Extending class group action attacks via sesquilinear pairings

Joseph Macula, CU Boulder
Joint work with Katherine Stange

Asiacrypt 2024

Background

- E a supersingular elliptic curve over finite field $\mathbb{F}$, $\mathrm{char}(\mathbb{F}) = p$, K an imaginary quadratic field, $\mathcal{O}$ an order in K

Background

- E a supersingular elliptic curve over finite field $\mathbb{F}$, $\mathrm{char}(\mathbb{F}) = p$, K an imaginary quadratic field, $\mathcal{O}$ an order in K
- A *K-orientation* of E is an embedding

$$\iota : K \hookrightarrow \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q} \cong B_{p,\infty}$$

If $\iota(\mathcal{O}) \subset \mathrm{End}(E)$, ι is an *$\mathcal{O}$-orientation*
If $\iota(\mathcal{O}) = \iota(K) \cap \mathrm{End}(E)$, ι is a *primitive* $\mathcal{O}$-orientation

Background

- E a supersingular elliptic curve over finite field $\mathbb{F}$, $\mathrm{char}(\mathbb{F}) = p$, K an imaginary quadratic field, $\mathcal{O}$ an order in K
- A *K-orientation* of E is an embedding

$$\iota : K \hookrightarrow \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q} \cong B_{p,\infty}$$

  If $\iota(\mathcal{O}) \subset \mathrm{End}(E)$, ι is an *$\mathcal{O}$-orientation*
  If $\iota(\mathcal{O}) = \iota(K) \cap \mathrm{End}(E)$, ι is a *primitive* $\mathcal{O}$-orientation
- We denote a supersingular curve E with a K-orientation ι by (E, ι)

Background

- $SS_{\mathcal{O}}^{pr} := \{(E, \iota) : \iota \text{ a primitive } \mathcal{O}\text{-orientation}\}/\sim$

Background

- $SS_{\mathcal{O}}^{pr} := \{(E, \iota) : \iota \text{ a primitive } \mathcal{O}\text{-orientation}\}/\sim$
- Given $(E, \iota) \in SS_{\mathcal{O}}^{pr}$, $[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O})$, define

$$E[\mathfrak{a}] = \bigcap_{\alpha \in \mathfrak{a}} \ker(\iota(\alpha))$$

Then there exists K-oriented isogeny $\varphi_{\mathfrak{a}}$ with kernel $E[\mathfrak{a}]$. This gives an action of $\mathrm{Cl}(\mathcal{O})$ on $SS_{\mathcal{O}}^{pr}$ by

$$[\mathfrak{a}] \cdot (E, \iota) = (E/E[\mathfrak{a}], \iota_{\mathfrak{a}}), \iota_{\mathfrak{a}} = \frac{1}{\deg \varphi_{\mathfrak{a}}} \varphi_{\mathfrak{a}} \circ \iota \circ \hat{\varphi}_{\mathfrak{a}}$$

Background

- The *vectorization problem*:

$$\text{Given a fixed orbit } X \text{ in } SS_{\mathcal{O}}^{pr},\ (E,\iota),(E',\iota') \in X,$$
$$\text{find } [\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O}) \text{ such that } [\mathfrak{a}] \cdot (E,\iota) = (E',\iota')$$

Motivating Question

- SIDH no longer secure, as shown by Castryck and Decru (23), Robert (23), Maino and Martindale (22), and Maino-Martindale-Panny-Pope-Wesolowski (23)

Motivating Question

- SIDH no longer secure, as shown by Castryck and Decru (23), Robert (23), Maino and Martindale (22), and Maino-Martindale-Panny-Pope-Wesolowski (23)
- (Castryck, Houben, Merz, Mula, Buuren, Vercauteren 23): Can this attack be applied to instances of the vectorization problem?

An Instructive Example (from CHM+ 23):

Assume: E, E' defined over $\mathbb{F}_p$, both with primitive orientation by $\mathbb{Z}[\sqrt{-p}]$; $\phi : E \to E'$ a secret $\mathbb{F}_p$-rational isogeny with $\ker\phi = E[\mathfrak{a}]$; $\deg\phi = d$ known; $[\mathfrak{a}] \in \mathrm{Cl}(\mathbb{Z}[\sqrt{-p}])$. Knowledge of $[\mathfrak{a}]$ reduces to knowledge of ϕ.

- With $m = \ell^r$, $(\ell, d) = 1$, ℓ a small prime splitting in $\mathbb{Q}(\sqrt{-p})$, there are bases $\{P, Q\}, \{P', Q'\}$ for $E[m], E'[m]$, respectively, and

$$P' = \lambda\phi(P), \quad Q' = \mu\phi(Q), \quad \lambda, \mu \in \mathbb{Z}/m\mathbb{Z}^*$$

An Instructive Example (from CHM+ 23):

Assume: E, E' defined over $\mathbb{F}_p$, both with primitive orientation by $\mathbb{Z}[\sqrt{-p}]$; $\phi : E \to E'$ a secret $\mathbb{F}_p$-rational isogeny with $\ker\phi = E[\mathfrak{a}]$; $\deg\phi = d$ known; $[\mathfrak{a}] \in \mathrm{Cl}(\mathbb{Z}[\sqrt{-p}])$. Knowledge of $[\mathfrak{a}]$ reduces to knowledge of ϕ.

- With $m = \ell^r$, $(\ell, d) = 1$, ℓ a small prime splitting in $\mathbb{Q}(\sqrt{-p})$, there are bases $\{P, Q\}, \{P', Q'\}$ for $E[m], E'[m]$, respectively, and

$$P' = \lambda\phi(P), \quad Q' = \mu\phi(Q), \quad \lambda, \mu \in \mathbb{Z}/m\mathbb{Z}^*$$

- Properties of the m-Weil pairing $e_m(\cdot,\cdot)$ imply

$$e_m(P', P') = e_m(P, P)^{\lambda^2 d}$$

An Instructive Example (from CHM+ 23):

Assume: E, E' defined over $\mathbb{F}_p$, both with primitive orientation by $\mathbb{Z}[\sqrt{-p}]$; $\phi : E \to E'$ a secret $\mathbb{F}_p$-rational isogeny with $\ker \phi = E[\mathfrak{a}]$; $\deg \phi = d$ known; $[\mathfrak{a}] \in \mathrm{Cl}(\mathbb{Z}[\sqrt{-p}])$. Knowledge of $[\mathfrak{a}]$ reduces to knowledge of ϕ.

- With $m = \ell^r$, $(\ell, d) = 1$, ℓ a small prime splitting in $\mathbb{Q}(\sqrt{-p})$, there are bases $\{P, Q\}, \{P', Q'\}$ for $E[m], E'[m]$, respectively, and

$$P' = \lambda\phi(P), \quad Q' = \mu\phi(Q), \quad \lambda, \mu \in \mathbb{Z}/m\mathbb{Z}^*$$

- Properties of the m-Weil pairing $e_m(\cdot, \cdot)$ imply

$$e_m(P', P') = e_m(P, P)^{\lambda^2 d}$$

- Unfortunately, $e_m(P, P) = 1$

Self-Pairings

- Search for pairings non-degenerate on a cyclic subgroup of E compatible with oriented isogenies

Self-Pairings

- Search for pairings non-degenerate on a cyclic subgroup of E compatible with oriented isogenies
- CHM+ construct such pairings. This yields efficient attacks on the vectorization problem when
  (i) The degree of the secret isogeny is known
  (ii) The discriminant $\Delta_{\mathcal{O}}$ of the primitive order contains a large smooth square factor
  (iii) To perform the necessary computations, may need to significantly extend the base field

  (N.B.: work in preparation by Castryck, Decru, Maino, Martindale, Panny, Pope, Robert, Wesolowski appears to remove the square part of condition (ii))

Sesquilinear Pairings

Can be defined purely formally, thus even for curves without CM ("Sesquilinear Pairings on Elliptic Curves", Stange, 2024)

First steps

- Given an imaginary quadratic order $\mathcal{O} = \mathbb{Z}[\tau]$, let ρ be the left-regular representation of $\mathcal{O}$ acting on basis $\{1, \tau\}$:

$$\rho(\alpha) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \iff \alpha = a + c\tau, \alpha\tau = b + d\tau$$

Sesquilinear Pairings

Can be defined purely formally, thus even for curves without CM ("Sesquilinear Pairings on Elliptic Curves", Stange, 2024)

First steps

- Given an imaginary quadratic order $\mathcal{O} = \mathbb{Z}[\tau]$, let ρ be the left-regular representation of $\mathcal{O}$ acting on basis $\{1, \tau\}$:

$$\rho(\alpha) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \iff \alpha = a + c\tau, \alpha\tau = b + d\tau$$

- Define action of $\mathcal{O}$ on $(\mathbb{F}^*)^{\times 2}$ by $(x, y)^\alpha = (x^a y^b, x^c y^d)$

Sesquilinear Pairings

Let $E/\mathbb{F}$ have CM by $\mathcal{O}$. Given $\alpha \in \mathcal{O}$, we construct a pairing

$$\widehat{T}_\alpha^\tau : E[\overline{\alpha}](\mathbb{F}) \times E(\mathbb{F})/[\alpha]E(\mathbb{F}) \to (\mathbb{F}^*)^{\times 2}/((\mathbb{F}^*)^{\times 2})^\alpha$$

as follows:

With $\rho(\alpha) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$,

$$\alpha = a + c\tau, \alpha\tau = b + d\tau, \overline{\alpha} = d - c\tau, \overline{\alpha}\tau = -b + a\tau$$

- Take $P \in E[\overline{\alpha}]$, define functions $f_{P,1}, f_{P,2}$ such that

$$\mathrm{div}(f_{P,1}) = a([-\tau]P) + b(P) - (a+b)(\infty)$$
$$\mathrm{div}(f_{P,2}) = c([-\tau]P) + d(P) - (c+d)(\infty)$$

Sesquilinear Pairings

- Define for $Q \in E(\mathbb{F})$,

  $$D_{Q,1} = ([-\tau]Q + [-\tau]R) - ([-\tau]R), \quad D_{Q,2} = (Q + R) - (R).$$

  with R chosen so that the supports of $\mathrm{div}(f_{P,i})$ and $D_{Q,j}$ are disjoint for each pair i, j

Sesquilinear Pairings

- Define for $Q \in E(\mathbb{F})$,

  $$D_{Q,1} = ([-\tau]Q + [-\tau]R) - ([-\tau]R), \quad D_{Q,2} = (Q + R) - (R).$$

  with R chosen so that the supports of $\mathrm{div}(f_{P,i})$ and $D_{Q,j}$ are disjoint for each pair i, j
- Then $\widehat{T}_{\alpha}^{\tau}(P, Q) =$

  $$(f_{P,1}(D_{Q,1}), f_{P,2}(D_{Q,1}))\,(f_{P,1}(D_{Q,2}), f_{P,2}(D_{Q,2}))^{\overline{\tau}}$$

Sesquilinear Pairings

- Define for $Q \in E(\mathbb{F})$,

$$D_{Q,1} = ([-\tau]Q + [-\tau]R) - ([-\tau]R), \quad D_{Q,2} = (Q + R) - (R).$$

with R chosen so that the supports of $\mathrm{div}(f_{P,i})$ and $D_{Q,j}$ are disjoint for each pair i, j

- Then $\widehat{T}_{\alpha}^{\tau}(P, Q) =$

$$(f_{P,1}(D_{Q,1}), f_{P,2}(D_{Q,1}))\,(f_{P,1}(D_{Q,2}), f_{P,2}(D_{Q,2}))^{\overline{\tau}}$$

- Unwinding the definitions, this turns out to be a somewhat natural extension of the Tate pairing; $\widehat{T}_{\alpha}^{\tau}(P, Q) = f_P(D_Q)$ for $f_P = f_{P,1}f_{P,2}^{\tau}$, $D_Q = D_{Q,1} + \tau \cdot D_{Q,2}$ (see Stange, 2024)

Sesquilinear Pairings

Theorem (Stange 2024):

The pairing above is well-defined and satisfies

- **Sesquilinearity:** For $P \in E[\overline{\alpha}](\mathbb{F})$ and $Q \in E(\mathbb{F})$,

$$\widehat{T}_{\alpha}^{\tau}([\gamma]P, [\delta]Q) = \widehat{T}_{\alpha}^{\tau}(P, Q)^{\overline{\gamma}\delta}.$$

Sesquilinear Pairings

Theorem (Stange 2024):

The pairing above is well-defined and satisfies

- **Sesquilinearity:** For $P \in E[\overline{\alpha}](\mathbb{F})$ and $Q \in E(\mathbb{F})$,

$$\widehat{T}_{\alpha}^{\tau}([\gamma]P, [\delta]Q) = \widehat{T}_{\alpha}^{\tau}(P, Q)^{\overline{\gamma}\delta}.$$

- **Compatibility:** $\phi : E \to E'$ $\mathcal{O}$-oriented, $P \in E[\overline{\alpha}](\mathbb{F})$ and $Q \in E(\mathbb{F})$,

$$\widehat{T}_{\alpha}^{\tau}(\phi P, \phi Q) = \widehat{T}_{\alpha}^{\tau}(P, Q)^{\deg \phi}.$$

Sesquilinear Pairings

Theorem (Stange 2024):

The pairing above is well-defined and satisfies

- **Sesquilinearity:** For $P \in E[\overline{\alpha}](\mathbb{F})$ and $Q \in E(\mathbb{F})$,

$$\widehat{T}_\alpha^\tau([\gamma]P, [\delta]Q) = \widehat{T}_\alpha^\tau(P, Q)^{\overline{\gamma}\delta}.$$

- **Compatibility:** $\phi : E \to E'$ $\mathcal{O}$-oriented, $P \in E[\overline{\alpha}](\mathbb{F})$ and $Q \in E(\mathbb{F})$,

$$\widehat{T}_\alpha^\tau(\phi P, \phi Q) = \widehat{T}_\alpha^\tau(P, Q)^{\deg \phi}.$$

- **Non-degeneracy:** $\alpha \in \mathcal{O}$ coprime to $\mathrm{char}(\mathbb{F})$ and $\Delta_{\mathcal{O}}$. $N = N(\alpha)$, $\mathbb{F}$ contains the N-th roots of unity, $P \in E[N](\mathbb{F})$ such that $\mathcal{O}P = E[N] = E[N](\mathbb{F})$. Then

$$\widehat{T}_\alpha^\tau : E[\overline{\alpha}](\mathbb{F}) \times E(\mathbb{F})/[\alpha]E(\mathbb{F}) \to (\mathbb{F}^*)^{\times 2}/((\mathbb{F}^*)^{\times 2})^{\alpha},$$

is non-degenerate.

Sesquilinear Pairings

These pairings are efficiently computable via a Miller-style algorithm (Algorithm 5.7, Stange, 2024)

Similar to the Tate pairing, a final exponentiation gives values in the roots of unity:

$$(\overline{\mathbb{F}}^*)/(\overline{\mathbb{F}}^*)^\alpha \to \mu_{N(\alpha)}^{\times 2} \subseteq (\overline{\mathbb{F}}^*)^{\times 2}, \quad x \mapsto x^{(q-1)\alpha^{-1}}.$$

Sesquilinear Pairings

Key idea:

Sesquilinear pairings respect $\mathcal{O}$-module structure, not merely $\mathbb{Z}$-module structure. This yields new instances of non-trivial self-pairings.

Sesquilinear Pairings

Recall that in the statement of non-degeneracy of $\widehat{T}_{\alpha}^{\tau}$, one condition is that $E[N]$ is a cyclic $\mathcal{O}$-module, where $N = N(\alpha)$. A straightforward extension of results of (Lenstra, 1996) yields:

Sesquilinear Pairings

Recall that in the statement of non-degeneracy of $\widehat{T}_{\alpha}^{\tau}$, one condition is that $E[N]$ is a cyclic $\mathcal{O}$-module, where $N = N(\alpha)$. A straightforward extension of results of (Lenstra, 1996) yields:

- Theorem (M., Stange): $E/\mathbb{F}$, K imaginary quadratic, $\mathcal{O} \subset K$, E $\mathcal{O}$-oriented, $f = [\mathcal{O}' : \mathcal{O}]$, $\mathcal{O}'$ primitive orientation. $E[m]$ cyclic $\mathcal{O}$-module iff $(m, f) = 1$.

Sesquilinear Pairings

So, there many instances where $\widehat{T}_\alpha^\tau$ is non-degenerate. This in turn yields non-degenerate self-pairings.

Theorem (M., Stange):

Let E be an elliptic curve oriented by $\mathcal{O} = \mathbb{Z}[\tau]$. Let m be coprime to the discriminant $\Delta_{\mathcal{O}}$. Let $\mathbb{F}$ be a finite field containing the m-th roots of unity. Suppose $E[m] = E[m](\mathbb{F})$. Let P have order m. Let s be the maximal divisor of m such that $E[s] \subseteq \mathcal{O}P$. Then the multiplicative order m' of $\widehat{T}_m^\tau(P, P)$ satisfies $s \mid m' \mid 2s^2$.

In particular, if $\mathcal{O}P = E[m]$, then $s = m$ and the self-pairing has order m. If $\mathcal{O}P = \mathbb{Z}P$, then $s = 1$, and in fact, in this case, the self-pairing is trivial.

Computational Assumptions

- Efficient = polynomial in size of input, i.e., polynomial in $\log m$ (the torsion) and $\log q$ (q the cardinality of base field where $E[m]$ fully rational)

Computational Assumptions

- Efficient = polynomial in size of input, i.e., polynomial in $\log m$ (the torsion) and $\log q$ (q the cardinality of base field where $E[m]$ fully rational)
- Having an $\mathcal{O}$-oriented curve means having an explicit orientation; given $\alpha \in \mathcal{O}$, can compute its action $[\alpha]$ on a point P on E efficiently

Computational Assumptions

- Efficient $=$ polynomial in size of input, i.e., polynomial in $\log m$ (the torsion) and $\log q$ (q the cardinality of base field where $E[m]$ fully rational)
- Having an $\mathcal{O}$-oriented curve means having an explicit orientation; given $\alpha \in \mathcal{O}$, can compute its action $[\alpha]$ on a point P on E efficiently
- Degree d of hidden isogeny ϕ is known

Computational Assumptions

- Efficient = polynomial in size of input, i.e., polynomial in $\log m$ (the torsion) and $\log q$ (q the cardinality of base field where $E[m]$ fully rational)
- Having an $\mathcal{O}$-oriented curve means having an explicit orientation; given $\alpha \in \mathcal{O}$, can compute its action $[\alpha]$ on a point P on E efficiently
- Degree d of hidden isogeny ϕ is known
- m is coprime to the characteristic p of the given field $\mathbb{F}$, and m is smooth, meaning that its factors are polynomial in size, so that discrete logarithms in μ_m or $E[m]$ are computable in polynomial time. In particular, we can efficiently write any element of $E[m]$ in terms of a given basis

Extending Prior Attacks

A slight modification of the sesquilinear pairing:

$$T'_m(P, Q) = (t_m([\tau]P, Q), t_m(P, Q))$$

This pairing remains non-degenerate whenever $E[m]$ is a cyclic $\mathcal{O}$-module, bilinear, compatible with $\mathcal{O}$-oriented isogenies. It yields the following result

Theorem (M., Stange):

Suppose $\phi : E \to E'$ of degree d, $m \mid \Delta_{\mathcal{O}}$, coprime to d, polynomially many square roots of 1 modulo m. $P \in E[m]$ and $P' \in E'[m]$ such that $\mathcal{O}P = E[m]$, $\mathcal{O}P' = E'[m]$. There exists efficiently computable point $Q \in E[m]$ of order m with $S \subset E'[m]$ of polynomial size containing $\phi(Q)$ computable in polynomially many operations in field of definition of $E[m]$.

Extending Prior Attacks

- With knowledge of $\phi(Q)$ for an order m point Q, $\mathcal{O}$-module structure of $E[m]$ and ϕ an $\mathcal{O}$-oriented isogeny yield knowledge of ϕ on $E[m]$.

Extending Prior Attacks

- With knowledge of $\phi(Q)$ for an order m point Q, $\mathcal{O}$-module structure of $E[m]$ and ϕ an $\mathcal{O}$-oriented isogeny yield knowledge of ϕ on $E[m]$.
- By exploiting $\mathcal{O}$-module structure, computations take place over field of definition of $E[m]$ instead of $E[m^2]$. This yields polynomial-time attacks on additional instances of the vectorization problem.

Extending Prior Attacks

Proof (Sketch, for m odd):

- $\exists \tau \in \mathcal{O}$ s.t. $\mathbb{Z}[\tau] \equiv \mathcal{O}$ modulo m; $Tr(\tau) \equiv N(\tau) \equiv 0 \pmod{m}$

Extending Prior Attacks

Proof (Sketch, for m odd):

- $\exists \tau \in \mathcal{O}$ s.t. $\mathbb{Z}[\tau] \equiv \mathcal{O}$ modulo m; $Tr(\tau) \equiv N(\tau) \equiv 0 \pmod{m}$
- $T'_m(P, P)^{\deg \phi} = T'_m(P', P')^{N(\lambda)}$

Extending Prior Attacks

Proof (Sketch, for m odd):

- $\exists \tau \in \mathcal{O}$ s.t. $\mathbb{Z}[\tau] \equiv \mathcal{O}$ modulo m; $Tr(\tau) \equiv N(\tau) \equiv 0 \pmod{m}$
- $T'_m(P, P)^{\deg \phi} = T'_m(P', P')^{N(\lambda)}$
- $\lambda \equiv a + b\tau$ modulo m, $N(\lambda) \equiv a^2 \pmod{m'}$, so $\phi[\tau]P = [a][\tau]P'$ for some a

Extending Prior Attacks

Proof (Sketch, for m odd):

- $\exists \tau \in \mathcal{O}$ s.t. $\mathbb{Z}[\tau] \equiv \mathcal{O}$ modulo m; $Tr(\tau) \equiv N(\tau) \equiv 0 \pmod{m}$
- $T'_m(P, P)^{\deg \phi} = T'_m(P', P')^{N(\lambda)}$
- $\lambda \equiv a + b\tau$ modulo m, $N(\lambda) \equiv a^2 \pmod{m'}$, so $\phi[\tau]P = [a][\tau]P'$ for some a
- Our assumptions imply set of possible values of a is efficiently computable and of polynomial size

Extending Prior Attacks

Example (adapted from Castryck):

$E : y^2 = x^3 + x$, $p = 4 \cdot 3^r - 1$. Then $j(E) = 1728$ and E is supersingular. With π_p the Frobenius endomorphism, $[i] : (x, y) \mapsto (-x, iy)$,

$$\tau := \frac{i + \pi_p}{2} \in \mathrm{End}(E).$$

$N(\tau) = 3^r$ and $Tr(\tau) = 0$. Let $\mathcal{O} = \mathbb{Z}[\tau]$, so $N(\tau) \mid \Delta_{\mathcal{O}}$. Let $m = 3^r$. Then $m \mid \Delta_{\mathcal{O}}$. $E(\mathbb{F}_{p^2}) \cong (\mathbb{Z}/4 \cdot 3^r\mathbb{Z})^2$, so $E[3^r] \subset E(\mathbb{F}_{p^2})$. All pairings computations take place in $E(\mathbb{F}_{p^2})$; with $m > 4d$, SIDH portion of attack is efficient.

- This is in contrast to methods of CHM+23, where a base change to field of definition of $E[3^{2r}]$ is required. This degree grows exponentially with r.

Thank you!