Genus theory characters and DDH

Jana Sotáková

University of Amsterdam/QuSoft

March 17, 2022

Joint work with Wouter Castryck and Frederik Vercauteren
Breaking the decisional Diffie-Hellman problem for class group actions using genus theory

https://eprint.iacr.org/2020/151

Today

- Want to study the CRS/CSIDH group action

$$E' = [\mathfrak{a}] \star E$$

- Given such E and E', what can we say about $[\mathfrak{a}]$?

- Attack the following problem:

  Decisional Diffie-Hellman problem for isogeny group actions:
  Given elliptic curves $E, E_A = [\mathfrak{a}] \star E, E_B = [\mathfrak{b}] \star E$ and an elliptic curve E', decide whether $E' = E_{AB} = [\mathfrak{a}\mathfrak{b}] \star E$.

Orders in imaginary quadratic fields

$\mathcal{O}$ order in an imaginary quadratic number field:

$$\mathcal{O} = \mathbb{Z}[\omega] = \{a + b\omega : a, b \in \mathbb{Z}\}$$

for some ω satisfying a quadratic equation

$$x^2 - tx + q = 0$$

with discriminant $\Delta = t^2 - 4q < 0$.

Examples

Let p be a prime.

- the order $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$ has discriminant $\Delta = -4p$.
- the order $\mathcal{O} = \mathbb{Z}\left[\frac{1+\sqrt{-p}}{2}\right]$ has discriminant $\Delta = -p$ (if $p \equiv 3 \mod 4$).

Quadratic characters of the class group

Let $\mathcal{O}$ be an order of discriminant Δ in an imaginary quadratic field.
Write $\Delta = -2^a \cdot \prod_{i=1}^r m_i^{e_i}$ for distinct odd primes m_i.

Theorem (Genus theory)

All quadratic characters of $\mathrm{Cl}(\mathcal{O})$ *are given by (products of):*

- *for every odd prime m_i:*

$$\chi_m : \mathrm{Cl}(\mathcal{O}) \to \{\pm 1\} \qquad [\mathfrak{a}] \mapsto \left(\frac{\mathrm{norm}(\mathfrak{a})}{m}\right)$$

  where $\mathfrak{a}$ is any representative of $[\mathfrak{a}]$ satisfying $\gcd(m, \mathrm{norm}(\mathfrak{a})) = 1$.

- *Define* $\delta : \mathfrak{a} \mapsto (-1)^{(\mathrm{norm}(\mathfrak{a})-1)/2} \qquad \varepsilon : \mathfrak{a} \mapsto (-1)^{(\mathrm{norm}(\mathfrak{a})^2-1)/8}$

  if $\Delta = -4n$, extend the set of characters by

  1. δ *if* $n \equiv 1, 4, 5 \pmod 8$,
  2. ε *if* $n \equiv 6 \pmod 8$,
  3. $\delta\varepsilon$ *if* $n \equiv 2 \pmod 8$.

There is one relation between these characters:

$$\chi_{m_1}^{e_1} \cdot \dots \cdot \chi_r^{e_r} \cdot \delta^{\frac{b+1}{2} \bmod 2} \cdot \varepsilon^{a \bmod 2} \equiv 1 \quad \textit{on } \mathrm{Cl}(\mathcal{O})$$

Endomorphisms

E elliptic curve over $\mathbb{F}_q$. The rational endomorphism ring

$$\mathrm{End}_{\mathbb{F}_q}(E) = \{\mathbb{F}_q\text{-isogenies } \varphi : E \to E\} \cup \{0\}.$$

Frobenius endomorphism: for $E/\mathbb{F}_q$, given as

$$\begin{aligned} \pi : E &\longrightarrow E \\ (x, y) &\longmapsto (x^q, y^q). \end{aligned}$$

Fact: Elliptic curve $E/\mathbb{F}_q$ with $\#E(\mathbb{F}_q) = q + 1 - t$, then $t = \operatorname{tr} \pi$ and

$$\pi^2 - t\pi + q = 0.$$

Endomorphism ring dichotomy

$E/\mathbb{F}_q$ elliptic curve. Frobenius satisfies

$$\pi^2 - t\pi + q = 0.$$

But $|t| \leq 2\sqrt{q}$ so $t^2 - 4q \leq 0$.

Theorem (Waterhouse, Theorem 4.1):[1]

1. If $t^2 - 4q < 0$ then $\mathbb{Q}(\pi)$ is an imaginary quadratic field and

$$\mathrm{End}_{\mathbb{F}_q}(E) \hookrightarrow \mathbb{Q}(\pi) = \mathbb{Q}(\sqrt{t^2 - 4q})$$

   as an order $\mathcal{O}$ containing $\mathbb{Z}[\pi]$.

2. If $t^2 - 4q = 0$ then $\pi = \pm\sqrt{q} = \pm p^{n/2}$ and

$$\mathrm{End}_{\mathbb{F}_q}(E) \hookrightarrow B_{p,\infty}$$

   as a maximal order $\mathcal{O}$ in a quaternion algebra ramified only at p and ∞.

[1] Waterhouse's thesis: *Abelian varieties over finite fields*, 1969

CM action

E elliptic curve over $\mathbb{F}_q$ with $q+1-t$ points, $\Delta = t^2 - 4q \neq 0$, $\mathrm{End}_{\mathbb{F}_q}(E) = \mathcal{O}$ an order in an imaginary quadratic field $\mathbb{Q}(\pi)$ and $\mathcal{O}$ contains $\mathbb{Z}[\pi]$.

Fact: Any (invertible) ideal $\mathfrak{a}$ defines an isogeny of degree $\deg\varphi = \mathrm{norm}(\mathfrak{a})$:

$$\varphi : E \to [\mathfrak{a}] \star E.$$

$$\mathcal{E}\ell\ell(\mathcal{O}, t) = \{\, \text{elliptic curves } E/\mathbb{F}_q \,:\, \mathrm{End}_{\mathbb{F}_q}(E) \cong \mathcal{O} \text{ and } \mathrm{tr}(\pi) = t \,\}/\cong_{\mathbb{F}_q}.$$

The main theorem of complex multiplication:

For any $E, E' \in \mathcal{E}\ell\ell(\mathcal{O}, t)$ there exists a unique class $[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O})$ such that

$$E' = [\mathfrak{a}] \star E.$$

The group $\mathrm{Cl}(\mathcal{O})$ acts on $\mathcal{E}\ell\ell(\mathcal{O}, t)$ freely and transitively* by $([\mathfrak{a}], E) \mapsto [\mathfrak{a}] \star E$.

Problems in isogeny-based cryptography

The main problem for group-action isogeny protocols:
Given two elliptic curves $E, E' = [\mathfrak{a}] \star E$ connected by a secret ideal class $[\mathfrak{a}]$, obtain $[\mathfrak{a}]$.

Computational Diffie-Hellman problem:
Given three elliptic curves $E, E_A = [\mathfrak{a}] \star E, E_B = [\mathfrak{b}] \star E$ connected by secret ideal classes $[\mathfrak{a}], [\mathfrak{b}]$, compute $E_{AB} = [\mathfrak{a}\mathfrak{b}] \star E$.

'Decisional Diffie-Hellman problem' for group-action isogeny protocols:
Given elliptic curves $E, E_A = [\mathfrak{a}] \star E, E_B = [\mathfrak{b}] \star E$ and an elliptic curve E', decide whether $E' = E_{AB} = [\mathfrak{a}\mathfrak{b}] \star E$.

Problem we start with:
Given two elliptic curves $E, E' = [\mathfrak{a}] \star E$ connected by a secret ideal class $[\mathfrak{a}]$, obtain non-trivial information about $[\mathfrak{a}]$.

Isogenies and pairings

Elliptic curves E, E', unknown isogeny $\varphi : E \to E'$. Take some m.

The (reduced) Tate pairing (assume that $\mu_m \subset \mathbb{F}_q$):

$$\begin{aligned} T_m : \quad E(\mathbb{F}_q)[m] \times E(\mathbb{F}_q)/mE(\mathbb{F}_q) &\longrightarrow \mu_m \subset \mathbb{F}_q \\ (P, Q) &\longmapsto T_m(P, Q) \end{aligned}$$

is a non-degenerate bilinear pairing compatible with isogenies:

$$T_m(\varphi(P), \varphi(Q)) = T_m(P, Q)^{\deg(\varphi)}.$$

More on the Tate pairing

Elliptic curves E, E', unknown isogeny $\varphi : E \to E'$. Take some m.

Non-degenerate bilinear pairing compatible with isogenies:

$$T_m(\varphi(P), \varphi(Q)) = T_m(P, Q)^{\deg(\varphi)}.$$

Self-pairings

There can be non-trivial self-pairings $T_m(P, P) \neq 1$;

Use discrete logs

From P and $\varphi(P)$, we get $\deg(\varphi) \pmod{m}$.

Problems

The isogeny $\varphi : E \to E'$ is secret.

Quadratic characters of the class group

Let $\mathcal{O}$ be an order of discriminant Δ in an imaginary quadratic field.
Write $\Delta = -2^a \cdot b$ with $b = \prod_{i=1}^r m_i^{e_i}$ for distinct odd primes m_i.

Theorem (Genus theory)

All quadratic characters of $\mathrm{Cl}(\mathcal{O})$ *are given by (products of):*

- *for every odd prime m_i:*

$$\chi_m : \mathrm{Cl}(\mathcal{O}) \to \{\pm 1\} \qquad [\mathfrak{a}] \mapsto \left(\frac{\mathrm{norm}(\mathfrak{a})}{m}\right)$$

  where $\mathfrak{a}$ is any representative of $[\mathfrak{a}]$ satisfying $\gcd(m, \mathrm{norm}(\mathfrak{a})) = 1$.

- *Define* $\quad \delta : \mathfrak{a} \mapsto (-1)^{(\mathrm{norm}(\mathfrak{a})-1)/2} \qquad \varepsilon : \mathfrak{a} \mapsto (-1)^{(\mathrm{norm}(\mathfrak{a})^2-1)/8}$

  if $\Delta = -4n$, extend the set of characters by

  1. *δ if $n \equiv 1, 4, 5 \pmod 8$,*
  2. *ε if $n \equiv 6 \pmod 8$,*
  3. *$\delta\varepsilon$ if $n \equiv 2 \pmod 8$.*

There is one relation between these characters:

$$\chi_{m_1}^{e_1} \cdot \cdots \cdot \chi_r^{e_r} \cdot \delta^{\frac{b+1}{2} \bmod 2} \cdot \varepsilon^{a \bmod 2} \equiv 1 \quad \text{on } \mathrm{Cl}(\mathcal{O})$$

Genus theory consequences

$\mathcal{O}$ imaginary quadratic order with discriminant Δ.

For every odd prime $m \mid \Delta$, there is a quadratic character

$$\chi_m : \mathrm{Cl}(\mathcal{O}) \to \{\pm 1\} \qquad [\mathfrak{a}] \mapsto \left(\frac{\mathrm{norm}(\mathfrak{a})}{m} \right).$$

We can then write $\chi_m([\mathfrak{a}])$.

Non-trivial characters: whenever $\Delta \neq -m, -4m$ for a prime $m \equiv 3 \bmod 4$.

No non-trivial characters for CSIDH or CSURF.

Almost always non-trivial characters for ordinary curves or supersingular curves with $p \equiv 1 \bmod 4$.

Problem 2 taken care of.

Dealing with problem 1

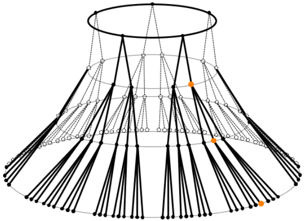
Assume now m prime and E ordinary.

We assumed $E(\mathbb{F}_q)[m]$ cyclic. What if $E(F_q)[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$?

Denote $E(\mathbb{F}_q)[m^\infty] = \{P \in E(\mathbb{F}_q) : P \text{ has order a power of } m\}$.

Isogeny volcanoes

By a sequence of isogenies, we can replace E with $\overline{E}$ with $\overline{E}(\mathbb{F}_q)[m^\infty]$ cyclic.



Isogeny volcano

Step back

$E, E' \in \mathcal{E}\ell\ell(\mathcal{O}, t)$ be elliptic curves with $E' = [\mathfrak{a}] \star E$.

If we have for an odd prime $m|\Delta$:

- such that χ_m is non-trivial,
  whenever $\Delta \neq -m, -4m$ for a prime $m \equiv 3 \bmod 4$
- there is a pair of points $P \in E(\mathbb{F}_q)[m]$ and $P' \in E'(\mathbb{F}_q)[m]$ satisfying $P \mapsto kP'$,
  e.g. whenever $E(\mathbb{F}_q)$ cyclic or reducing by using volcanoes to this case
- and the self-pairing $T_m(P, P) \neq 1$ is non-trivial,

then we can compute

$$\chi_m([\mathfrak{a}]) = \left(\frac{\mathrm{norm}(\mathfrak{a})}{m}\right)$$

just from the elliptic curves E and E'.

New exciting work

Castryck, Houben, Vercauteren, Wesolowski
`ia.cr/2022/345`

- Play the same game for $\mathcal{O}$-oriented curves
- Oriented curves form **infinite** volcanoes
- Fixable using ‘distortion maps’ and the Weil pairing

Conclusions

1. We can compute characters $\chi_m([\mathfrak{a}])$ and the even modulus characters $\delta, \epsilon, \delta\epsilon$, directly from the elliptic curves $E, E' = [\mathfrak{a}] \star E$.

2. Use any character χ to break DDH:
   Given three elliptic curves E_A, E_B, E' with $E_A = [\mathfrak{a}] \star E_0, E_B = [\mathfrak{b}] \star E_0$ obtained by the Diffie-Hellman protocol, decide whether $E' = E_{AB} = [\mathfrak{a}\mathfrak{b}] \star E_0$.
   - From E_A and E_0 compute $\chi([\mathfrak{a}])$,
   - Compute the character from E' and E_B and check whether it is equal to $\chi([\mathfrak{a}])$.

3. The attack works in polynomial time in $\log p$ whenever Δ has a small factor: heuristically almost always,

4. Only use $\mathcal{O}$ with odd class group to avoid this attack $\Rightarrow$ use CSIDH, CSURF.

Thanks for your attention!

Breaking the decisional Diffie-Hellman problem for class group actions using genus theory

Wouter Castryck and Jana Sotáková and Frederik Vercauteren

`https://eprint.iacr.org/2020/151`

`jana-sotakova.github.io`