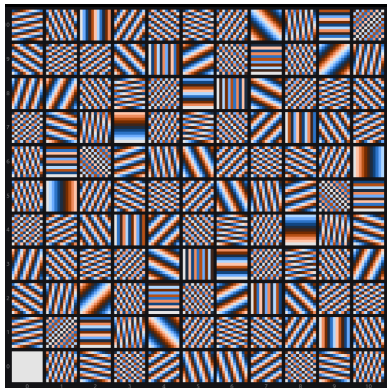
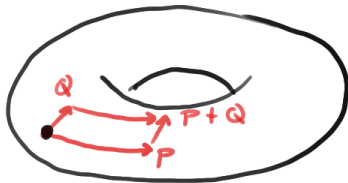
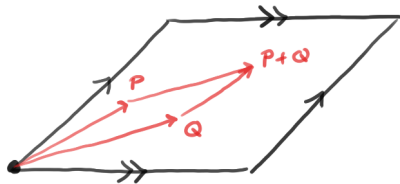
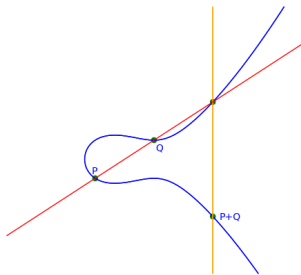


Pairings in Cryptography

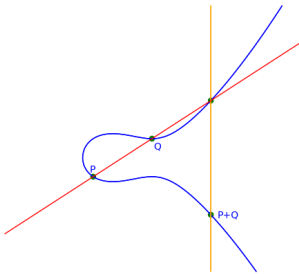


Katherine E. Stange
NuTMiC, September 22, 2026

This is a talk about elliptic curves...



... which are useful for cryptography ...



Given P and nP , what is n ?

... and about pairings

Given abelian groups G_1, G_2, G_3 , a **bilinear** map:

$$\langle \cdot, \cdot \rangle : G_1 \times G_2 \rightarrow G_3$$

$$(P, Q) \mapsto \langle P, Q \rangle$$

with

$$\langle P_1 + P_2, Q \rangle = \langle P_1, Q \rangle \langle P_2, Q \rangle$$

$$\langle P, Q_1 + Q_2 \rangle = \langle P, Q_1 \rangle \langle P, Q_2 \rangle$$

Weil and Tate pairings

E = elliptic curve, K = field, $E[m] = m$ -torsion, $\mu_m = m$ th roots of unity

Weil pairing:

$$e_m : E(K)[m] \times E(K)[m] \rightarrow \mu_m$$

Tate pairing:

$$t_m : E(K)[m] \times E(K)/mE(K) \rightarrow K^*/(K^*)^m$$

Destructive

- ▶ Discrete logarithm in $\mathbb{F}_q^*$: subexponential runtime (index calculus)

Destructive

- ▶ Discrete logarithm in $\mathbb{F}_q^*$: subexponential runtime (index calculus)
- ▶ Discrete logarithm on an elliptic curve E : exponential runtime (generic group algorithms)

Destructive

- ▶ Discrete logarithm in $\mathbb{F}_q^*$: subexponential runtime (index calculus)
- ▶ Discrete logarithm on an elliptic curve E : exponential runtime (generic group algorithms)
- ▶ Transfer from E to $\mathbb{F}_q^*/(\mathbb{F}_q^*)^m$:

$$t_m(R, nP) = t_m(R, P)^n$$

Destructive

- ▶ Discrete logarithm in $\mathbb{F}_q^*$: subexponential runtime (index calculus)
- ▶ Discrete logarithm on an elliptic curve E : exponential runtime (generic group algorithms)
- ▶ Transfer from E to $\mathbb{F}_q^*/(\mathbb{F}_q^*)^m$:

$$t_m(R, nP) = t_m(R, P)^n$$

- ▶ Only useful if $\mathbb{F}_q^*/(\mathbb{F}_q^*)^m$ and the result are non-trivial!

Destructive

- ▶ Discrete logarithm in $\mathbb{F}_q^*$: subexponential runtime (index calculus)
- ▶ Discrete logarithm on an elliptic curve E : exponential runtime (generic group algorithms)
- ▶ Transfer from E to $\mathbb{F}_q^*/(\mathbb{F}_q^*)^m$:

$$t_m(R, nP) = t_m(R, P)^n$$

- ▶ Only useful if $\mathbb{F}_q^*/(\mathbb{F}_q^*)^m$ and the result are non-trivial!
- ▶ Menezes-Okamoto-Vanstone attack (1991)

Constructive

- ▶ Joux (2000): Tripartite Diffie-Hellman (1 round)
- ▶ Boneh-Lynn-Shacham (2001): Signatures
- ▶ Boneh-Franklin (2001): Identity-based encryption

Multilinear?

Multilinear maps $\langle P, Q, R \rangle$ on DLP-hard groups, which are efficient and non-degenerate?

Would allow for:

- ▶ multi-party key exchange
- ▶ broadcast encryption
- ▶ verifiable pseudorandom functions
- ▶ functional encryption
- ▶ indistinguishability obfuscation
- ▶ etc.

There are now some partial candidates...

Post-quantum?

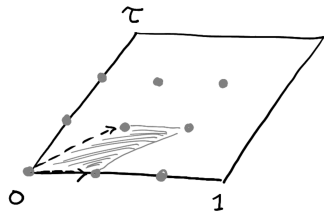
How do we build these pairings and functionalities in the age of quantum computers?

Interpretation One: Independence (Weil pairing over $\mathbb{C}$)

Weil pairing over $\mathbb{C}$ (Galbraith has nice notes):

Let 1 and τ form a basis for Λ giving $E \cong \mathbb{C}/\Lambda$:

$$e_m\left(\frac{a+b\tau}{m}, \frac{c+d\tau}{m}\right) = e^{2\pi i \frac{ad-bc}{m}}.$$



Interpretation Two: Monodromy in Extensions

An extension

$$0 \longrightarrow \mathbb{G}_m \longrightarrow X \longrightarrow E \longrightarrow 0$$

is given by a factor set

$$s : E \times E \rightarrow \mathbb{G}_m$$

determining the group law on X via

$$(x, P)(y, Q) = (xy s(P, Q), P + Q).$$

Monodromy

A group fact in E ,

$$\sum P_i = \mathcal{O},$$

Monodromy

A group fact in E ,

$$\sum P_i = \mathcal{O},$$

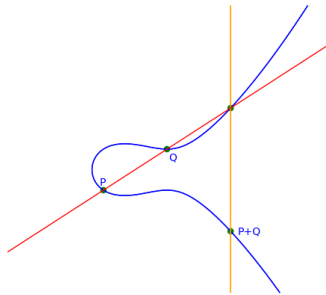


a monodromy $\alpha \in K^*$:

$$\sum (x_i, P_i) = ((\prod x_i) \alpha, \mathcal{O}).$$

From point to extension

Given a computation $P + Q$ with the group law, there's a function $f_{P,Q} : E \rightarrow \mathbb{P}^1$ with poles at P and Q and zeroes at $P + Q$ and $\mathcal{O}$.



$$\operatorname{div}(f_{P,Q}) = (P + Q) - (P) - (Q) + (\mathcal{O})$$

Let $Q \in E$. Then we can define a group extension X_Q by factor set

$$s(P_1, P_2) = f_{P_1, P_2}(Q + X) / f_{P_1, P_2}(X).$$

where X is an auxiliary point.

Monodromy

Fixing Q in E , we have an extension X_Q .

If $P \in E[m]$, then the group fact $mP = \mathcal{O}$ gives a monodromy on X_Q .

This is the Tate pairing $t_m(P, Q)$.

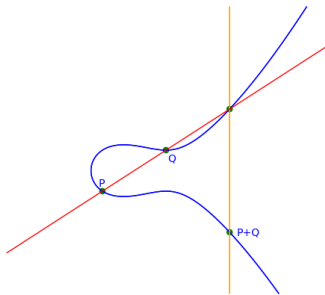
The Weil pairing is the quotient:

$$e_m(P, Q) = \frac{\text{monodromy of } mP = \mathcal{O} \text{ on } X_Q}{\text{monodromy of } mQ = \mathcal{O} \text{ on } X_P}$$

Tate pairing computation

$$t_m(P, Q) = f_P(D_Q), \quad \text{div}(f_P) = m(P) - m(\mathcal{O}), \quad D_Q = (Q + S) - (S).$$

$$t_m(P, Q) = \frac{f_P(Q + S)}{f_P(S)}$$

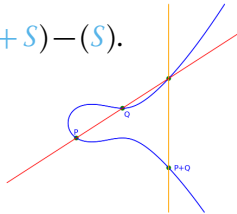


$$\text{div}(f_{P,Q}) = (P + Q) - (P) - (Q) + (\mathcal{O})$$

Tate pairing computation (Miller's algorithm)

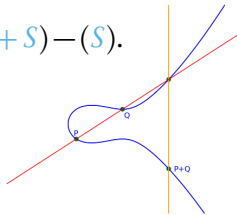
$$t_m(P, Q) = f_P(D_Q), \quad \text{div}(f_P) = m(P) - m(\mathcal{O}), \quad D_Q = (Q + S) - (S).$$

1. Create double-and-add chain of operations $k_1 + k_2$ for m .



Tate pairing computation (Miller's algorithm)

$$t_m(P, Q) = f_P(D_Q), \quad \operatorname{div}(f_P) = m(P) - m(\mathcal{O}), \quad D_Q = (Q + S) - (S).$$



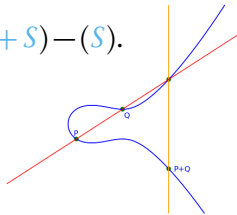
1. Create double-and-add chain of operations $k_1 + k_2$ for m .

2. This

gives a double-and-add chain of divisors $D_k := k(P) - ([k]P) - (k-1)(\mathcal{O})$ satisfying $D_{k_1} + D_{k_2} \sim D_{k_1+k_2}$. Note that $\operatorname{div}(f_P) = D_m$.

Tate pairing computation (Miller's algorithm)

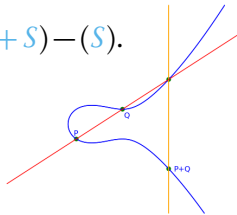
$$t_m(P, Q) = f_P(D_Q), \quad \text{div}(f_P) = m(P) - m(\mathcal{O}), \quad D_Q = (Q + S) - (S).$$



1. Create double-and-add chain of operations $k_1 + k_2$ for m .
2. This gives a double-and-add chain of divisors $D_k := k(P) - ([k]P) - (k-1)(\mathcal{O})$ satisfying $D_{k_1} + D_{k_2} \sim D_{k_1+k_2}$. Note that $\text{div}(f_P) = D_m$.
3. Each step $D_{k_1+k_2} - D_{k_1} - D_{k_2} = ([k_1]P) + ([k_2]P) - ([k_1+k_2]P) - (\mathcal{O})$ is an instance of the group law, i.e. rational function f_{k_1, k_2}^{-1} . Thus $f_P = \prod f_{k_{i,1}, k_{i,2}}^{-1}$.

Tate pairing computation (Miller's algorithm)

$$t_m(P, Q) = f_P(D_Q), \quad \text{div}(f_P) = m(P) - m(\mathcal{O}), \quad D_Q = (Q + S) - (S).$$



1. Create double-and-add chain of operations $k_1 + k_2$ for m .
2. This gives a double-and-add chain of divisors $D_k := k(P) - ([k]P) - (k-1)(\mathcal{O})$ satisfying $D_{k_1} + D_{k_2} \sim D_{k_1+k_2}$. Note that $\text{div}(f_P) = D_m$.
3. Each step $D_{k_1+k_2} - D_{k_1} - D_{k_2} = ([k_1]P) + ([k_2]P) - ([k_1+k_2]P) - (\mathcal{O})$ is an instance of the group law, i.e. rational function f_{k_1, k_2}^{-1} . Thus $f_P = \prod f_{k_{i,1}, k_{i,2}}^{-1}$.
4. Compute the double-and-add chain to compute $f_P(D_Q) = \prod f_{k_{i,1}, k_{i,2}}(D_Q)^{-1}$ (always evaluated, i.e. elements of K^*).

Isogenies

A group homomorphism between elliptic curves is called an *isogeny* if it is realized as rational functions.

Example

Modulo 11, there is an isogeny from $y^2 = x^3 + 1$ to $y^2 = x^3 + 6$, given by

$$(x, y) \mapsto \left(\frac{x^3 + 4}{x^2}, \frac{x^3 y + 3y}{x^3} \right)$$

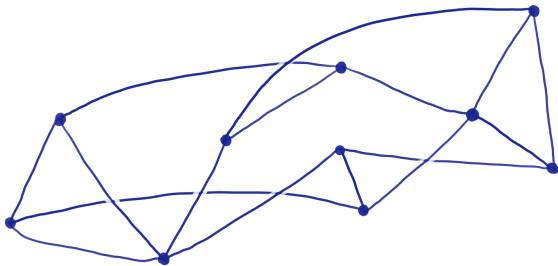
with kernel

$$\{(0, 1), (0, 10), id\}.$$

The *degree* of the isogeny is the cardinality of its kernel. (e.g. this is a 3-isogeny)

Isogeny graphs

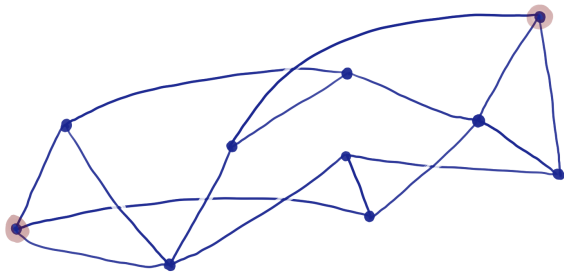
- ▶ vertices = supersingular elliptic curves over $\mathbb{F}_{p^2}$ (up to iso)
 - ▶ label: $j = 1728 \frac{4a^3}{4a^3 + 27b^2}$, isomorphism invariant
- ▶ edges = E and E' connected by an ℓ -isogeny
 - ▶ label: kernel of isogeny



Isogeny hard problem

Hard Problem

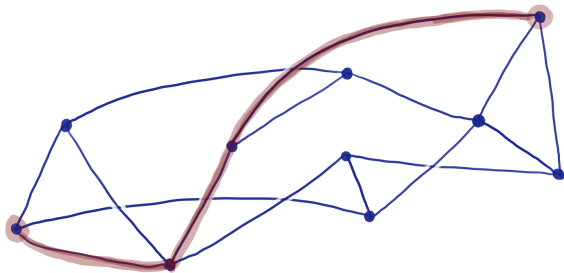
Given two vertices (j -invariants) construct a path between them (sequence of isogenies/kernels).



Isogeny hard problem

Hard Problem

Given two vertices (j -invariants) construct a path between them (sequence of isogenies/kernels).



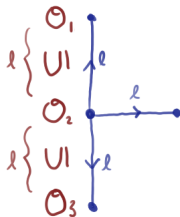
Endomorphism rings

A supersingular elliptic curve has a rank 4 ring of endomorphisms (quaternion order).

Quadratic rings embed:

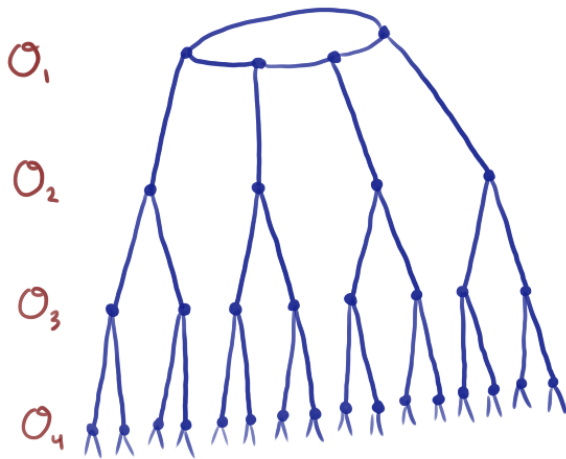
$$\mathcal{O} \hookrightarrow \text{End}(E).$$

An isogeny can be ascending, descending, or horizontal: $\mathcal{O}$ gets bigger, smaller, or stays the same.



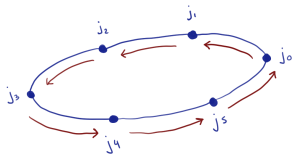
Orientations

Locally, from the point of view of $\mathcal{O}$, the supersingular graph is a volcano:



Comparison to DLP

The volcano rim has a *group action* by the *class group* $\text{Cl}(\mathcal{O})$.



Comparison to DLP

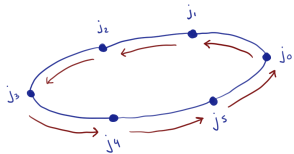
The volcano rim has a *group action* by the *class group* $\text{Cl}(\mathcal{O})$.

Hard Problem (Rephrased Isogeny Problem)

Given E and $\mathfrak{s} \cdot E$, compute ideal class $\mathfrak{s}$.

Hard Problem (Discrete Log Problem)

Modulo p , given g and g^s , compute exponent s .



Comparison to DLP

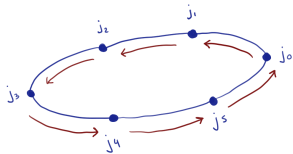
The volcano rim has a *group action* by the *class group* $\text{Cl}(\mathcal{O})$.

Hard Problem (Rephrased Isogeny Problem)

Given E and $\mathfrak{s} \cdot E$, compute ideal class $\mathfrak{s}$.

Hard Problem (Discrete Log Problem)

Modulo p , given g and g^s , compute exponent s .



Shor's algorithm computes the 'period' (kernel) of the map

$$(x, y) \mapsto g^x (g^s)^{-y},$$

which gives away the secret s such that $x = sy$.

Comparison to DLP

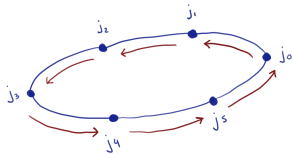
The volcano rim has a *group action* by the *class group* $\text{Cl}(\mathcal{O})$.

Hard Problem (Rephrased Isogeny Problem)

Given E and $\mathfrak{s} \cdot E$, compute ideal class $\mathfrak{s}$.

Hard Problem (Discrete Log Problem)

Modulo p , given g and g^s , compute exponent s .



Shor's algorithm computes the 'period' (kernel) of the map

$$(x, y) \mapsto g^x (g^s)^{-y},$$

which gives away the secret s such that $x = sy$.

In our case, no way to 'multiply': $\mathfrak{x} \cdot E \text{ ??} \longleftrightarrow \text{??} \eta^{-1} \cdot (\mathfrak{s} \cdot E)$

Isogeny Hard Problems

Finite $\mathbb{F}$. There is a faithful action of $\text{Cl}(\mathcal{O})$ on

$$\text{Ell}(\mathcal{O}) = \{E/\mathbb{F} : E \text{ has CM by } \mathcal{O}\}.$$

When $\mathfrak{a} \cdot E_1 = E_2$, this gives an isogeny $\phi_{\mathfrak{a}} : E_1 \rightarrow E_2$ respecting $\mathcal{O}$.

Isogeny Hard Problems

Finite $\mathbb{F}$. There is a faithful action of $\text{Cl}(\mathcal{O})$ on

$$\text{Ell}(\mathcal{O}) = \{E/\mathbb{F} : E \text{ has CM by } \mathcal{O}\}.$$

When $\mathfrak{a} \cdot E_1 = E_2$, this gives an isogeny $\phi_{\mathfrak{a}} : E_1 \rightarrow E_2$ respecting $\mathcal{O}$.

Hard Problem 1: Given E_1 and $E_2 \in \text{Ell}(\mathcal{O})$, find $\phi : E_1 \rightarrow E_2$ respecting $\mathcal{O}$.

Isogeny Hard Problems

Finite $\mathbb{F}$. There is a faithful action of $\text{Cl}(\mathcal{O})$ on

$$\text{Ell}(\mathcal{O}) = \{E/\mathbb{F} : E \text{ has CM by } \mathcal{O}\}.$$

When $\mathfrak{a} \cdot E_1 = E_2$, this gives an isogeny $\phi_{\mathfrak{a}} : E_1 \rightarrow E_2$ respecting $\mathcal{O}$.

Hard Problem 1: Given E_1 and $E_2 \in \text{Ell}(\mathcal{O})$, find $\phi : E_1 \rightarrow E_2$ respecting $\mathcal{O}$.

Hard Problem 2: Given E_1 and $E_2 \in \text{Ell}(\mathcal{O})$, and $\deg \phi$, find $\phi : E_1 \rightarrow E_2$ respecting $\mathcal{O}$.

Isogeny interpolation

(Castryck-Decru-Maino-Martindale-Panny-Pope-Robert-Wesolowski)

Hard Problem 2: Given E_1 and $E_2 \in \text{Ell}(\mathcal{O})$, and $\deg \phi$, find $\phi : E_1 \rightarrow E_2$ respecting $\mathcal{O}$.

Isogeny interpolation

(Castryck-Decru-Maino-Martindale-Panny-Pope-Robert-Wesolowski)

Hard Problem 2: Given E_1 and $E_2 \in \text{Ell}(\mathcal{O})$, and $\deg \phi$, find $\phi : E_1 \rightarrow E_2$ respecting $\mathcal{O}$.

[CDM+24]: to efficiently determine $\phi : E_1 \rightarrow E_2$, it suffices to find $\phi(G)$ (actually ϕ of generators) for some subgroup G of size at least $4 \deg \phi + 1$.

Isogeny interpolation

(Castrick-Decru-Maino-Martindale-Panny-Pope-Robert-Wesolowski)

Hard Problem 2: Given E_1 and $E_2 \in \text{Ell}(\mathcal{O})$, and $\deg \phi$, find $\phi : E_1 \rightarrow E_2$ respecting $\mathcal{O}$.

[CDM+24]: to efficiently determine $\phi : E_1 \rightarrow E_2$, it suffices to find $\phi(G)$ (actually ϕ of generators) for some subgroup G of size at least $4 \deg \phi + 1$.

So it suffices to solve....

Hard Problem 3: Given E_1 and $E_2 \in \text{Ell}(\mathcal{O})$, and $\deg \phi$, find $\phi(G)$, $\#G > 4 \deg \phi$ for $\phi : E_1 \rightarrow E_2$ respecting $\mathcal{O}$.

Pairings and isogenies

We have a very nice property:

$$\langle \phi P, \phi Q \rangle = \langle P, Q \rangle^{\deg \phi}$$

Pairings – destructively

An idea of Castryck-Houben-Merz-Mula-van Buuren-Vercauteren: Let $m > 4 \deg \phi$. Suppose $P \in E_1[m]$, and suppose $\phi(P) = kP' \in E_2[m]$. Use a pairing:

$$\langle P, P \rangle^{\deg \phi} = \langle \phi P, \phi P \rangle = \langle kP', kP' \rangle = \langle P', P' \rangle^{k^2}.$$

Pairings – destructively

An idea of Castryck-Houben-Merz-Mula-van Buuren-Vercauteren: Let $m > 4 \deg \phi$. Suppose $P \in E_1[m]$, and suppose $\phi(P) = kP' \in E_2[m]$. Use a pairing:

$$\langle P, P \rangle^{\deg \phi} = \langle \phi P, \phi P \rangle = \langle kP', kP' \rangle = \langle P', P' \rangle^{k^2}.$$

So

$$P, P', \deg \phi \xrightarrow[\text{non-deg. pair.}]{\text{discrete log}} k^2 \pmod{m}$$

Pairings – destructively

An idea of Castryck-Houben-Merz-Mula-van Buuren-Vercauteren: Let $m > 4 \deg \phi$. Suppose $P \in E_1[m]$, and suppose $\phi(P) = kP' \in E_2[m]$. Use a pairing:

$$\langle P, P \rangle^{\deg \phi} = \langle \phi P, \phi P \rangle = \langle kP', kP' \rangle = \langle P', P' \rangle^{k^2}.$$

So

$$P, P', \deg \phi \xrightarrow[\text{non-deg. pair.}]{\text{discrete log}} k^2 \pmod{m} \implies k$$

Pairings – destructively

An idea of Castryck-Houben-Merz-Mula-van Buuren-Vercauteren: Let $m > 4 \deg \phi$. Suppose $P \in E_1[m]$, and suppose $\phi(P) = kP' \in E_2[m]$. Use a pairing:

$$\langle P, P \rangle^{\deg \phi} = \langle \phi P, \phi P \rangle = \langle kP', kP' \rangle = \langle P', P' \rangle^{k^2}.$$

So

$$P, P', \deg \phi \xrightarrow[\text{non-deg. pair.}]{\text{discrete log}} k^2 \pmod{m} \implies k \implies \phi P$$

Pairings – destructively

An idea of Castryck-Houben-Merz-Mula-van Buuren-Vercauteren: Let $m > 4 \deg \phi$. Suppose $P \in E_1[m]$, and suppose $\phi(P) = kP' \in E_2[m]$. Use a pairing:

$$\langle P, P \rangle^{\deg \phi} = \langle \phi P, \phi P \rangle = \langle kP', kP' \rangle = \langle P', P' \rangle^{k^2}.$$

So

$$P, P', \deg \phi \xrightarrow[\text{non-deg. pair.}]{\text{discrete log}} k^2 \pmod{m} \implies k \implies \phi P \xrightarrow{\text{isog. interp.}} \phi$$

Pairings – destructively

An idea of Castryck-Houben-Merz-Mula-van Buuren-Vercauteren: Let $m > 4 \deg \phi$. Suppose $P \in E_1[m]$, and suppose $\phi(P) = kP' \in E_2[m]$. Use a pairing:

$$\langle P, P \rangle^{\deg \phi} = \langle \phi P, \phi P \rangle = \langle kP', kP' \rangle = \langle P', P' \rangle^{k^2}.$$

So

$$P, P', \deg \phi \xrightarrow[\text{non-deg. pair.}]{\text{discrete log}} k^2 \pmod{m} \implies k \implies \phi P \xrightarrow{\text{isog. interp.}} \phi$$

Challenges:

1. Make sure $\phi P \in \mathbb{Z}P'$.
2. Make sure $\langle P, P \rangle$ is non-trivial.

CHMMvBV: Non-degenerate self-pairings on one cyclic subgroup when $m \mid \Delta_\phi$.

Sesquilinear pairings

Let $\alpha, \beta \in \mathcal{O}$, an order in an imaginary quadratic field. A sesquilinear pairing is a bilinear pairing with:

$$\langle \alpha P, \beta Q \rangle = \langle P, Q \rangle^{\alpha \overline{\beta}}.$$

Sesquilinear pairings

Let $\alpha, \beta \in \mathcal{O}$, an order in an imaginary quadratic field. A sesquilinear pairing is a bilinear pairing with:

$$\langle \alpha P, \beta Q \rangle = \langle P, Q \rangle^{\alpha \bar{\beta}}.$$

Theorem (S.)

Sesquilinear Weil and Tate exist and have all the nice properties, including a Miller-style computation.

Using $\mathcal{O}$ -sesquilinear pairings (joint with Joseph Macula)

Let $m^2 > 4 \deg \phi$. Suppose $P \in E_1[m]$, suppose $\mathcal{O}P' = E_2[m]$ and ϕ oriented. Use a pairing:

$$\langle P, P \rangle^{\deg \phi} = \langle \phi P, \phi P \rangle = \langle \lambda P', \lambda P' \rangle = \langle P', P' \rangle^{N(\lambda)}.$$

Using $\mathcal{O}$ -sesquilinear pairings (joint with Joseph Macula)

Let $m^2 > 4 \deg \phi$. Suppose $P \in E_1[m]$, suppose $\mathcal{O}P' = E_2[m]$ and ϕ oriented. Use a pairing:

$$\langle P, P \rangle^{\deg \phi} = \langle \phi P, \phi P \rangle = \langle \lambda P', \lambda P' \rangle = \langle P', P' \rangle^{N(\lambda)}.$$

So

$$P, P', \deg \phi \xrightarrow[\text{non-deg. pair.}]{\text{discrete log}} N(\lambda) \pmod{m}$$

Using $\mathcal{O}$ -sesquilinear pairings (joint with Joseph Macula)

Let $m^2 > 4 \deg \phi$. Suppose $P \in E_1[m]$, suppose $\mathcal{O}P' = E_2[m]$ and ϕ oriented. Use a pairing:

$$\langle P, P \rangle^{\deg \phi} = \langle \phi P, \phi P \rangle = \langle \lambda P', \lambda P' \rangle = \langle P', P' \rangle^{N(\lambda)}.$$

So

$$P, P', \deg \phi \xrightarrow[\text{non-deg. pair.}]{\text{discrete log}} N(\lambda) \pmod{m} \not\Rightarrow \lambda$$

Using $\mathcal{O}$ -sesquilinear pairings (joint with Joseph Macula)

Let $m^2 > 4 \deg \phi$. Suppose $P \in E_1[m]$, suppose $\mathcal{O}P' = E_2[m]$ and ϕ oriented. Use a pairing:

$$\langle P, P \rangle^{\deg \phi} = \langle \phi P, \phi P \rangle = \langle \lambda P', \lambda P' \rangle = \langle P', P' \rangle^{N(\lambda)}.$$

So

$$P, P', \deg \phi \xrightleftharpoons[\text{non-deg. pair.}]{\text{discrete log}} N(\lambda) \pmod{m} \not\Rightarrow \lambda \Rightarrow \phi P$$

Using $\mathcal{O}$ -sesquilinear pairings (joint with Joseph Macula)

Let $m^2 > 4 \deg \phi$. Suppose $P \in E_1[m]$, suppose $\mathcal{O}P' = E_2[m]$ and ϕ oriented. Use a pairing:

$$\langle P, P \rangle^{\deg \phi} = \langle \phi P, \phi P \rangle = \langle \lambda P', \lambda P' \rangle = \langle P', P' \rangle^{N(\lambda)}.$$

So

$$P, P', \deg \phi \xrightleftharpoons[\text{non-deg. pair.}]{\text{discrete log}} N(\lambda) \pmod{m} \not\Rightarrow \lambda \Rightarrow \phi P \xrightleftharpoons{\text{isog. interp.}} \phi$$

Using $\mathcal{O}$ -sesquilinear pairings (joint with Joseph Macula)

Let $m^2 > 4 \deg \phi$. Suppose $P \in E_1[m]$, suppose $\mathcal{O}P' = E_2[m]$ and ϕ oriented. Use a pairing:

$$\langle P, P \rangle^{\deg \phi} = \langle \phi P, \phi P \rangle = \langle \lambda P', \lambda P' \rangle = \langle P', P' \rangle^{N(\lambda)}.$$

So

$$P, P', \deg \phi \xrightleftharpoons[\text{non-deg. pair.}]{\text{discrete log}} N(\lambda) \pmod{m} \not\Rightarrow \lambda \Rightarrow \phi P \xrightleftharpoons{\text{isog. interp.}} \phi$$

Pros/Cons:

1. Can use generic P and P' ?
2. Don't need $m \mid \Delta_{\mathcal{O}}$?
3. For m coprime to $\Delta_{\mathcal{O}}$, knowing $N(\lambda) \pmod{m}$ only cuts down $\lambda \pmod{m}$ from $\approx m^2$ options to $\approx m$ options.

When is $\langle P, P \rangle$ non-degenerate?

Theorem (Macula-S.)

Suppose $\mu_m \subseteq \mathbb{F}$, m is coprime to $\Delta_{\mathcal{O}}$, and $E[m] \subseteq E(\mathbb{F})$. Then $\langle P, P \rangle$ (sesquilinear Tate pairing) has full order whenever $\mathcal{O}P = E[m]$, which can happen as long as $\mathcal{O}$ is maximal in $\text{End}(E)$.

When $m \mid \Delta_{\mathcal{O}}$

We have $\sigma \in \mathcal{O}$, $P \in E[m]$ with:

1. $N(a + b\sigma) \equiv N(a) \pmod{m}$, $a, b \in \mathbb{Z}$;
2. $\sigma P = \infty$.

Then knowing $N(\lambda) = N(a + b\sigma)$ means knowing a^2 ; proceed as before.

When $m \mid \Delta_{\mathcal{O}}$

We have $\sigma \in \mathcal{O}$, $P \in E[m]$ with:

1. $N(a + b\sigma) \equiv N(a) \pmod{m}$, $a, b \in \mathbb{Z}$;
2. $\sigma P = \infty$.

Then knowing $N(\lambda) = N(a + b\sigma)$ means knowing a^2 ; proceed as before.

Main advantage: compute pairing in field of definition of $E[m]$ not $E[m^2]$.

When $m \mid \Delta_{\mathcal{O}}$

We have $\sigma \in \mathcal{O}$, $P \in E[m]$ with:

1. $N(a + b\sigma) \equiv N(a) \pmod{m}$, $a, b \in \mathbb{Z}$;
2. $\sigma P = \infty$.

Then knowing $N(\lambda) = N(a + b\sigma)$ means knowing a^2 ; proceed as before.

Main advantage: compute pairing in field of definition of $E[m]$ not $E[m^2]$.

Example (adapted from W. Castryck): $E : y^2 = x^3 + x$, $p = 4 \cdot 3^r - 1$ with $E[3^r] \subseteq \mathbb{F}_{p^2}$ but $E[3^{2r}]$ field degree grows exponentially with r .

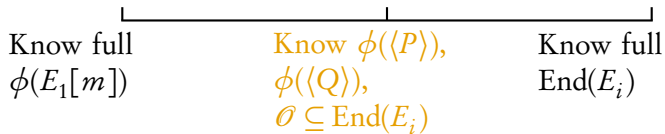
Bilinear and sesquilinear

	bilinear	sesquilinear	
	$m \mid \Delta_{\mathcal{O}}$	m coprime to $\Delta_{\mathcal{O}}$	$m \mid \Delta_{\mathcal{O}}$
size of m :	$m > 4 \deg \phi$	$m^2 > 4 \deg \phi$	$m > 4 \deg \phi$
# poss. images:	# square roots mod m	$\approx m$ with given norm	# square roots mod m
field:	$E[m^2]$	$E[m]$	$E[m]$
advantage?:		free choice of m	pairing computation

A trade-off

Suppose $m^2 > 4 \deg \phi$, coprime to Δ_ϕ and $\deg \phi$.

Situations where we can obtain ϕ :



Constructively and otherwise

- ▶ **Galbraith–Gilchrist–Robert (LATINCRYPT 2025)**
 - ▶ Self-pairings for ascending isogenies; PEARL/SCALLOP.
- ▶ **Reijnders, *The Tate Profile* (LATINCRYPT 2025)**
 - ▶ ϕ -Tate pairings and profiles; divisibility, basis sampling, and rational-cokernel.
- ▶ **Reijnders, *The Cokernel Pairing* (2026)**
 - ▶ Pairing on $E(\mathbb{F}_q)/mE(\mathbb{F}_q)$; applications to torsion bases and ℓ^k -isogenies.
- ▶ **Pope–Reijnders–Robert–Sferlazza–Smith (2025)**
 - ▶ Weil and Tate via Montgomery ladders & cubical arithmetic; SQIsign and CSIDH.
- ▶ **Higher-dimensional extensions (2026)**
 - ▶ Eriksen: generalized Tate arbitrary fields; Corte-Real Santos–Reijnders: genus-2/Kummer tools.
- ▶ **PIKE (PKC 2026)**
 - ▶ Pairing-assisted decryption for faster isogeny-based public-key encryption.

Thank you!

