Криптопреобразования в группах точек эллиптических кривых

Лекция

Ревизия: 0.1

Последняя модификация: Vlad Kovtun

Дата последней модификации: 31.01.2011 21:26:00

История изменений

29.03.2009 – Версия 0.1. Первичный документ. Владислав Ковтун

Содержание

Лекция 5. Криптопреобразования в группах точек эллиптических кривых. Часть 3

Вопросы

1. Аффинные и проективные базисы.
2. Примеры преобразований.
3. Сравнение преобразований в полях, кольцах, группе ЭК.

Аффинный и проективный базисы

Известно 2 представления групп точек ЭК, 2 базиса:

- Аффинный.
- Проективный.

Аффинный базис

Далее рассмотрим более специфичные представления эллиптической кривой над различными полями:

- Поле нечетной характеристики:
    - Представление Дочи-Икарт-Кохеля (Doche-Icart-Kohel)

$$E_{(a)}: y^2 = x^3 + ax^2 + 16ax,\ a \in k,\ a(a-64) \neq 0. \tag{3}$$

Нейтральным элементом, в этом случае, является точка O на ∞ в проективных координатах $(0:1:0)$. Впервые представлено Дочи, Икартом и Кохелем и развито в работе Бернштейна и Ланге.

    - Представление Дочи-Икарт-Кохеля (Doche-Icart-Kohel) ориентированное на утроение точек:

$$E_{(a)}: y^2 = x^3 + 3x^2 + 3a(x+1)^2,\ a \in k,\ a \neq 0,\ a \neq \tfrac{9}{4}. \tag{4}$$

Нейтральным элементом, в этом случае, является точка O на ∞ в проективных координатах $(0:1:0)$. Впервые представлено Дочи, Икартом и Кохелем и развито в работе Бернштейна и Ланге.

    - Представление Эдвардса (Edwards):

$$E_{(c,d)}: x^2 + y^2 = c^2(1 + dx^2y^2),\ c, d \in k, d = 1. \tag{5}$$

Технически, кривая Эдвардса не является эллиптической, т.к. является сингулярной. Нейтральным элементом, в этом случае, является точка O на ∞ в координатах $(0, c)$. Отметим, что точка $(0, -c)$ обладает порядком 2, в то время как точки $(c, 0)$ и $(-c, 0)$ обладают порядком 4. Впервые представлено в работе Брайера и Джоя.

    - Представление Хассе (Hasse) - кубическая кривая в аффинных координатах:

$$E_{(d)}: x^3 + y^3 + 1 = 3dxy,\ d \in k. \tag{6}$$

или в стандартных проективных координатах $(x, y) \mapsto (X/Z,\ Y/Z)$:

$$E_{(d)} : X^3 + Y^3 + Z^3 = 3dXYZ,\ d \in k,\ d^3 \neq 1. \quad (7)$$

Нейтральным элементом, в этом случае, является точка O на ∞ в проективных координатах $(1:-1:0)$. Над полем с нетривиальным кубическим корем w из 1, существует две дургие точки на бесконечности $(1:-w:0)$ и $(1:-w^2:0)$. Впервые представление Хассе было описано в работе Брайера и Джоя, как и указывалось ранее, после чего было обращено внимание в работе Смарта в 2001 году, после чего дальнейшее развитие произошло в работе Хисила, Вонга и Картера в 2007 году.

- Представление скрещивание Якоби (Jacobi intersection)

$$E_{(a)} : s^2 + c^2 = 1,\ as^2 + d^2 = 1,\ a \in k, a \neq 0 \text{ и } a \neq 1. \quad (8)$$

Нейтральным элементом, в этом случае, является точка O на ∞ в проективных координатах $(0:1:1)$. Было инициировано в работе Давида и Григория Чудновских в 1986 году, после чего Лардет и Смарт обратили внимание в 2001 году, на такое представление кривой.

- Представление в форме уравнения Якоби 4-ой степени (Jacobi quartics) ориентированное на удвоение:

$$E_{(a)} : y^2 = x^4 + 2ax^2 + 1,\ a \in k,\ \mathrm{char}(k) \neq 2, 3,\ a^2 \neq 1. \quad (9)$$

Также может быть представлено в следующем частном виде:

$$E_{(a)} : y^2 = (1 - x^2)(1 - a^2x^2),\ a \in k,\ a^2 \neq 1. \quad (10)$$

Нейтральным элементом, в этом случае, является точка O на ∞ с координатами $(0, 1)$. Предложено в работе Дэвида и Григория Чудновских в 1986 году, после чего было развито Биллетом и Джоем в 2003 году.

- Представление Монтгомери (Montgomery):

$$E_{(a,b)} : by^2 = x^3 + ax^2 + x,\ a, b \in k. \quad (11)$$

Нейтральным элементом, в этом случае, является точка O на ∞ в координатах $(0, 1)$. Предложено Питером Монтгомери в 1987 году.

- Представление Вейерштрасса (Weierstrass):

$$E_{(a,b)} : y^2 = x^3 + ax^2 + b,\ a, b \in k,\ b \neq 0 \text{ и } a^3 + 27b^3 \neq 0. \quad (12)$$

Нейтральным элементом, в этом случае, является точка O на ∞ в проективных координатах $(0:1:0)$.

- Поле четной характеристики:
  - Двоичное представление Эдвардса (Edwards):

$$E_{(d_1,d_2)} : d_1(x + y) + d_2(x^2 + y^2) = (x + x^2)(y + y^2),\ d_1, d_2 \in k. \quad (13)$$

Нейтральным элементом, в этом случае, является точка O на ∞ в проективных координатах $(0:1:0)$. Харольдом Эдвардсом была предложена 2007 году.

- Представление W, такое, что паре (x, y) соответствует $W = x + y$.
- Представление Вейерштрасса (Weierstrass):

$$E_{(a,b)}: y^2 + xy = x^3 + ax^2 + b,\ a, b \in k. \tag{14}$$

Нейтральным элементом, в этом случае, является точка O на ∞ в проективных координатах $(0, 0)$ для случая $b \neq 0$, в противном случае $(0, 1)$.

Проективный базис

Ни для кого не является секретом, что операция мультипликативного инвертирования является вычислительно сложной, по сравнению с другими операциями: сложение, возведение в квадрат, умножение. В связи с этим, было предложено уйти от выполнения операции мультипликативного инвертирования в промежуточных вычислениях, посредством перехода к проективному представлению (однородным координатам).

Проективное представление может быть получено посредством замены аффинных координат на однородные [7].

На сегодняшний день известно несколько проективных представлений, в зависимости базового поля и формы кривой:

- Поле нечетной характеристики.
  - Уравнение кривой в форме Вейерштрасса. Следует рассмотреть несколько вариантов кривой, когда a в общем виде и $a = -3$.
    - Стандартное проективное представление $[X:Y:Z]$: $(x, y) \mapsto (X/Z,\ Y/Z)$.
    - Проективное представление Якоби $[X:Y:Z]$: $(x, y) \mapsto (X/Z^2, Y/Z^3)$.
    - Модифицированное представление Якоби $[X:Y:Z^2:Z^3]$: $(x, y) \mapsto (X/Z^2, Y/Z^3)$.
    - Обобщенное модифицированное представление Якоби $[X:Y:Z^2:Z^3]$: $(x, y) \mapsto (X/Z^2, Y/Z^3)$.
  - Уравнение кривой в форме Якоби 4-ой степени. Следует рассмотреть вариантов кривой, когда $a^2 + c^2 = 1$ и в общем случае.
    - Расширенное проективное представление $[X:X^2:Y:Z:Z^2]$: $(x, y) \mapsto (X/Z, Y/Z)$.
    - Представление Лопеса-Дахаба $[X:Y:Z]$: $(x, y) \mapsto (X/Z, Y/Z^2)$.
    - Расширенное представление Лопеса-Дахаба $[X:X^2:Y:Z:Z^2]$: $(x, y) \mapsto (X/Z, Y/Z^2)$.
    - Модифицированное расширенное представление Лопеса-Дахаба $[X:X^2:Y:Z:Z^2:R]$, $R = 2XZ$: $(x, y) \mapsto (X/Z, Y/Z^2)$.
  - Уравнение кривой в форме скрещивания Якоби.
    - Стандартное представление $[S:C:D:Z]$: $(s, c, d) \mapsto (S/Z, C/Z, D/Z)$.

        - Расширенное стандартное проективное представление $[S:C:D:Z:SC:DZ]$, $SC=SC$ и $DZ=DZ$: $(s,c,d)\mapsto(S/Z,C/Z,D/Z)$.
    - Кривая в форме Монтгомери.
        - Стандартное проективное представление $[X:Z]$: $(x,y)\mapsto(X/Z,Y/Z)$.
    - Уравнение кривой в форме Дочи-Икарт-Кохеля (ориентированное на удвоение).
        - Представление Лопеса-Дахаба $[X:Y:Z:Z^2]$: $(x,y)\mapsto(X/Z,Y/Z^2)$.
    - Уравнение кривой в форме Дочи-Икарт-Кохеля (ориентированное на утроение).
        - Модифицированное проективное представление Якоби $[X:Y:Z:Z^2]$: $(x,y)\mapsto(X/Z^2,Y/Z^3)$
    - Уравнение кривой в форме Хассе.
        - Стандартное проективное представление $[X:Y:Z]$: $(x,y)\mapsto(X/Z,Y/Z)$.
        - Расширенное стандартное проективное представление $[X:Y:Z:X^2:Y^2:Z^2:XY:XZ:YZ]$, $XY=2XY$, $XZ=2XZ$ и $YZ=2YZ$: $(x,y)\mapsto(X/Z,Y/Z)$
    - Уравнение кривой в форме Эдвардса.
        - Стандартное проективное представление $[X:Y:Z]$: $(x,y)\mapsto(X/Z,Y/Z)$.
        - Инвертированное проективное представление $[X:Y:Z]$: $(x,y)\mapsto(Z/X,Z/Y)$.
- Поле четной характеристики.
    - Уравнение кривой в форме Вейерштрасса. Рассматриваются кривые для которых $a=1$, $a=0$ и в общем виде.
        - Стандартное проективное представление $[X:Y:Z]$: $(x,y)\mapsto(X/Z,Y/Z)$.
        - Проективное представление Якоби $[X:Y:Z]$: $(x,y)\mapsto(X/Z^2,Y/Z^3)$.
        - Проективное представление Лопеса-Дахаба $[X:Y:Z]$: $(x,y)\mapsto(X/Z,Y/Z^2)$.
        - Расширенное проективное представление Лопеса-Дахаба $[X:Y:Z:Z^2]$: $(x,y)\mapsto(X/Z,Y/Z^2)$.
    - Уравнение кривой в форме Эдвардса. Рассматриваются кривые в общем виде, так и частные случаи, когда $d_1=d_2$.
        - Проективное WZ представление (x,y) соответствует $x+y=W/Z$.
        - Стандартное проективное представление $[X:Y:Z]$: $(x,y)\mapsto[X/Z,Y/Z]$.

Более детальную информацию об арифметических операциях на ЭК над различными полями в различных базисах, можно почерпнуть из публикаций [5, 6]

Рассмотрим вывод уравнения ЭК в форме Вейерштрасса для проективного представления Якоби. Переход от аффинного представления к проективному, осуществляется посредством замены:

$$x = \frac{X}{Z^2},\ y = \frac{Y}{Z^3}. \tag{15}$$

Произведем подстановку (15) в уравнение ЭК в аффинном виде и получаем:

$$Y^2 + XYZ = X^3 + aX^2Z^2 + bZ^6. \tag{16}$$

Арифметические преобразования в проективном представлении Якоби могут быть получены посредством постановки.

Аналогии

Проведем аналогию между групповыми операциями в полях, кольцах и ЭК, в таблице 3.

Таблица 1. Аналогия между групповыми операциями в полях, кольцах и ЭК

Название операции в поле	Название операции на ЭК
Умножение элементов поля $\mathbf{GF}(p)$, с последующим приведением по модулю p: $c = a \cdot b \bmod p$	Сложение точек ЭК E: $P_3 = P_1 + P_2$
Возведение в квадрат элементов поля $\mathbf{GF}(p)$ с последующим приведением по модулю p: $c = a \cdot a \bmod p = a^2 \bmod p$	Удвоение точек ЭК E: $P_3 = P_1 + P_1 = 2P_1$
Возведение в степень (мультипликативное экспоненцирование) элемента поля $\mathbf{GF}(p)$, с последующим приведением по модулю p после каждого умножения: $c = a^k \bmod p$. Следует обратить внимание, что при возведении в степень, используются операции умножения и возведения в квадрат.	Скалярное умножение точки ЭК E: $P_3 = kP = \underbrace{P + P + \cdots + P}_{k}$, где k - число, которое меньше порядка группы, которая образована точкой P. Следует обратить внимание, что при скалярном умножении точек, используются операции сложения и удвоения точек.

Литература

1. Криптографическая защита информации в АСУ СН. Курс лекций. В.И. Долгов. ХВУ. 1998.

2. Криптографическая защита информации в информационных системах. Курс лекций. И.Д. Горбенко. ХНУРЭ. 2002.

3. Криптопреобразования с открытым ключом. Текущее состояние. Обзор. В.Ю. Ковтун. 2006.

4. Теорема Виета для представления коэффициентов многочлена через его корни. http://ru.wikipedia.org/wiki/Формулы_виета

5. Ковтун В.Ю. Криптография с открытым ключом. http://www.nrjetix.com/fileadmin/doc/publications/additional_info/public_key_cryptography_-_lecture.pdf

6. Таня Ланге. База арифметических операций в группе точек ЭК. http://www.hyperelliptic.org/EFD/

7. http://ru.wikipedia.org/wiki/Однородные_координаты