Криптосистеми на еліптичних кривих

Lecture 10: Pairings Cryptography

Грубіян Євген Олександрович

Степінь вкладення

Нам відомо що структура групи кручення: $E[n] \cong Z_n \times Z_n$ якщо $q \nmid n$.
Тобто $\#E[n] = n^2$
Нагадаємо що степінь вкладення ЕК E/F_q, $E(F_q) = r$ в поле F_q - таке мінімальне значення k що $r | q^k - 1$.
Нехай спарювання Вейля визначене $e : E[r] \times E[r] \to F^*_{q^k}$.

Теорема

Якщо k - степінь вкладення E/F_q то $E[r] \subseteq E(F_{q^k})$.

На практиці нам потрібні не тільки ефективно обчислювати значення спарювання, але й ефективно гешувати в елементи групи (обирати випадкові точки наприклад) та відображати елементи між групами. До того ж порядок груп має бути простим. Тому більш специфічно можна визначити спарювання як:

$$e : \mathbb{G}_1 \times \mathbb{G}_2 \to F^*_{q^k}$$

Де $\mathbb{G}_1, \mathbb{G}_2$ деякі підгрупи $E[r]$.

Структура групи: приклад

Теорема

$$\#E(F_{q^k}) = q^k + 1 - \alpha^k - \beta^k$$

Де α, β - корені характеристичного рівняння $x^2 - tx + q$ в F_{q^k} (t - слід ендоморфізму Фробеніуса)

Візьмемо суперсингулярну криву $E/F_{11} : y^2 = x^3 + 4$, $E(F_{11}) = 12$, $E(F_{11^2}) = 144$. Бачимо що $r \nmid q - 1$, але $r \mid q^2 - 1$. тому степінь вкладення $k = 2$. Таким чином $E[3] \cong Z_3 \times Z_3$ тобто $\#E[3] = 9$ та ми маємо 4 циклічні підгрупи порядку 3:

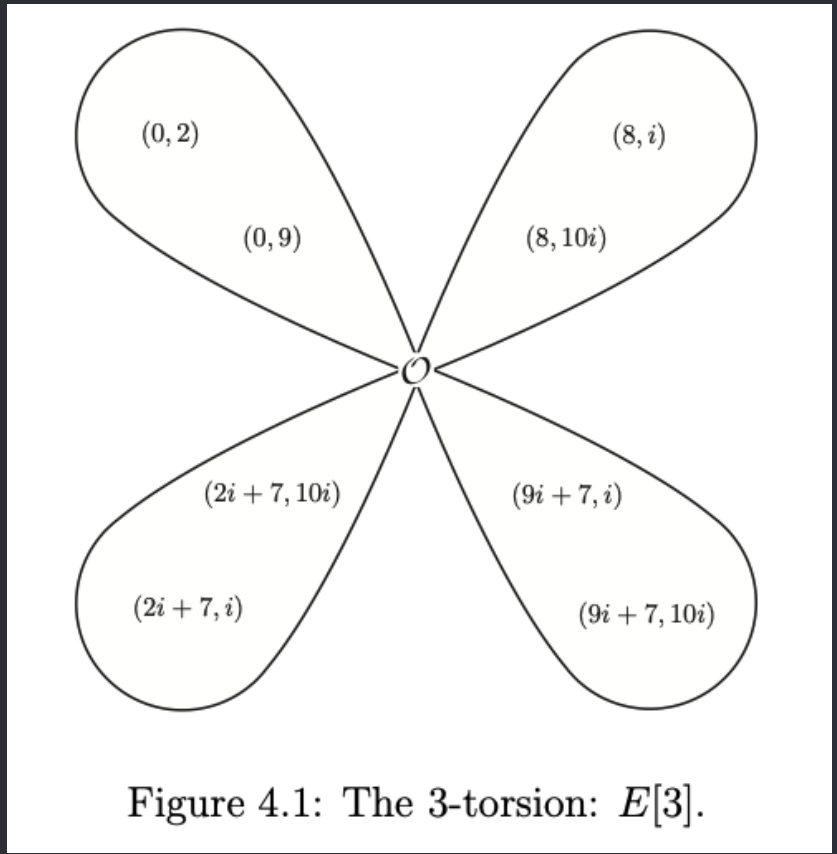


Figure 4.1: The 3-torsion: $E[3]$.

Вибір підгруп для спарювань

Слід точки P

$$Tr(P) = \sum_{i=0}^{k-1} \pi^i(P) = \sum_{i=0}^{k-1} (x^{q^i}, y^{q^i})$$

Де $\pi : \pi((x, y)) = (x^q, y^q)$ - ендоморфізм Фробеніуса.

Підгрупа $\mathscr{G}_1 \subset E[r]$

$$\mathscr{G}_1 = E[r] \cap \ker(\pi - [1]) = \{P \in E[r] | Tr(P) \in \mathscr{G}_1\}$$

Ця група співпадає із $E(F_q)$, оскільки $\forall P \in \mathscr{G}_1 : Tr(P) = [k]P$.

Підгрупа сліду 0: $\mathscr{G}_2 \subset E[r]$

$$\mathscr{G}_2 = E[r] \cap \ker(\pi - [q]) = \{P \in E[r] | Tr(P) = \mathscr{O}_E\}$$

Це єдина підгрупа в $E[r]$, для якої $\forall P \in E[r] : Tr(P) = \mathscr{O}$

Структура підгруп

Анти-слід точки P

$$aTr(P) = [k]P - Tr(P)$$

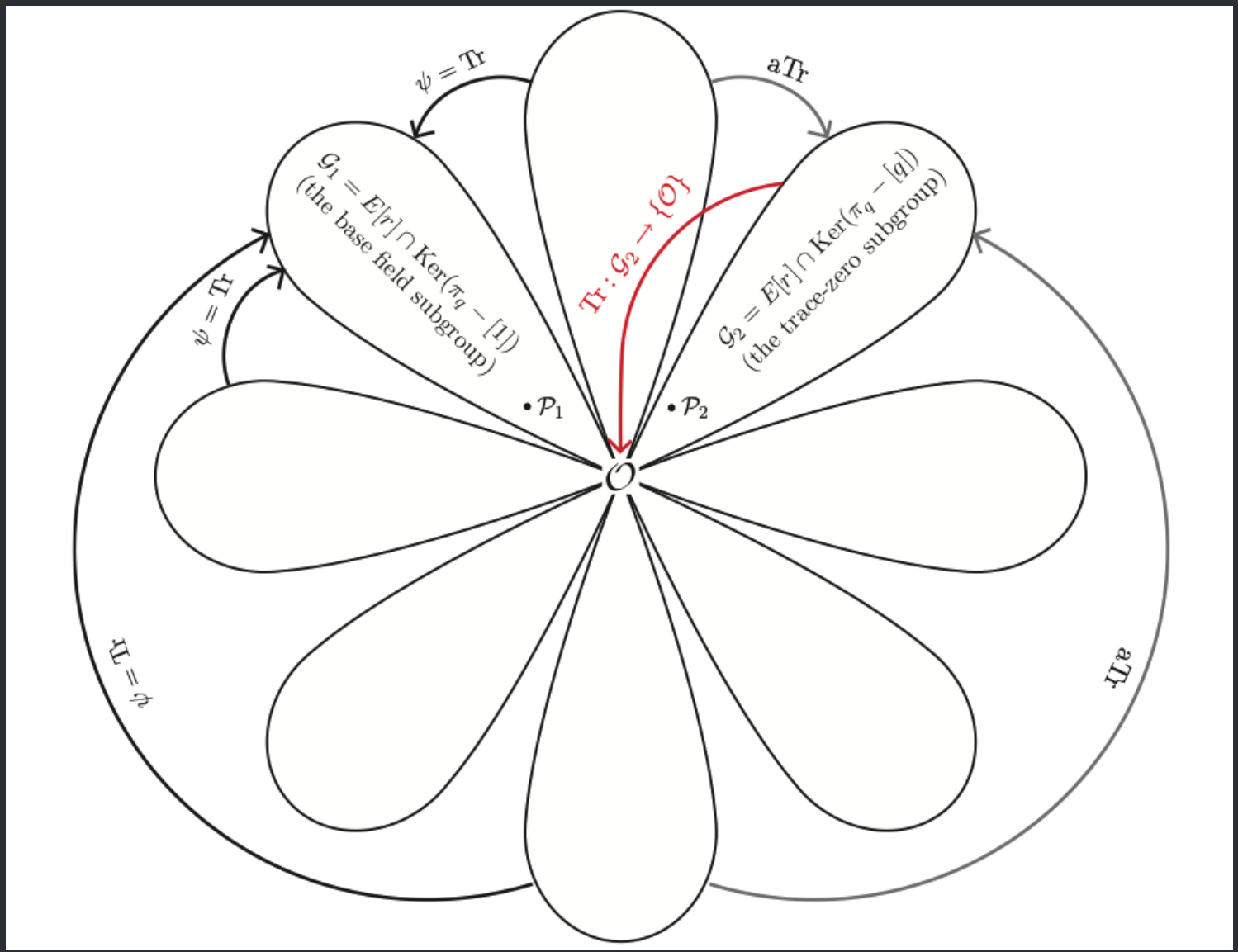
Зауважимо що $\forall P \in E[r] : aTr(P) \in \mathscr{G}_2$

Теорема

Нехай $P_1 \in \mathscr{G}_1, P_2 \in \mathscr{G}_2$, тоді $\forall P \in E[r] \exists i, j \in Z_q^* : P = [i]P_1 + [j]P_2$

Таким чином $\mathscr{G}_1$ та $\mathscr{G}_2$ свого роду утворюють базис групи $E[r]$ як «векторного простору розмірності 2» (група $E[r]$ є модулем над Z_q). Тому якщо в якості $\mathbb{G}_1$ взяти $\mathscr{G}_1$, а $\mathbb{G}_2 = \mathscr{G}_2$ то спарювання Вейля точно буде не виродженим: $\forall P \in \mathscr{G}_1, Q \in \mathscr{G}_2 : e(P, Q) \neq 1$! Зауважимо якщо $\mathbb{G}_1 = \mathbb{G}_2 = \mathscr{G}_1$ то відображення буде виродженим за властивостями спарювання Вейля. Хоч такий вибір параметрів найбільш поширений на практиці (так званий Type 3), але такий підхід має ряд недоліків, зокрема відсутність жодного ефективно-обчислюваного відображення із $\mathscr{G}_2$ в $\mathscr{G}_1$.

Діграма підгруп



Типи спарювань

Відображення розсіювання

Якщо E/F_q - суперсингулярна, тоді існує відображення розсіювання $\psi : E(F_q) \to E(F_{q^k})$. Зокрема якщо $k = 2$ тоді $\psi(x, y) = (-x, iy)$.

На практиці виділяють 4 типи білінійних спарювань на еліптичних кривих. У всіх 4х типах зручно взяти $\mathbb{G}_1 = \mathscr{G}_1$. Таким чином вибір $\mathbb{G}_2$ буде визначати тип.

Type 1: $\mathbb{G}_1 = \mathbb{G}_2 = \mathscr{G}_1$, при чому E/F_q - суперсингулярна, тобто $\#E(F_q) = q + 1$. В такому випадку $e(P, Q) = e_w(P, \psi(Q))$. Основним недоліком цього підходу є ефективність, оскільки суперсингулярні криві мають як правило значно більший розмір поля для забезпечення рівня стійкості.

Type 2: $\mathbb{G}_1 = \mathscr{G}_1$, $\mathbb{G}_2$ - довільна підгрупа що не співпадає із $\mathbb{G}_1$. Осеновний недолік - неможливість ефективно гешувати в елементи $\mathbb{G}_2$, що унеможливлює застосування в ряді протоколів.

Типи спарювань

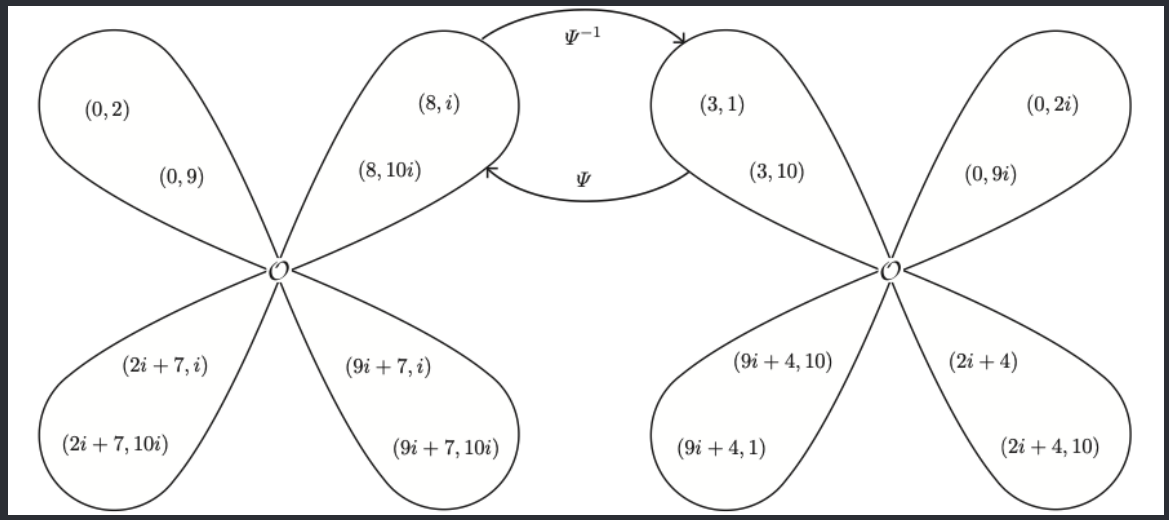


Рис.: E та її квадратичне кручення E′

Type 3: $\mathbb{G}_1 = \mathscr{G}_1, \mathbb{G}_2 = \mathscr{G}_2$. Найбільш поширений та ефективний вид спарювань (зокрема через змогу застосовувати криві кручення для прискорення). Можна ефективно гешувати в елементи $\mathbb{G}_2$ за допомогою aTr. Основний недолік - відсутність ефективних відображень $\mathbb{G}_2 \to \mathbb{G}_1$.

Type 4: $\mathbb{G}_1 = \mathscr{G}_1, \mathbb{G}_2 = \mathrm{E}[\mathrm{r}]$. Гешування в $\mathbb{G}_2$ можливе, але не настільки легке, також ефективність даного типу програє порівняно з третім

Спарювання в криптографії

Зазвичай спарювання застосовують в різноманітних протоколах де задача CDH(Computational Diffie-Hellman) вважається складною. Також додатково вводять припущення безпеки на саме спарювання, до прикладу The fixed argument pairing inversion problem (FAPI-1) - маючи $P \in \mathbb{G}_1, g \in F_{q^k}$ обчислити $Q \in \mathbb{G}_2$ таке що $e(P, Q) = g$.
На практиці дизайн протоколу має передбачати ефективність обчислення e, стійкість до DLP в $E(F_{q^k})$ зокрема із врахуванням MOV-атаки(що майже неодмінно веде до росту розміру підгрупи або степеня вкладення), такі криві називаються pairing-friendly.

Barreto-Naehrig curves

Криві $E/F_p : y^2 = x^3 + b$, де $p = 36x^4 + 36x^3 + 24x^2 + 6x + 1$ - просте для деякого x та відповідно підібраного генератора F_p^* b. Тоді $r = 36x^4 + 36x^3 + 18x^2 + 6x + 1$, а степінь вкладення $k = 12$. Знаменита крива BN254 задається $x = 4965661367192848881, b = 2$.

Спарювання для перевірки квадратичних рівнянь

Зазначимо що перевіряти лінійні співвідношення на точках еліптичної кривої досить легко застосовуючи звичайну арифметику: тобто якщо $x_1 + x_2 = c$ то $[x_1]P + [x_2]P = [c]P$

Ускладнимо задачу: нехай Аліса має переконати Боба що вона знає деякі x_1, x_2 що добуток $x_1 x_2 = c$, але при цьому не розкриваючи значень x_1, x_2 Бобу.

Протокол перевірки квадратичності

1. Аліса обирає $P \in E[r]$, обчислює $[x_1]P, [x_2]P$ та надсилає їх Бобу
2. Боб перевіряє $e([x_1]P, [x_2]P) = e(P, P)^c$

Зауваження: для спрощення наведено спарювання першого типу, але нічого не заважає узагальнити протокол на довільне.

Взагалі кажучи цей протокол можна поширити на довільну арифметичну схему (QAP), тобто довести що ми коректно обчислили значення складного арифметичного виразу без розкриття його входів.

Криптосистема BLS-підпису

Підпис BLS(Boneh–Lynn–Shacham)

Сторони узгоджують параметри: спарювання $e : \mathbb{G}_1 \times \mathbb{G}_{\neq} \to \mathbb{G}_T$, генератори $G_1 \in \mathbb{G}_1, G_2 \in \mathbb{G}_2$, геш функцію $H : \mathscr{M} \to \mathbb{G}_1$

$\mathrm{KeyGen}(1^\lambda) \to (\mathrm{sk}, \mathrm{pk})$ $\mathrm{sk} \leftarrow Z_r, \mathrm{pk} \leftarrow [\mathrm{sk}]G_2$

$\mathrm{Sign}(m) \to \sigma$ $\sigma \leftarrow [\mathrm{sk}]H(m) \in \mathbb{G}_1$

$\mathrm{Verify}(\sigma, m) \to \mathrm{bool}$ $e(H(m), \mathrm{pk}) =^? (\sigma, G_2)$

З плюсів: криптосистема підтримує можливість ефективно агрегувати та перевіряти підписи різних підписників на різні повідомлення.

Криптосистема шифрування на ідентифікаторах IBE (Boneh-Franklin)

Перша криптосистема шифрування на основі ідентифікаторів із застосуванням білінійного спарювання, що запропонована в 2001р Боне та Франкліном.

Сторони узгоджують параметри: спарювання $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_T$, генератор $G_1 \in \mathbb{G}_1$, геш функцію $H_1 : \{0,1\}^* \to \mathbb{G}_1, H_2 : \mathbb{G}_2 \to \mathscr{M}$.

$\mathrm{KeyGen}(1^\lambda) \to (mk, P_{pub})$ $mk \leftarrow Z_q, P_{pub} = [mk]P$

$\mathrm{Extract}(mk, ID) \to (sk_{ID}, Q_{ID})$ $Q_{ID} = H_1(ID), sk_{ID} = [mk]Q_{ID}$

$\mathrm{Encrypt}(m, P_{pub}, ID) \to (U, V)$

$$t \xleftarrow{R} Z_r, U \leftarrow [t]P_1, V = M \oplus H_2(e(Q_{ID}, P_{pub})^t)$$

$\mathrm{Decrypt}(U, V) \to M$ $M \leftarrow V \oplus H_2(e(sk_{ID}, U))$