Efficiently Computable Distortion Maps for Supersingular Curves

ANTS 2008

2008 / 5 / 20

Katsuyuki Takashima

Mitsubishi Electric

Our results

- **Galbraith-Pujolas-Ritzenthaler-Smith [GPRS] gave unsolved problems on distortion maps for special supersingular curves.**

  We solve them based on explicit construction of

  - **a basis $\widetilde{\mathcal{B}} = \{\widetilde{D}_i\}$ of $\mathbb{F}_r$ - vector space $\mathrm{Jac}_C[r] \cong (\mathbb{F}_r)^{2g}$ consisting of eigenvectors of the Frobenius endomorphism π (π-eigenvector basis)**

  - **a $\mathbb{F}_r$-basis Δ of $\mathbb{F}_r$ - vector space $\mathrm{End}(\mathrm{Jac}_C) \otimes_{\mathbb{Z}} \mathbb{F}_r \cong (\mathbb{F}_r)^{(2g)^2}$.**

- **We explicitly determine the discrete logarithms of the Weil pairing $e(\widetilde{D}_i, \widetilde{D}_j)$ to one base $u \neq 1$ where $0 \leq i, j \leq 2g-1$.**

  ⇒ **We obtain an efficiently constructible (semi-)symplectic π-eigenvector basis.**

Agenda

- Target supersingular curves
- Distortion maps
- Computational problems on distortion maps
- Results and unsolved problem given in [GPRS]
- Our approach
- Our results on $C/\mathbb{F}_p : Y^2 = X^w + 1$
- Our results on $C/\mathbb{F}_{2^m} : Y^2 + Y = X^5 + X^3 + b$
- Conclusions

Target supersingular curves

- $C/\mathbb{F}_q$: **proj., nonsingular, geom. irred. curve.**
  - C **:supersingular** $\overset{\text{Def.}}{\Leftrightarrow}$ Jac_C **:supersingular** $\overset{\text{Def.}}{\Leftrightarrow}$
    isogeneous to a product of supersingular elliptic curves

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

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

  π : p **-power Frobenius endomorphism**

  ρ : **action of a primitive** w**-th root of unity** ζ **on** Jac_C
  induced by $(x, y) \mapsto (\zeta x, y)$ **on** C

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

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

  π : 2^m **-power Frobenius endomorphism**

  Action of an extra-special 2-group $\mathbb{G} = \langle \pm\sigma_\omega \rangle\ (\subset \mathrm{Aut}_C)$
  of order 32 [vdGvdV].

Distortion maps

r : **prime 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 : **nondegenerate bilinear pairing from** $\mathrm{Jac}_C[r]$ **to** $\mu_r \subset K$.

Definition [GPRS]

For a pair $D, D' \neq \mathcal{O} \in \mathrm{Jac}_C[r]$,

$\phi = \phi_{D,D'} \in \mathrm{End}(\mathrm{Jac}_C)$ s.t. $e(D, \phi(D')) \neq 1$ **is called a distortion map.**

Theorem 1 [GPRS]

Let C **be a target supersingular curve.**

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

$\mathrm{End}_K(\mathrm{Jac}_C)\ (\subset \mathrm{End}(\mathrm{Jac}_C))$: **endo. defined over** $K = \mathbb{F}_{q^k}$,

$\mathrm{End}_{\mathbb{F}_r}(\mathrm{Jac}_C[r])$: **endo. of** $\mathbb{F}_r$ **- vector space** $\mathrm{Jac}_C[r] \cong (\mathbb{F}_r)^{2g}$.

In particular, for every pair $D, D' \neq \mathcal{O} \in \mathrm{Jac}_C[r]$,

there exists a distortion map $\phi = \phi_{D,D'} \in \mathrm{End}_K(\mathrm{Jac}_C)$.

Computational problems on distortion maps

- **Theorem 1 doesn't assure the existence of an efficiently computable distortion map.**

Computational problem 1

For every pair $D, D' \neq \mathcal{O} \in \mathrm{Jac}_C[r]$, **can we efficiently compute a distortion map** $\phi = \phi_{D,D'} \in \mathrm{End}(\mathrm{Jac}_C)$ **s.t.** $e(D, \phi(D')) \neq 1$ **?**

Cf. [GR] for the case of supersingular elliptic curves.

Computational problem 2

Is there a basis Δ **of** $\mathrm{End}_K(\mathrm{Jac}_C) \otimes_{\mathbb{Z}} \mathbb{F}_r \cong M_{2g}(\mathbb{F}_r) \cong (\mathbb{F}_r)^{(2g)^2}$

s.t. $\forall \delta \in \Delta$ **are efficiently computable ?**

- **Basis** Δ **in problem 2**

  ⇒ **an answer (efficient algorithm) to problem 1.**

Results and unsolved problem given in [GPRS]

- **[GPRS] gave bases of $\mathbb{Q}$-vector space**

  $\mathrm{End}^0(\mathrm{Jac}_C) := \mathrm{End}(\mathrm{Jac}_C) \otimes \mathbb{Q}$ **for target curves.**

  - **For** $C/\mathbb{F}_p : Y^2 = X^w + 1$, $\Delta := \{\pi^i \rho^j \mid 0 \leq i, j \leq 2g-1\}$ **is a $\mathbb{Q}$-basis.**
  - **For** $C/\mathbb{F}_{2^m} : Y^2 + Y = X^5 + X^3 + b$,
    $\Delta := \{\pi^i, \pi^j \sigma_\theta, \pi^\kappa \sigma_\tau, \pi^l \sigma_\xi \mid 0 \leq i, j, \kappa, l \leq 3\}$ **and**
    $\Delta^* := \{\pi^i, \sigma_\theta \pi^j, \sigma_\tau \pi^\kappa, \sigma_\xi \pi^l \mid 0 \leq i, j, \kappa, l \leq 3\}$ **are $\mathbb{Q}$-bases.**

Unsolved problem given in [GPRS]

Are the above Δ and Δ^* $\mathbb{F}_r$-bases of $\mathrm{End}_K(\mathrm{Jac}_C) \otimes_{\mathbb{Z}} \mathbb{F}_r$?

We show that it holds
for 1-st curve when $\gcd(r, 2gw) = 1$ and 2-nd curve when $r > 19$
by using a direct approach different from theirs.

⇒ **positive answer to problem 2 (and 1) for target curves.**

Our approach

- We construct a π-eigenvector basis $\widetilde{\mathcal{B}} = \{\widetilde{D}_i\}$ of $\mathrm{Jac}_C[r]$
  with a nonzero $D^* \in \mathrm{Jac}_C(\mathbb{F}_q)[r]$
  and explicit generating operators $G_i \in \mathrm{End}_K(\mathrm{Jac}_C) \otimes \mathbb{F}_r$
  s.t. $\widetilde{D}_i = G_i D^*$ for $i = 0, \ldots, 2g-1$.
  - For example, G_i are given by Gauss sums for the 1-st curve.
  - We show that G_i are invertible and G_i^{-1} are also efficiently computable.
    A key fact: $G(\psi^{-j}, \chi) G(\psi^j, \chi) = \psi^{-j}(-1) w \neq 0 \in \mathbb{F}_r$.
- $\mathrm{Pr}_j := \left(\prod_{i \neq j}(\lambda_j - \lambda_i)\right)^{-1} \prod_{i \neq j}(\pi - \lambda_i)$: projection to $\widetilde{D}_j$
  where λ_i are eigenvalues of π.
  $E_{i,j} := G_{i,j}\mathrm{Pr}_j \in \mathrm{End}_K(\mathrm{Jac}_C) \otimes \mathbb{F}_r$ where $G_{i,j} := G_i G_j^{-1}$
  : matrix units w.r.t. $\widetilde{\mathcal{B}} = \{\widetilde{D}_i\}$
- Since $E_{i,j} \in \langle \delta \mid \delta \in \Delta \rangle$, we know that
  Δ (and Δ^*) are $\mathbb{F}_r$-bases of $\mathrm{End}_K(\mathrm{Jac}_C) \otimes_{\mathbb{Z}} \mathbb{F}_r$.

Our results on $C/\mathbb{F}_p : Y^2 = X^{2g+1} + 1$.

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

We show that Δ is a $\mathbb{F}_r$-basis of $\mathrm{End}_K(\mathrm{Jac}_C) \otimes_{\mathbb{Z}} \mathbb{F}_r \cong M_{2g}(\mathbb{F}_r)$ when $\gcd(r, 2gw) = 1$ for $w = 2g+1$. (it holds if $r > w = 2g+1$.)

- **π-eigenvector basis $\widetilde{\mathcal{B}} = \{\widetilde{D}_i\}$ of $\mathrm{Jac}_C[r]$.**

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

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

: Gauss sum operator

- **multiplicative character of $\mathbb{F}_w$ of order $2g$**

$$\psi : \mathbb{F}_w^* = \langle a \rangle \ni a \mapsto p \in \langle p \rangle \subset \mathbb{F}_r^* \ , (\because \text{order of } p \in \mathbb{F}_r^* \text{ is } 2g \text{ since } r \mid p^g + 1.)$$

- **additive character of $\mathbb{F}_w$**

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

Our results on $C/\mathbb{F}_p : Y^2 = X^{2g+1} + 1$.

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

  $\Longrightarrow \widetilde{D}_j \neq \mathcal{O}. \Longrightarrow \widetilde{\mathcal{B}} = \{\widetilde{D}_i\}$ **is a** π **-eigenvector basis of** $\mathrm{Jac}_C[r]$.

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

  $\Longrightarrow \mathrm{Pr}_j(\widetilde{D}_\kappa) = \begin{cases} \mathcal{O} & \text{if } \kappa \neq j \\ \widetilde{D}_j & \text{if } \kappa = j \end{cases}$
- $E_{i,j} := c_j \cdot G(\psi^i, \chi)G(\psi^{-j}, \chi)\mathrm{Pr}_j = c_j \cdot J(\psi^i, \psi^{-j})G(\psi^{i-j}, \chi)\mathrm{Pr}_j$

  where $c_j := (-1)^j w^{-1}$, **and** $J(\psi^i, \psi^{-j}) \in \mathbb{F}_r$ **is a Jacobi sum.**

  $\Longrightarrow E_{i,j}(\widetilde{D}_\kappa) = \begin{cases} \mathcal{O} & \text{if } \kappa \neq j \\ \widetilde{D}_i & \text{if } \kappa = j \end{cases} \Longrightarrow \{E_{i,j}\}$ **is a basis of** $\mathrm{End}_K(\mathrm{Jac}_C) \otimes_{\mathbb{Z}} \mathbb{F}_r$.
- **From** $E_{i,j} \in \mathbb{F}_r[\pi, \rho]$ **and** $\pi^\ell \rho = \rho^{a^\ell} \pi^\ell$ **for** $\forall \ell \in \mathbb{Z}$,

  we see that $\Delta = \{\pi^i \rho^j\}$ **is a basis of** $\mathrm{End}_K(\mathrm{Jac}_C) \otimes_{\mathbb{Z}} \mathbb{F}_r$. $\square$

Fundamental properties of the Weil pairing $e = e_r$.

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

  where $D, D' \in \mathrm{Jac}_C[r]$, $f \in \mathrm{End}(\mathrm{Jac}_C)$, **and** $\widehat{f}$ **: the dual of** f.

  e.g. [Mil, p.132]

  In particular, we use the following two cases.

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

- **For example, we calculate**

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

Weil pairing on $C/\mathbb{F}_p : Y^2 = X^{2g+1} + 1$.

- **Using the fundamental properties of e, we obtain**

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

where $u := e(D^*, \rho(D^*))$,

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

⇒ $u \neq 1$ **when** $\gcd(r, 2gw) = 1$

for any nonzero $D^* \in \mathrm{Jac}_C(\mathbb{F}_p)[r]$. **(Corollary 2)**

- **If we normalize** $\widetilde{D}_i$ **to** $(2g\eta_{2g-1-i})^{-1}\widetilde{D}_i$ **for** $i = 0, \ldots, g-1$,
  we obtain an efficiently constructible (semi-)symplectic basis
  w.r.t. the Weil pairing.

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

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

  (full) embedding degree k for $\mathrm{Jac}_C(\mathbb{F}_q)$ is 12, i.e., order of $q \in \mathbb{F}_r^*$ is 12.

- **Action of an extra-special 2-group $\mathbb{G} = \langle \pm\sigma_\omega \rangle$ $(\subset \mathrm{Aut}_C)$ of order 32.**
  - $E(z) = z^{16} + z^8 + z^2 + z$
    $= (z^6 + z^5 + z^3 + z^2 + 1)(z^3 + z^2 + 1)(z^3 + z + 1)(z^2 + z + 1)(z + 1)z$
  - **For any** $\omega \in \mathbb{F}_{2^6}$ s.t. $E(\omega) = 0$,
    $\sigma_\omega : (x, y) \mapsto (x + \omega, y + s_2 x^2 + s_1 x + s_0)$
    where $s_2 = \omega^8 + \omega^4 + \omega$, $s_1 = \omega^4 + \omega^2$,
    s_0 **is a root of the quadratic eq.** $s^2 + s = \omega^5 + \omega^3$.

- **The dihedral subgroup $\mathbb{G}_0 := \langle \sigma_\tau, \sigma_\theta \rangle \subset \mathbb{G}$ of order 8.**
  - $\tau \in \mathbb{F}_{2^6}$ s.t. $\tau^6 + \tau^5 + \tau^3 + \tau^2 + 1 = 0$.
    $\xi := \tau^4 + \tau^2 \in \mathbb{F}_{2^3}$, $\theta := \tau^4 + \tau^2 + \tau \in \mathbb{F}_{2^2}$ $\Longrightarrow$ $E(\xi) = E(\theta) = 0$.
  - $\sigma_\xi = \pm\sigma_\theta\sigma_\tau, \sigma_\tau^2 = -1, \sigma_\theta^2 = 1, \sigma_\xi^2 = 1, \sigma_\tau\sigma_\theta = -\sigma_\theta\sigma_\tau$.

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

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

We show that Δ and Δ^* are $\mathbb{F}_r$-bases of $\mathrm{End}_K(\mathrm{Jac}_C) \otimes_{\mathbb{Z}} \mathbb{F}_r \cong M_{2g}(\mathbb{F}_r)$ when $r > 19$.

- **We consider the following** $\mathcal{B} = \{D_i\}$.
  1. **Generate a nonzero** $D_1 = D^* \in \mathrm{Jac}_C(\mathbb{F}_q)[r]$.
  2. $D_2 := \sigma_\theta D_1$, $D_3 := \sigma_\tau D_1$, $D_4 := \sigma_\xi D_1$.
     $\Rightarrow$ $D_2 \in \mathrm{Jac}_C(\mathbb{F}_{q^4})[r]$, $D_3 \in \mathrm{Jac}_C(\mathbb{F}_{q^{12}})[r]$, $D_4 \in \mathrm{Jac}_C(\mathbb{F}_{q^3})[r]$.
- $\pi D_1 = D_1$, $\pi D_2 = \lambda D_2$, $\pi D_3 = \lambda(\mu D_3 + dD_2)$, **and** $\pi D_4 = \mu D_4 + dD_1$,
  where $\lambda = q^3$ or $-q^3 = q^9$, $\mu = q^4$ or q^8,
  $$d = \begin{cases} q^5 \text{ or } -q^5 & \text{when } \mu = q^4, \\ q \text{ or } -q & \text{when } \mu = q^8. \end{cases}$$

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

- $\nu := \frac{d}{\lambda - 1} \in \mathbb{F}_r$ ⟹ $\nu \neq \pm 1$ **when** $r > 19$. **(Lemma 5)**
- **A basis** $\widetilde{\mathcal{B}} = \{\widetilde{D}_i\}$ **of** $\mathrm{Jac}_C[r]$ **consisting of eigenvectors of** π.
  - $\widetilde{D}_1 := D_1,\ \widetilde{D}_2 := D_2,\ \widetilde{D}_3 := D_3 + \nu D_2,\ \widetilde{D}_4 := D_4 + \nu D_1.$

    $\pi \widetilde{D}_i = \lambda_i \widetilde{D}_i,\quad \lambda_1 := 1,\ \lambda_2 := \lambda,\ \lambda_3 := \lambda\mu,\ \lambda_4 := \mu.$
  - $G_1 := 1,\ G_2 := \sigma_\theta,\ G_3 := \sigma_\theta(\sigma_\xi + \nu),\ G_4 := \sigma_\xi + \nu,$

    ⟹ $\widetilde{D}_i = G_i D_1$ **for** $i = 1, \ldots, 4.$
  - $(\sigma_\xi - \nu)(\sigma_\xi + \nu) = 1 - \nu^2 =: c \neq 0$ **when** $r > 19.$

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

    ⟹ $G_i^{-1}\widetilde{D}_i = D_1 \neq \mathcal{O}$ **for** $i = 1, \ldots, 4.$

    ⟹ $\widetilde{\mathcal{B}} = \{\widetilde{D}_i\}$ **is a** π**-eigenvector basis of** $\mathrm{Jac}_C[r]$.

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

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

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

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

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

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

  are $\mathbb{F}_r$-bases of $\mathrm{End}_K(\mathrm{Jac}_C) \otimes_{\mathbb{Z}} \mathbb{F}_r$

  since $\mathbb{G}_0 = \langle \sigma_\tau, \sigma_\theta \rangle$ is the dihedral group.

- $u := e(D_1, D_3) = e(D_1, \sigma_\tau(D_1))$. By the fundamental properties of e,

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

$\widetilde{\mathcal{B}}$: (semi-)symplectic basis w.r.t. the Weil pairing e.

Conclusions

- **We proved several facts on distortion maps given in [GPRS].**
- **Our explicit results seem useful**

  to use $2g$- dim. vector space $\mathrm{Jac}_C[r] \cong (\mathbb{F}_r)^{2g}$ in cryptography.
- **Can we obtain a similar or general result for a broader class of curves ? Cf. [GR]**
- **Is there another application of our results ?**