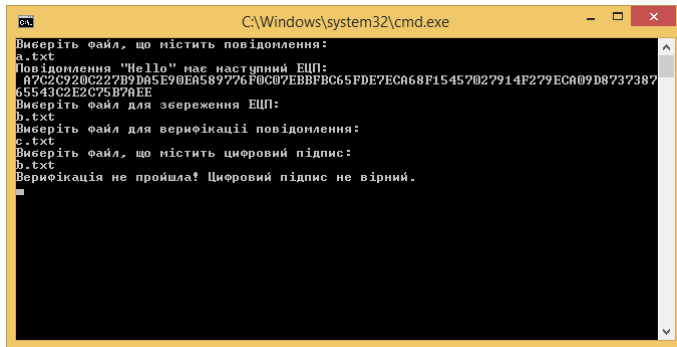
$b = 64210519e59c80e70fa7e9ab72243049feb8deecc146b9b1;$

$xG = 03188da80eb03090f67cbf20eb43a18800f4ff0afd82ff1012;$

$n = \text{ffffffffffffffffffffffff99def836146bc9b1b4d22831}.$

```
C:\Windows\system32\cmd.exe
Виберіть файл, що містить повідомлення:
a.txt
Повідомлення "Hello" має наступний ЕЦП:
C3E127F8F237EB18D9F0A8C3EE907A00629CCED595E841CD470AD2439D78E25D6A6F7A7CB39EE94
A4926A863DBA4BC19
Виберіть файл для збереження ЕЦП:
b.txt
Виберіть файл для верифікації повідомлення:
a.txt
Виберіть файл, що містить цифровий підпис:
b.txt
Верифікація пройшла успішно. Цифровий підпис вірний.
```

Результати виконання програми



```
C:\Windows\system32\cmd.exe

Виберіть файл, що містить повідомлення:
a.txt
Повідомлення "Hello" має наступний ЕЦП:
A7C2C920C227B9DA5E90EA589776F0C07EBBFBC65FDE7ECA68F15457027914F279ECA09D8737387
65543C2E2C75B70EE
Виберіть файл для збереження ЕЦП:
b.txt
Виберіть файл для верифікації повідомлення:
c.txt
Виберіть файл, що містить цифровий підпис:
b.txt
Верифікація не пройшла! Цифровий підпис не вірний.
```

Рис. 6.2. Приклад невдалого виконання програми.

Висновки

- Розглянуто криптографічні протоколи, що базуються на доведенні з нульовим знанням, які є основою реалізації методів захисту інформації.
- Наведені результати програмної реалізації узгоджуються з доведеними теоретичними твердженнями.
- Актуальність криптографії росте з кожним роком, і реалізовує методи шифрування/дешифрування, електронного цифрового підпису, ідентифікації / аутентифікації які є невід'ємною частиною інформаційних технологій.



Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія:Теорія.Практика. Застосування: Монографія. Вид.2-ге, перероб.ідоп. — Харків: Видавництво «Форт», 2012. — 880с.



Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях, — М.:Кудиц-Образ, 2001 г. — 368с.



Рябко Б.Я., Фионов А.Н. Основы современной криптографии и стеганографии, - М.: Научный мир, 2004 г. - 173с.



О.В.Вербіцький Вступ до криптології, - Львів: Видавництво наукової технічної літератури, 1998. - 247 с.



Шнайер Брюс, Фергюсон Нильс Практическая криптография, 2-е изд. - М: ООО "И.Д.Вильямс 2005. — 424 с.

Дякую за увагу!