超特異曲線上の効率的に計算可能な distortion 写像

JANT 18

2008 / 7 / 5

高島 克幸

三菱電機

＊ANTS VIII（2008 ／ 05）での講演内容

今回の結果

- Galbraith-Pujolas-Ritzenthaler-Smith [GPRS] で，特殊な 超特異曲線上の distortion 写像に関する未解決問題が提出された．

  以下の 具体的な構成 に基づいて，それを解決した．

  - Frobenius 準同型 π の固有ベクトルからなる $\mathbb{F}_r$ - ベクトル空間 $\mathrm{Jac}_C[r] \cong (\mathbb{F}_r)^{2g}$ の基底 $\widetilde{\mathcal{B}} = \{\widetilde{D}_i\}$ （ π - 固有ベクトル基底 ）

  - $\mathbb{F}_r$ - ベクトル空間 $\mathrm{End}(\mathrm{Jac}_C) \otimes_{\mathbb{Z}} \mathbb{F}_r \cong (\mathbb{F}_r)^{(2g)^2}$ の基底 Δ

- 全ての i, j s.t. $0 \leq i, j \leq 2g-1$ に関し，Weil ペアリング $e(\widetilde{D}_i, \widetilde{D}_j)$ の ある底 $u \neq 1$ に関する離散対数を具体的に決定した．

  $\Longrightarrow$ これにより，効率的に計算可能な (セミ) シンプレクティック π - 固有ベクトル基底 が得られた．

アジェンダ

- ペアリング暗号と distortion 写像
- 対象とする超特異曲線（ターゲット曲線）
- Distortion 写像
- Distortion 写像に関する計算量問題
- [GPRS] での結果と未解決問題
- 私のアプローチ
- $C/\mathbb{F}_p : Y^2 = X^w + 1$ に関する今回の結果
- $C/\mathbb{F}_{2^m} : Y^2 + Y = X^5 + X^3 + b$ に関する今回の結果
- まとめ

ペアリング暗号 と distortion 写像

- ペアリング暗号では，distortion 写像は有用である.
  - 計算効率化
  - データサイズ削減
  - 安全性証明

- $E/\mathbb{F}_p : Y^2 = X^3 + 1$

  p : 素数 $(\equiv 2 \bmod 3)$,

  $\zeta (\in \mathbb{F}_{p^2}^*)$ s.t. $\zeta^3 = 1$

  素数 $r \mid \sharp E(\mathbb{F}_p)$

$$
\begin{array}{ccc}
\rho : E(\mathbb{F}_p) & \to & E(\mathbb{F}_{p^2}) \\
\cup & & \cup \\
P = (x, y) & \mapsto & (\zeta x, y) = \rho(P) \notin \langle P \rangle \\
\mathcal{O}_E & \mapsto & \mathcal{O}_E
\end{array}
$$

- 例えば，Weil ペアリング e に対し，$e(P, \rho(P)) \neq 1$

  このような性質を持つ写像 ρ を distortion 写像という.

- $Q = \rho(P)$ であるので，基底 $\{P, Q\}$ に対する計算の多くが，

  $\mathbb{F}_p$ での計算で行えて，計算効率化 及び データサイズ削減が行える.

対象とする超特異曲線 (ターゲット曲線)

- $C/\mathbb{F}_q$ ：幾何的に既約な非特異射影曲線
  - C :超特異 $\overset{\text{Def.}}{\Longleftrightarrow}$ Jac_C :超特異 $\overset{\text{Def.}}{\Longleftrightarrow}$ 超特異楕円曲線の直積に同種

- $C/\mathbb{F}_p : Y^2 = X^w + 1,$

  $w = 2g+1 :$ 素数, $q = p :$ 素数 s.t. $p \equiv a \bmod w, \mathbb{F}_w^* = \langle a \rangle.$

  $\pi : p$ - 乗 Frobenius 準同型写像

  $\rho :$ 1 の原始 w 乗根 ζ を用いた C 上の写像 $(x, y) \mapsto (\zeta x, y)$

  から 誘導される Jac_C 上の同型写像

- $C/\mathbb{F}_{2^m} : Y^2 + Y = X^5 + X^3 + b,$

  $b \in \mathbb{F}_2, \ m \equiv \pm 1 \bmod 6$

  $\pi : 2^m$ - 乗 Frobenius 準同型写像

  位数 32 の extra-special 2 - 群 $\mathbb{G} = \langle \pm\sigma_\omega \rangle \ (\subset \mathrm{Aut}_C)$

  による作用 [vdGvdV].

Distortion 写像

r ：素数 s.t. $r \mid \sharp \mathrm{Jac}_C(\mathbb{F}_q)$, $K := \mathbb{F}_{q^k}$ s.t. $\mathrm{Jac}_C[r] \subset \mathrm{Jac}_C(K)$.

$e : \mathrm{Jac}_C[r]$ 上の $\mu_r \subset K$ に値を取る非退化双線型写像 (ペアリング)

定義 [GPRS]

2点 $D, D' \neq \mathcal{O} \in \mathrm{Jac}_C[r]$ に対し, $e(D, \phi(D')) \neq 1$ となる自己準同型

$\phi = \phi_{D,D'} \in \mathrm{End}(\mathrm{Jac}_C)$ を distortion 写像と呼ぶ.

定理 1 [GPRS]

C ：ターゲット超特異曲線とする.

$$\mathrm{End}_K(\mathrm{Jac}_C) \otimes_{\mathbb{Z}} \mathbb{F}_r \cong \mathrm{End}_{\mathbb{F}_r}(\mathrm{Jac}_C[r]) \cong M_{2g}(\mathbb{F}_r) \cong (\mathbb{F}_r)^{(2g)^2},$$

$\mathrm{End}_K(\mathrm{Jac}_C)\,(\subset \mathrm{End}(\mathrm{Jac}_C))$: $K = \mathbb{F}_{q^k}$ 上定義された自己準同型 全体

$\mathrm{End}_{\mathbb{F}_r}(\mathrm{Jac}_C[r])$: $\mathbb{F}_r$- ベクトル空間 $\mathrm{Jac}_C[r] \cong (\mathbb{F}_r)^{2g}$ の自己準同型 全体

特に, 任意の 2点 $D, D' \neq \mathcal{O} \in \mathrm{Jac}_C[r]$ に対し,

distortion 写像 $\phi = \phi_{D,D'} \in \mathrm{End}_K(\mathrm{Jac}_C)$ が存在する.

Distortion 写像に関する計算量問題

- 定理 1 は，効率的に計算可能な distortion 写像の存在を保証するものでない．

計算量問題 1

任意の 2点 $D, D' \neq \mathcal{O} \in \mathrm{Jac}_C[r]$ に対し，distortion 写像 $\phi = \phi_{D,D'} \in \mathrm{End}(\mathrm{Jac}_C)$ s.t. $e(D, \phi(D')) \neq 1$ を 効率的に計算 せよ．

Cf. [GR] で，一般の超特異楕円曲線の場合が扱われている．

計算量問題 2

効率的に計算可能な 写像からなる
$\mathrm{End}_K(\mathrm{Jac}_C) \otimes_{\mathbb{Z}} \mathbb{F}_r \cong M_{2g}(\mathbb{F}_r) \cong (\mathbb{F}_r)^{(2g)^2}$ の基底 Δ の存在を示せ．

- 問題 2 での基底 Δ

⟹ 問題 1 への肯定的解答 (効率的アルゴリズム)

[GPRS] での結果と未解決問題

- **[GPRS] は，ターゲット曲線に対して，$\mathbb{Q}$ - ベクトル空間**
  $\mathrm{End}^0(\mathrm{Jac}_C) := \mathrm{End}(\mathrm{Jac}_C) \otimes \mathbb{Q}$ の基底を与えた.

  - $C/\mathbb{F}_p : Y^2 = X^w + 1$ に対しては，
    $\Delta := \{\pi^i \rho^j \mid 0 \leq i, j \leq 2g-1\}$ が，$\mathbb{Q}$ 上の基底である.
  - $C/\mathbb{F}_{2^m} : Y^2 + Y = X^5 + X^3 + b$ に対しては，
    $\Delta := \{\pi^i, \pi^j \sigma_\theta, \pi^\kappa \sigma_\tau, \pi^l \sigma_\xi \mid 0 \leq i, j, \kappa, l \leq 3\}$ と
    $\Delta^* := \{\pi^i, \sigma_\theta \pi^j, \sigma_\tau \pi^\kappa, \sigma_\xi \pi^l \mid 0 \leq i, j, \kappa, l \leq 3\}$ は，$\mathbb{Q}$ 上の基底である.

[GPRS] での未解決問題

上記の Δ 及び Δ^* は，$\mathrm{End}_K(\mathrm{Jac}_C) \otimes_{\mathbb{Z}} \mathbb{F}_r$ の $\mathbb{F}_r$ 上の基底であるか？

1番目の曲線に関しては，$\gcd(r, 2gw) = 1$ の時に，
2番目の曲線に関しては，$r > 19$ の時に，[GPRS]より直接的な方法を用いて，私は上記問題を肯定的に解決した.

⇒ ターゲット曲線 に関する問題 2 (及び 1) に対する肯定的解答.

私のアプローチ

- 非零な $D^* \in \mathrm{Jac}_C(\mathbb{F}_q)[r]$ と具体的な生成作用素 $G_i \in \mathrm{End}_K(\mathrm{Jac}_C) \otimes \mathbb{F}_r$ を用いて，$\mathrm{Jac}_C[r]$ の π- 固有ベクトル基底 $\widetilde{\mathcal{B}} = \{\widetilde{D}_i\}$ を構成する.

  i.e. $\widetilde{D}_i := G_i D^* \quad (i = 0, \ldots, 2g-1)$.

  - 例えば，1 番目の曲線に関しては，G_i は Gauss 和 で与えられる.
  - G_i は 可逆であり，G_i^{-1} も，また効率的に計算可能であることを示す.

  キーファクト: $G(\psi^{-j}, \chi)G(\psi^j, \chi) = \psi^{-j}(-1)w \neq 0 \in \mathbb{F}_r$.

- $\mathrm{Pr}_j := \left(\prod_{i \neq j}(\lambda_j - \lambda_i)\right)^{-1} \prod_{i \neq j}(\pi - \lambda_i)$: $\langle \widetilde{D}_j \rangle$ への射影作用素

  但し，λ_i は，$\widetilde{D}_j$ に対する π の固有値とする.

  $G_{i,j} := G_i G_j^{-1}$ として $E_{i,j} := G_{i,j}\mathrm{Pr}_j \in \mathrm{End}_K(\mathrm{Jac}_C) \otimes \mathbb{F}_r$ とする.

  $\Longrightarrow$ $E_{i,j}$: 基底 $\widetilde{\mathcal{B}} = \{\widetilde{D}_i\}$ に関する行列単位.

- 構成より $E_{i,j} \in \langle \delta \mid \delta \in \Delta \rangle$ であるので，

  Δ (及びΔ^*) は $\mathbb{F}_r$- ベクトル空間 $\mathrm{End}_K(\mathrm{Jac}_C) \otimes_{\mathbb{Z}} \mathbb{F}_r$ の基底である.

$C/\mathbb{F}_p : Y^2 = X^{2g+1}+1$ に関する今回の結果

- $\Delta := \{\pi^i\rho^j \mid 0 \le i,j \le 2g-1\}$. $\pi, \rho \in \mathrm{End}_K(\mathrm{Jac}_C)$　但し，$K = \mathbb{F}_{p^{2g}}$.

> $\gcd(r, 2gw) = 1$ の時に，Δ が $\mathbb{F}_r$ - ベクトル空間　$\mathrm{End}_K(\mathrm{Jac}_C) \otimes_{\mathbb{Z}} \mathbb{F}_r$
> $\cong M_{2g}(\mathbb{F}_r)$ の基底であることを示す．(特に，$r > w = 2g+1$ 時に成立．)

- $\mathrm{Jac}_C[r]$ の　π - 固有ベクトル基底　$\widetilde{\mathcal{B}} = \{\widetilde{D}_i\}$　の構成

1. 非零な　$D^* \in \mathrm{Jac}_C(\mathbb{F}_p)[r]$　を生成.
2. $\widetilde{D}_j := G_j D^*$　$(j = 0, \ldots, 2g-1)$.

$$G_j := G(\psi^j, \chi) := \sum_{i=0}^{2g-1} \left(p^j\right)^i \rho^{a^i} \in \mathbb{F}_r[\rho] \subset \mathrm{End}(\mathrm{Jac}_C) \otimes \mathbb{F}_r$$

: Gauss 和 作用素

- $\mathbb{F}_w$ の 位数　$2g$ の 乗法的指標

$\psi : \mathbb{F}_w^* = \langle a \rangle \ni a \mapsto p \in \langle p \rangle \subset \mathbb{F}_r^*$, ($\because$ $r \mid p^g + 1$ より，$p \in \mathbb{F}_r^*$ の 位数は $2g$　だから.)

- $\mathbb{F}_w$　の 加法的指標

$\chi : \mathbb{F}_w \ni v \mapsto \rho^v \in (\mathbb{F}_r[\rho])^* \subset \mathrm{End}(\mathrm{Jac}_C) \otimes_{\mathbb{Z}} \mathbb{F}_r$.

$C/\mathbb{F}_p : Y^2 = X^{2g+1} + 1$ に関する今回の結果

- $\pi(\widetilde{D}_j) = \lambda_j \widetilde{D}_j$, 但し $\lambda_j := p^{-j}$.
- $G(\psi^{-j}, \chi)\widetilde{D}_j = G(\psi^{-j}, \chi)G(\psi^{j}, \chi)D^* = \psi^{-j}(-1)wD^* = (-1)^j wD^* \neq \mathcal{O}$.

  $\Longrightarrow$ $\widetilde{D}_j \neq \mathcal{O}$. $\Longrightarrow$ $\widetilde{\mathcal{B}} = \{\widetilde{D}_i\}$ は $\mathrm{Jac}_C[r]$ の π - 固有ベクトル基底.

- $\mathrm{Pr}_j := \left(\prod_{i\neq j}(\lambda_j - \lambda_i)\right)^{-1} \prod_{i \neq j}(\pi - \lambda_i)$,

  $\Longrightarrow$ $\mathrm{Pr}_j(\widetilde{D}_\kappa) = \begin{cases} \mathcal{O} & \text{if } \kappa \neq j \\ \widetilde{D}_j & \text{if } \kappa = j \end{cases}$

- $E_{i,j} := c_j \cdot G(\psi^i, \chi)G(\psi^{-j}, \chi)\mathrm{Pr}_j = c_j \cdot J(\psi^i, \psi^{-j})G(\psi^{i-j}, \chi)\mathrm{Pr}_j$

  但し, $c_j := (-1)^j w^{-1}$, かつ $J(\psi^i, \psi^{-j}) \in \mathbb{F}_r$ は Jacobi 和.

  $\Longrightarrow$ $E_{i,j}(\widetilde{D}_\kappa) = \begin{cases} \mathcal{O} & \text{if } \kappa \neq j \\ \widetilde{D}_i & \text{if } \kappa = j \end{cases}$ $\Longrightarrow$ $\{E_{i,j}\}$ は $\mathrm{End}_K(\mathrm{Jac}_C) \otimes_{\mathbb{Z}} \mathbb{F}_r$ の基底.

- $E_{i,j} \in \mathbb{F}_r[\pi, \rho]$, $\quad \pi^\ell \rho = \rho^{a^\ell} \pi^\ell$ ($\forall \ell \in \mathbb{Z}$).

  $\Longrightarrow$ $\Delta = \{\pi^i \rho^j\}$ は $\mathrm{End}_K(\mathrm{Jac}_C) \otimes_{\mathbb{Z}} \mathbb{F}_r$ の基底. $\square$

Weil ペアリング $e = e_r$ の基本的性質

- $e(D, \widehat{f}(D')) = e(f(D), D')$

  但し $D, D' \in \mathrm{Jac}_C[r],\ \ f \in \mathrm{End}(\mathrm{Jac}_C)$, かつ $\widehat{f}$: f の dual.
  e.g. [Mil, p.132]

  特に, 以下の 2 ケースを用いる.

  - $f = \pi, \widehat{\pi}\pi = p.$ $\qquad e(\pi(D), \pi(D')) = e(D, D')^p.$
  - $f \in \mathrm{Aut}(C).$ $\qquad e(f(D), f(D')) = e(D, D').$

- 例えば, 以下の式変形を用いる.

$$
\begin{aligned}
& e(\rho^{a^i}(D^*), \rho^{a^j}(D^*)) = e(\rho^{a^i}(D^*), \rho^{a^i}\rho^{a^j - a^i}(D^*)) = e(D^*, \rho^{a^j - a^i}(D^*)) \\
= \ & e(D^*, \rho^{a^i(a^{j-i}-1)}(D^*)) = e(D^*, \rho^{a^i(a^{j-i}-1)}\pi^i(D^*)) \\
= \ & e(\pi^i(D^*), \pi^i\rho^{a^{j-i}-1}(D^*)) = e(D^*, \rho^{a^{j-i}-1}(D^*))^{p^i}.
\end{aligned}
$$

$C/\mathbb{F}_p : Y^2 = X^{2g+1} + 1$ 上の Weil ペアリング

- Weil ペアリング e の前スライドの性質より，以下が計算できた．

$$(\log_u(e(\widetilde{D}_i, \widetilde{D}_j)))_{i,j} = 2g \cdot \begin{pmatrix} 0 & \cdots & \eta_{2g-1} \\ \vdots & \iddots & \vdots \\ \eta_0 & \cdots & 0 \end{pmatrix}$$

但し $u := e(D^*, \rho(D^*))$,

$\eta_0 := 1$ かつ $\eta_i := -J(\psi, \psi^i) \in \mathbb{F}_r^* \quad (i = 1, \ldots, 2g-1)$.

⇒ 特に，$\gcd(r, 2gw) = 1$ の時，任意の非零 $D^* \in \mathrm{Jac}_C(\mathbb{F}_p)[r]$ に対して，$u \neq 1$.

- $i = 0, \ldots, g-1$ に対し，$\widetilde{D}_i$ を $(2g\eta_{2g-1-i})^{-1}\widetilde{D}_i$ に正規化することで，Weil ペアリングに関する

効率的に計算可能な (セミ) シンプレクティック 基底 を得た．

$C/\mathbb{F}_{2^m} : Y^2 + Y = X^5 + X^3 + b.$

- $b \in \mathbb{F}_2,\ m \equiv \pm 1 \bmod 6,\ q := 2^m$

  $\mathrm{Jac}_C(\mathbb{F}_q)$ の (全) 埋め込み次数 k は 12, i.e., $q \in \mathbb{F}_r^*$ の位数は 12.

- 位数 32 の extra-special 2-群 $\mathbb{G} = \langle \pm\sigma_\omega \rangle$ $(\subset \mathrm{Aut}_C)$ の作用
  - $E(z) = z^{16} + z^8 + z^2 + z$

    $= (z^6 + z^5 + z^3 + z^2 + 1)(z^3 + z^2 + 1)(z^3 + z + 1)(z^2 + z + 1)(z + 1)z$

  - 任意の $\omega \in \mathbb{F}_{2^6}$ s.t. $E(\omega) = 0$ に対して,

    $\sigma_\omega : (x, y) \mapsto (x + \omega, y + s_2 x^2 + s_1 x + s_0)$

    但し $s_2 = \omega^8 + \omega^4 + \omega,\quad s_1 = \omega^4 + \omega^2,$

    s_0 は $s^2 + s = \omega^5 + \omega^3$ のどちらかの根.

- 位数 8 の2面体部分群 $\mathbb{G}_0 := \langle \sigma_\tau, \sigma_\theta \rangle \subset \mathbb{G}$
  - $\tau \in \mathbb{F}_{2^6}$ s.t. $\tau^6 + \tau^5 + \tau^3 + \tau^2 + 1 = 0.$

    $\xi := \tau^4 + \tau^2 \in \mathbb{F}_{2^3},\ \theta := \tau^4 + \tau^2 + \tau \in \mathbb{F}_{2^2} \Longrightarrow E(\xi) = E(\theta) = 0.$

  - $\sigma_\xi = \pm\sigma_\theta\sigma_\tau, \sigma_\tau^2 = -1, \sigma_\theta^2 = 1, \sigma_\xi^2 = 1, \sigma_\tau\sigma_\theta = -\sigma_\theta\sigma_\tau.$

$C/\mathbb{F}_{2^m} : Y^2 + Y = X^5 + X^3 + b$ に関する今回の結果

- $\Delta := \{\pi^i, \pi^j\sigma_\theta, \pi^\kappa\sigma_\tau, \pi^l\sigma_\xi \mid 0 \le i, j, \kappa, l \le 3\}$,
  $\Delta^* := \{\pi^i, \sigma_\theta\pi^j, \sigma_\tau\pi^\kappa, \sigma_\xi\pi^l \mid 0 \le i, j, \kappa, l \le 3\}$.
- $\pi, \sigma_\theta, \sigma_\tau, \sigma_\xi \in \mathrm{End}_K(\mathrm{Jac}_C)$ s.t. $K = \mathbb{F}_{q^{12}}$. $r \mid q^{12} - 1$.

> $r > 19$ の時に，Δ 及び Δ^* が，$\mathbb{F}_r$ - ベクトル空間
> $\mathrm{End}_K(\mathrm{Jac}_C) \otimes_{\mathbb{Z}} \mathbb{F}_r \cong M_{2g}(\mathbb{F}_r)$ の基底であることを示す.

- 以下で構成される $\mathcal{B} := \{D_i\}$ を考える.
  1. 非零な $D_1 := D^* \in \mathrm{Jac}_C(\mathbb{F}_q)[r]$ を生成.
  2. $D_2 := \sigma_\theta D_1,\ D_3 := \sigma_\tau D_1,\ D_4 := \sigma_\xi D_1$.

  $\Rightarrow$ $D_2 \in \mathrm{Jac}_C(\mathbb{F}_{q^4})[r],\ D_3 \in \mathrm{Jac}_C(\mathbb{F}_{q^{12}})[r],\ D_4 \in \mathrm{Jac}_C(\mathbb{F}_{q^3})[r]$.

- $\pi D_1 = D_1,\ \pi D_2 = \lambda D_2,\ \pi D_3 = \lambda(\mu D_3 + dD_2),\quad \pi D_4 = \mu D_4 + dD_1$,

  但し $\lambda = q^3 \text{ or } -q^3 = q^9, \qquad \mu = q^4 \text{ or } q^8$,

$$d = \begin{cases} q^5 \text{ or } -q^5 & \text{when } \mu = q^4, \\ q \text{ or } -q & \text{when } \mu = q^8. \end{cases}$$

$C/\mathbb{F}_{2^m} : Y^2 + Y = X^5 + X^3 + b$ に関する今回の結果

- $\nu := \frac{d}{\lambda-1} \in \mathbb{F}_r \Longrightarrow$ $r > 19$ の時, $\nu \neq \pm 1$.

- 以下の $\widetilde{\mathcal{B}} := \{\widetilde{D}_i\}$ が $\mathrm{Jac}_C[r]$ の π - 固有ベクトル基底であることを示す.
  - $\widetilde{D}_1 := D_1,\ \widetilde{D}_2 := D_2,\ \widetilde{D}_3 := D_3 + \nu D_2,\ \widetilde{D}_4 := D_4 + \nu D_1.$

    $\pi \widetilde{D}_i = \lambda_i \widetilde{D}_i,\quad \lambda_1 := 1,\ \lambda_2 := \lambda,\ \lambda_3 := \lambda\mu,\ \lambda_4 := \mu.$

  - $G_1 := 1,\ G_2 := \sigma_\theta,\ G_3 := \sigma_\theta(\sigma_\xi + \nu),\ G_4 := \sigma_\xi + \nu,$

    $\Longrightarrow \widetilde{D}_i = G_i D_1 \quad (i = 1, \ldots, 4).$

  - $r > 19$ の時, $(\sigma_\xi - \nu)(\sigma_\xi + \nu) = 1 - \nu^2 =: c \neq 0.$

    $G_1^{-1} = 1,\ G_2^{-1} = \sigma_\theta,\ G_3^{-1} = c^{-1}(\sigma_\xi - \nu)\sigma_\theta,\ G_4^{-1} = c^{-1}(\sigma_\xi - \nu).$

    $\Longrightarrow G_i^{-1}\widetilde{D}_i = D_1 \neq \mathcal{O} \quad (i = 1, \ldots, 4).$

    $\Longrightarrow \widetilde{\mathcal{B}} = \{\widetilde{D}_i\}$ は $\mathrm{Jac}_C[r]$ の π - 固有ベクトル基底.

$C/\mathbb{F}_{2^m} : Y^2 + Y = X^5 + X^3 + b$ に関する今回の結果

- $\mathrm{Pr}_j := \left(\prod_{i \neq j}(\lambda_j - \lambda_i)\right)^{-1} \prod_{i \neq j}(\pi - \lambda_i),$

  $G_{i,j} := G_i G_j^{-1} \in \mathbb{F}_r[\sigma_\tau, \sigma_\theta].$

  $E_{i,j} := G_{i,j}\mathrm{Pr}_j \in \mathbb{F}_r[\pi] \oplus \sigma_\theta \mathbb{F}_r[\pi] \oplus \sigma_\tau \mathbb{F}_r[\pi] \oplus \sigma_\xi \mathbb{F}_r[\pi].$

  $\Longrightarrow$ $\mathbb{G}_0 = \langle \sigma_\tau, \sigma_\theta \rangle$ は (2面体)部分群であるので,

  $\Delta := \{\pi^i, \pi^j\sigma_\theta, \pi^\kappa\sigma_\tau, \pi^l\sigma_\xi \mid 0 \leq i, j, \kappa, l \leq 3\}$

  及び $\Delta^* := \{\pi^i, \sigma_\theta\pi^j, \sigma_\tau\pi^\kappa, \sigma_\xi\pi^l \mid 0 \leq i, j, \kappa, l \leq 3\}$

  は $\mathbb{F}_r$ - ベクトル空間 $\mathrm{End}_K(\mathrm{Jac}_C) \otimes_{\mathbb{Z}} \mathbb{F}_r$ の基底.

- $u := e(D_1, D_3) = e(D_1, \sigma_\tau(D_1)).$ Weil ペアリング e の性質を用いて

$$(\log_u(e(\widetilde{D}_i, \widetilde{D}_j)))_{i,j} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}. \Longrightarrow u \neq 1$$

$\widetilde{\mathcal{B}}$: Weil ペアリングに関する (セミ) シンプレクティック 基底.

まとめ

- **Distortion 写像 に関して [GPRS] で与えられた未解決問題を解決した.**

- **$2g$ 次元 $\mathbb{F}_r$- ベクトル空間 $\mathrm{Jac}_C[r] \cong (\mathbb{F}_r)^{2g}$ の暗号応用を考える上で，今回の具体的な構成は有用であると思われる.**

- **より広いクラスの曲線に対して，同様な 又は 一般的な結果を示すことは出来るだろうか？ Cf. [GR]**

- **暗号以外にも，今回の結果の応用がないか？**