Криптосистеми на еліптичних кривих

Lecture 9: Pairings

Грубіян Євген Олександрович

Функції від дівізора

Функція $f \in \overline{K}(E)$ від дівізора $D = \sum_{P \in E} n_P (P) \in \mathrm{Div}(E)$

Визначена як

$$f(D) = \prod_{P \in E} f(P)^{n_P} \in \overline{K}$$

За умови якщо $\mathrm{supp}(D) \cap \mathrm{supp}((f)) = \emptyset$

Зазначимо що умова того що носії дівізорів (f) та D не перетинаються є важливою, оскільки якщо наприклад $\exists P_0 \in \mathrm{supp}((f)) \cap \mathrm{supp}(D)$ то $f(D) = 0$ або $f(D) = \infty$ в залежності від коефіцієнту біля P_0 в (f)

Закон взаємності Вейля

Якщо для ненульових $f, g \in \overline{K}(E) : \mathrm{supp}((f)) \cap \mathrm{supp}((g)) = \emptyset$ то

$$f((g)) = g((f))$$

Цей закон використовується при доведенні властивостей білінійності спарювання.

Означення спарювання Вейля

Спарювання Вейля на кривій E/F_q

Нехай для деякого $k \geq 1$, точок $P, Q \in E(F_{q^k})[r]$, дівізорів $D_P \sim (P) - (\mathcal{O}), D_Q \sim (Q) - (\mathcal{O}) : \mathrm{supp}(D_P) \cap \mathrm{supp}(D_Q) = \emptyset$ та функцій $f, g \in \overline{F_q}(E)$ таких що $(f) = rD_P, (g) = rD_Q$ то відображення

$$w_r : E(F_{q^k})[r] \times E(F_{q^k})[r] \to F^*_{q^k}$$

що визначене як

$$w_r(P, Q) = \frac{f(D_Q)}{g(D_P)}$$

називається спарюванням Вейля точок P, Q.

Це відображення є зокрема білінійним та невиродженим.
Найбільш цікавий з прикладної точки зору випадок коли k - степінь вкладення кривої E/F_q, r - просте число, порядок циклічної підгрупи F_q-раціональних точок $r | \# E(F_q)$. Тоді $w_r : E[r] \times E[r] \to \mu_r \subset F^*_{q^k}$
І як це обчислити ?

Функції Вейля

Ключовим будівельним блоком для обчислення спарювання Вейля є функції Вейля.

Функція Вейля $f_{m,P}$

Така раціональна функція, що $(f_{m,P}) = m(P) - ([m]P) - (m-1)(\mathcal{O}) \in \mathrm{Prin}(E)$

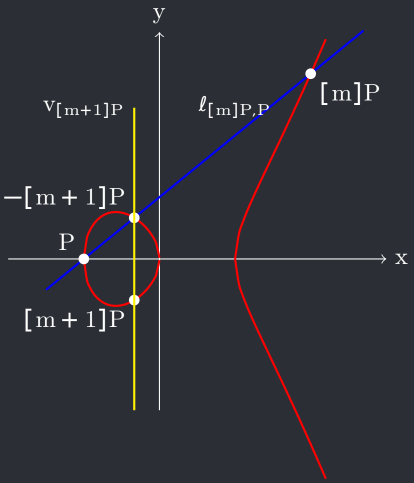
Властивості функцій Вейля:

- $(f_{0,P}) = 0$
- $\forall P \in E[r] : (f_{r,P}) = r(P) - r(\mathcal{O})$
- Нехай $\ell_{[m]P,P}$ - пряма, що проходить через точки $[m]P, P$, $v_{[m+1]P}$ - вертикаль що проходить через $[m+1]P$, тоді:

$$(f_{m+1,P})-(f_{m,P}) = (P)+([m]P)-([m+1]P)-(\mathcal{O}) = (\ell_{[m]P,P}/v_{[m+1]P})$$

Таким чином $f_{m+1,P} = f_{m,P} \frac{\ell_{[m]P,P}}{v_{[m+1]P}}$ що дозволяє ітеративно обчислювати функції Вейля

Функції Вейля



Спарювання Вейля

Можна припустити що функції Вейля корисні для визначення спарювання, оскільки функція Вейля з дівізором $(f_{r,P}) = r(P) - r(\mathcal{O})$ підходить під опис функції f з визначення і ми можемо визначити спарювання Вейля як $w_r(P,Q) = \frac{f_{r,P}(D_Q)}{f_{r,Q}(D_P)}$, де
$D_P = (P) - (\mathcal{O}), D_Q = (Q) - (\mathcal{O})$, проте $supp(D_P) \cap supp(D_Q) = \{\mathcal{O}\}$, таким чином отримали протиріччя із визначенням.
На щастя, це досить легко обійти, взявши деяку точку
$R \notin \{\mathcal{O}, Q, -P, Q-P\}$ можна показати що

$$w_r(P,Q) = \frac{f_{r,Q}(R) f_{r,P}(Q-R)}{f_{r,P}(-R) f_{r,Q}(P+R)}$$

Дійсно, якщо задамо $D_P = (P+R) - (R) \sim (P) - (\mathcal{O}), D_Q = (Q) - (\mathcal{O}) \implies supp(D_P) \cap supp(D_Q) = \emptyset$, $f = f_{r,P} \circ \tau, g = f_{r,Q}$, де
$\tau : P \to P - R$ отримаємо наш вираз для w_r
Також справедливий граничний випадок $R \to \mathcal{O}$:

$$w_r(P,Q) = (-1)^r \frac{f_{r,P}(Q)}{f_{r,Q}(P)}$$

Алгоритм Міллера

Зауважимо що наведений раніше ітеративний спосіб обчислення функцій Вейля не є ефективним, оскільки має лінійну відносно r складність(на практиці r велике просте). Але можна зауважити що значення функції $f_{2m,P}$ можна обчислити досить легко маючи $f_{m,P}$. Дійсно:

$$(f^2_{m,P}) = 2m(P) - 2([m]P) - 2(m-1)(\mathcal{O})$$

$$(f_{2m,P}) = 2m(P) - ([2m]P) - (2m-1)(\mathcal{O})$$

$$(f_{2m,P}) - (f^2_{m,P}) = 2([m]P) - ([2m]P) - (\mathcal{O}) = \left(\frac{\ell_{[m]P,[m]P}}{v_{[2m]P}}\right)$$

$$f_{2m,P} = f^2_{m,P} \cdot \frac{\ell_{[m]P,[m]P}}{v_{[2m]P}}$$

Тут $\ell_{[m]P,[m]P}$ - функція дотичної до E в точці $[m]P$, а $v_{[2m]P}$ - вертикаль через точку $[2m]P$ (Перевірте самостійно). Таким чином ми маємо всі будівельні блоки для алгоритму в стилі експоненціювання (DoubleAndAdd) !

Алгоритм Міллера (для дівізора)

Вхід: Точка $P \in E[r]$, дівізор $D_Q \sim (Q) - (\mathcal{O})$, $Q \notin \{P, \mathcal{O}\}$, бінарний розклад $r = \sum_{i=0}^{n-1} 2^i r_i$

Вихід: Значення $f_{r,P}(D_Q)$

Алгоритм:

$f \leftarrow 1$

$R \leftarrow P$

for $i = n-2..0$ do

    $R \leftarrow 2R$

    $f \leftarrow f^2 \cdot \frac{\ell_{R,R}}{v_{[2]R}}(D_Q)$ ▷ Виражаємо $f_{2m,P}$ через $f_{m,P}$

    if $r_i = 1$ then

        $R \leftarrow R + P$

        $f \leftarrow f \cdot \frac{\ell_{R,P}}{v_{R+P}}(D_Q)$ ▷ Виражаємо $f_{m+1,P}$ через $f_{m,P}$

    end if

end for

return f

Алгоритм Міллера (для точки)

Зазначимо що оскільки $D_Q \sim (Q) - (\mathcal{O})$ можна представити як $D_Q = (Q + T) - (T)$ для деякої точки $T \notin \{-Q, P, \mathcal{O}\}$ то $f_{r,P}(D_Q) = \frac{f_{r,P}(Q+T)}{f_{r,P}(T)}$

Вхід: Точки $P, Q \in E[r], Q \notin \{P, \mathcal{O}\}$, бінарний розклад $r = \sum_{i=0}^{n-1} 2^i r_i$

Алгоритм:

Обираємо деяку точку $T \notin \{-Q, P, \mathcal{O}\}$
$f \leftarrow 1$
$R \leftarrow P$
for $i = n - 2..0$ do
    $R \leftarrow 2R$
    $f \leftarrow f^2 \cdot \frac{\ell_{R,R}(Q+T)v_{[2]R}(T)}{v_{[2]R}(Q+T)\ell_{R,R}(T)}$ ▷ Виражаємо $f_{2m,P}$ через $f_{m,P}$
    if $r_i = 1$ then
        $R \leftarrow R + P$
        $f \leftarrow f \cdot \frac{\ell_{R,P}(Q+T)v_{R+P}(T)}{v_{R+P}(Q+T)\ell_{R,P}(T)}$ ▷ Виражаємо $f_{m+1,P}$ через $f_{m,P}$
    end if
end for
return f

Властивості спарювання Вейля

Наведемо властивості спарювання Вейля $w_r : E[r] \times E[r] \to \mu_r$

1. Білінійність: $\forall P, P', Q, Q' \in E[r]$:

$$w_r(P + P', Q) = w_r(P, Q)\, w_r(P', Q),$$

$$w_r(P, Q + Q') = w_r(P, Q)\, w_r(P, Q'),$$

2. Невиродженість: Якщо $P \neq \mathcal{O}$, то існує $Q \in E[r]$ таке, що

$$w_r(P, Q) \neq 1.$$

3. Взаємність

$$w_r(P, Q) = w_r(Q, P)^{-1}$$

4. Наслідок із попереднього:

$$\forall P \in E[r] : w_r(P, P) = 1$$

Спарювання Тейта

На практиці використовують більш «дешевий» варіант білінійного спарювання: спарювання Тейта, яке щоправда визначається в асиметричній манері:

Спарювання Тейта

Нехай $P \in E(\mathbb{F}_{q^k})[r], Q \in E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k})$ - це деяка точка-представник класу еквіваленності із фактор групи $E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k})$, $f \in \overline{\mathbb{F}_q}(E) : (f) = (P) - (\mathcal{O})$, $D_Q \sim (Q) - (\mathcal{O}), \operatorname{supp}(D_Q) \cap \operatorname{supp}((f)) = \emptyset$, тоді відображення(скорочене спарювання Тейта)

$$t_w : E(\mathbb{F}_{q^k})[r] \times E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k}) \to \mu_r \subset \mathbb{F}_{q^k}^*$$

Визначене як

$$t_w(P, Q) = f(D_Q)^{(q^k-1)/r}$$

Є білінійним та невиродженим