Weak instances of class group action based cryptography via self-pairings

Crypto 2023, Santa Barbara

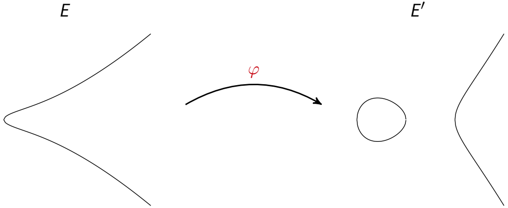
W. Castryck, M. Houben, S.-P. Merz,
M. Mula, S. van Buuren, F. Vercauteren

COSIC KU LEUVEN · ROYAL HOLLOWAY UNIVERSITY OF LONDON · UNIVERSITÀ DI TRENTO Department of Mathematics

Motivation

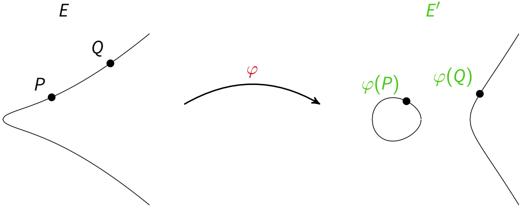
SIDH ATTACK + SELF-PAIRINGS: A DEADLY COMBINATION?

Consider a public-key cryptosystem where the **secret key** is an isogeny φ of known, smooth degree:



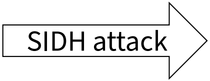
SIDH ATTACK + SELF-PAIRINGS: A DEADLY COMBINATION?

Consider a public-key cryptosystem where the **secret key** is an isogeny φ of known, smooth degree:



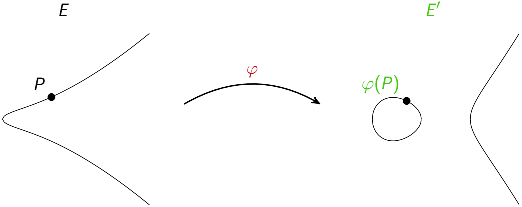
SIDH attack [CD23; Mai+23; Rob23]

Public key: E' and $\varphi(P)$, $\varphi(Q)$
(for suitable points P, Q on E)



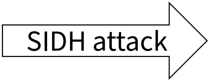
φ

Consider a public-key cryptosystem where the **secret key** is an isogeny φ of known, smooth degree:



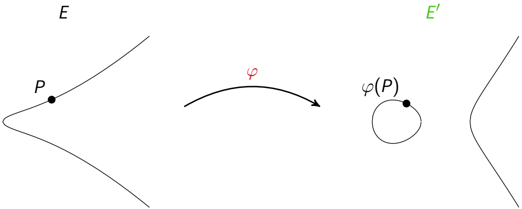
SIDH attack + reduction by De Feo et al.

Public key: E' and $\varphi(P)$
(for suitable point P on E)



φ

Consider a public-key cryptosystem where the **secret key** is an isogeny φ of known, smooth degree:

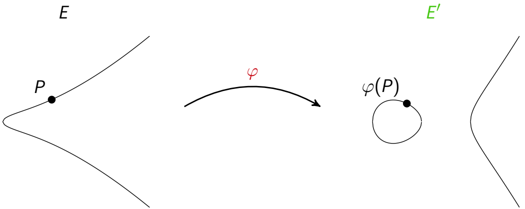


The attack that would put us out of business

Public key: E' → ? → $\varphi(P)$ (for suitable point P on E) → SIDH attack → φ

SIDH ATTACK + SELF-PAIRINGS: A DEADLY COMBINATION?

Consider a public-key cryptosystem where the **secret key** is an isogeny φ of known, smooth degree:



The attack that would put us out of business

Public key: E' → ? → $\varphi(P)$ (for suitable point P on E) → SIDH attack → φ

Our work: for which cryptosystems can we use **self-pairings** to fill this gap?

Our attack idea

Fact: in a class group action based cryptosystem, one can always find $\lambda\varphi(P)$ for some (unknown) $\lambda \in \mathbb{Z}$.

Goal of the attack: finding λ.

Our attack idea

Fact: in a class group action based cryptosystem, one can always find $\lambda\varphi(P)$ for some (unknown) $\lambda \in \mathbb{Z}$.

Goal of the attack: finding λ.

Naive approach:

- Compute the Weil (self-)pairing

$$e(\lambda\varphi(P), \lambda\varphi(P)) = e(P, P)^{\lambda^2 \deg(\varphi)}.$$

- Recover λ using a dlog computation.

→ $\varphi(P)$ → SIDH attack → φ

Our attack idea

Fact: in a class group action based cryptosystem, one can always find $\lambda\varphi(P)$ for some (unknown) $\lambda \in \mathbb{Z}$.

Goal of the attack: finding λ.

Naive approach:

- Compute the Weil (self-)pairing

$$e(\lambda\varphi(P), \lambda\varphi(P)) = e(P, P)^{\lambda^2 \deg(\varphi)}.$$

- Recover λ using a dlog computation.

→ $\varphi(P)$ → SIDH attack → φ

Problem: The Weil (self-)pairing $e(P, P)$ is always 1.

Fact: in a class group action based cryptosystem, one can always find $\lambda\varphi(P)$ for some (unknown) $\lambda \in \mathbb{Z}$.

Goal of the attack: finding λ.

Naive approach:

- Compute the Weil (self-)pairing

$$e(\lambda\varphi(P), \lambda\varphi(P)) = e(P, P)^{\lambda^2 \deg(\varphi)}.$$

- Recover λ using a dlog computation.

→ $\varphi(P)$ → SIDH attack → φ

Problem: The Weil (self-)pairing $e(P, P)$ is always 1.

Can we construct non-trivial self-pairings to make this attack work?

Class group action based cryptography

Crypto 101: Diffie-Hellman key exchange

Let $X = \langle x \rangle$ be a cyclic group of order n.

Alice		Bob
$a \xleftarrow{\$} \mathbb{Z}/n\mathbb{Z}$		$b \xleftarrow{\$} \mathbb{Z}/n\mathbb{Z}$
	$\xrightarrow{x^a}$	
	$\xleftarrow{x^b}$	
Computes $(x^b)^a$		Computes $(x^a)^b$

x^{ab} is the shared key

Crypto 101: Diffie-Hellman key exchange

Let $X = \langle x \rangle$ be a cyclic group of order n.

Alice		Bob
$a \xleftarrow{\$} \mathbb{Z}/n\mathbb{Z}$		$b \xleftarrow{\$} \mathbb{Z}/n\mathbb{Z}$
	$\xrightarrow{x^a}$	
	$\xleftarrow{x^b}$	
Computes $(x^b)^a$		Computes $(x^a)^b$

x^{ab} is the shared key

In [Cou06; RS06] this construction is generalized to group actions...

CRS: Diffie-Hellman with isogenies, 1

$$E_0 = \text{an ordinary elliptic curve defined over } \mathbb{F}_q,$$
$$\mathcal{O} = \mathbb{Z}[\sqrt{-d}] \cong \mathrm{End}(E_0).$$

Alice		Bob
$[\mathfrak{a}] \xleftarrow{\$} \mathrm{Cl}(\mathcal{O})$		$[\mathfrak{b}] \xleftarrow{\$} \mathrm{Cl}(\mathcal{O})$
$E_0 \xrightarrow{\varphi_{\mathfrak{a}}} [\mathfrak{a}]E_0$		$E_0 \xrightarrow{\varphi_{\mathfrak{b}}} [\mathfrak{b}]E_0$
	$\xrightarrow{[\mathfrak{a}]E_0}$	
	$\xleftarrow[{[\mathfrak{b}]E_0}]{}$	
Computes $[\mathfrak{a}]([\mathfrak{b}]E_0)$		Computes $[\mathfrak{b}]([\mathfrak{a}]E_0)$

$[\mathfrak{a}\mathfrak{b}]E_0$ is the shared key

CRS: Diffie-Hellman with isogenies, 2

$E_0 =$ an ordinary elliptic curve defined over $\mathbb{F}_q$,

$\mathcal{O} = \mathbb{Z}[\sqrt{-d}] \cong \mathrm{End}(E_0)$ (some imaginary quadratic order)

(also $\mathcal{O} = \mathbb{Z}\left[(1+\sqrt{-d})/2\right]$ is fine if $d \equiv 3 \bmod 4$).

$E_0 =$ an ordinary elliptic curve defined over $\mathbb{F}_q$,

$\mathcal{O} = \mathbb{Z}[\sqrt{-d}] \cong \mathrm{End}(E_0)$ (some imaginary quadratic order)

(also $\mathcal{O} = \mathbb{Z}\left[(1+\sqrt{-d})/2\right]$ is fine if $d \equiv 3 \bmod 4$).

Consider the set

$X = \{$ E over $\mathbb{F}_q$ which are $\mathbb{F}_q$-isogenous to E_0 and s.t. $\mathrm{End}(E) \cong \mathcal{O}$ $\}$

and the group

$G =$ class group of $\mathcal{O}$.

CRS: Diffie-Hellman with isogenies, 2

$E_0 =$ an ordinary elliptic curve defined over $\mathbb{F}_q$,

$\mathcal{O} = \mathbb{Z}[\sqrt{-d}] \cong \mathrm{End}(E_0)$ (some imaginary quadratic order)

(also $\mathcal{O} = \mathbb{Z}\left[(1+\sqrt{-d})/2\right]$ is fine if $d \equiv 3 \bmod 4$).

Consider the set

$X = \{\ E$ over $\mathbb{F}_q$ which are $\mathbb{F}_q$-isogenous to E_0 and s.t. $\mathrm{End}(E) \cong \mathcal{O}\ \}$

and the group

$G =$ class group of $\mathcal{O}$.

Action of G over X

$[\mathfrak{a}] \in G$

$E \in X$

$\longrightarrow$ $[\mathfrak{a}]E =$ codomain of the isogeny $\varphi_{\mathfrak{a}}$ with kernel $\ker(\varphi_{\mathfrak{a}}) = \bigcap_{\alpha \in \mathfrak{a}} \ker(\alpha)$.

$E_0 =$ a supersingular elliptic curve defined over $\mathbb{F}_p$, for $p \equiv 3 \bmod 4$.
$\pi =$ the Frobenius endomorphism on E, i.e. $\pi\colon (x, y) \mapsto (x^p, y^p)$.
$\mathcal{O} = \mathbb{Z}\left[\sqrt{-p}\right]$.
$\iota_0 =$ the map $\sqrt{-p} \mapsto \pi$.

The pair (E_0, ι_0) is called an *$\mathcal{O}$-orientation*.
In particular, $\iota_0(\mathcal{O}) = \mathrm{End}_{\mathbb{F}_p}(E_0)$.

CSIDH: Diffie-Hellman with (Frobenius-oriented) isogenies

$E_0 =$ a supersingular elliptic curve defined over $\mathbb{F}_p$, for $p \equiv 3 \bmod 4$.
$\pi =$ the Frobenius endomorphism on E, i.e. $\pi\colon (x, y) \mapsto (x^p, y^p)$.
$\mathcal{O} = \mathbb{Z}\left[\sqrt{-p}\right]$.
$\iota_0 =$ the map $\sqrt{-p} \mapsto \pi$.

The pair (E_0, ι_0) is called an *$\mathcal{O}$-orientation*.
In particular, $\iota_0(\mathcal{O}) = \mathrm{End}_{\mathbb{F}_p}(E_0)$.

Define the set

$$X = \{\ (E, \iota) \text{ over } \mathbb{F}_p \text{ oriented by } \mathcal{O} \text{ and } \mathbb{F}_p\text{-isogenous to } E_0\ \}.$$

The group G and its action over X are defined exactly as before.

More generally...

$E_0 =$ an ~~supersingular~~ elliptic curve defined over $\mathbb{F}_q$.

$\mathcal{O} = \mathbb{Z}\left[\sqrt{-d}\right]$ for some positive integer d.

$\iota_0 =$ an injective homomorphism $\mathcal{O} \hookrightarrow \mathrm{End}(E_0)$.

OSIDH: Diffie-Hellman with (oriented) isogenies

More generally...

$E_0 =$ an ~~supersingular~~ elliptic curve defined over $\mathbb{F}_q$.

$\mathcal{O} = \mathbb{Z}\left[\sqrt{-d}\right]$ for some positive integer d.

$\iota_0 =$ an injective homomorphism $\mathcal{O} \hookrightarrow \mathrm{End}(E_0)$.

Define the set

$$X = \{\ (E, \iota) \text{ over } \mathbb{F}_q \text{ oriented by } \mathcal{O} \text{ and s.t. there exists an } \underbrace{\mathcal{O}\text{-oriented}} \text{ isogeny } \alpha\colon E_0 \to E\ \}.$$

satisfying $\iota(\sqrt{-d}) \circ \alpha = \alpha \circ \iota_0\left(\sqrt{-d}\right)$

The group G and its action over X are defined exactly as before.

Bottom line

Given *p*, there are lots of imaginary quadratic orders $\mathcal{O} = \mathbb{Z}[\sqrt{-d}]$ and orientations to choose from to build a class group action based cryptosystem.

Bottom line

Given p, there are lots of imaginary quadratic orders $\mathcal{O} = \mathbb{Z}[\sqrt{-d}]$ and orientations to choose from to build a class group action based cryptosystem.

Which choices are bad?

- Trivial: d small.
- **Our work:** d with a factor ℓ^{2r} for some small ℓ.

Self-pairings

Self-pairings

$$E = \text{an elliptic curve } E \text{ over } \mathbb{F}_q.$$
$$G = \text{a finite subgroup of } E.$$

A *self-pairing* on G is a map

$$f : G \to \overline{\mathbb{F}_q}^*$$

such that $f(\lambda P) = f(P)^{\lambda^2}$ for all $P \in G$ and $\lambda \in \mathbb{Z}$.

Self-pairings

$$E = \text{an elliptic curve } E \text{ over } \mathbb{F}_q.$$
$$G = \text{a finite subgroup of } E.$$

A *self-pairing* on G is a map

$$f : G \to \overline{\mathbb{F}_q}^*$$

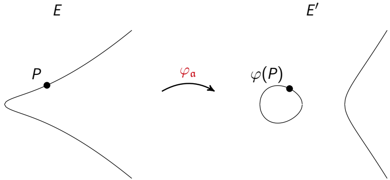
such that $f(\lambda P) = f(P)^{\lambda^2}$ for all $P \in G$ and $\lambda \in \mathbb{Z}$.
Given

- an isogeny $\varphi : E \to E'$,
- a self-pairing $f : G \to \overline{\mathbb{F}_q}^*$ on E,
- a self-pairing $f' : G' \to \overline{\mathbb{F}_q}^*$ on E',

f and f' are *compatible* with φ if

$$\varphi(G) \subseteq G' \qquad \text{and} \qquad f'(\varphi(P)) = f(P)^{\deg(\varphi)}$$

for all $P \in G$.



$$\mathcal{O} = \mathbb{Z}[\sqrt{-d}].$$

$$E, E' = \mathcal{O}\text{-oriented elliptic curves.}$$

$[\mathfrak{a}] =$ a (secret) ideal class of $\mathrm{Cl}(\mathcal{O})$ such that $E' = [\mathfrak{a}]E$.

$\varphi_{\mathfrak{a}} =$ (secret) isogeny corresponding to $\mathfrak{a}$.

We assume that $\deg(\varphi_{\mathfrak{a}})$ is smooth and known to the attacker.

Sketch of the attack

Self-pairings compatible with all $\mathcal{O}$-oriented isogenies $\varphi\colon E \to E'$ → $\varphi_{\mathfrak{a}}(P)$ → SIDH attack → $\varphi_{\mathfrak{a}}$

More detailed sketch of the attack

$\ell =$ small prime not dividing $\deg(\varphi_{\mathfrak{a}})$.

$G =$ (suitable) cyclic subgroup of E of order $\ell^{2r} > \deg(\varphi_{\mathfrak{a}})$.

$G' = \varphi_{\mathfrak{a}}(G)$.

$P, P' =$ generators of G, G'. In particular, $P' = \lambda \varphi_{\mathfrak{a}}(P)$ for some λ.

$f, f' =$ self-pairings on G, G' compatible with all $\mathcal{O}$-oriented isogenies $\varphi : E \to E'$.

- Compute $f'(P') = f(P)^{\lambda^2 \deg(\varphi_{\mathfrak{a}})}$.
- Deduce λ by comparing $f(P)$ and $f'(P')$.

$\varphi_{\mathfrak{a}}(P)$ → SIDH attack → $\varphi_{\mathfrak{a}}$

More detailed sketch of the attack

$\ell =$ small prime not dividing $\deg(\varphi_{\mathfrak{a}})$.

$G =$ (suitable) cyclic subgroup of E of order $\ell^{2r} > \deg(\varphi_{\mathfrak{a}})$.

$G' = \varphi_{\mathfrak{a}}(G)$.

$P, P' =$ generators of G, G'. In particular, $P' = \lambda\varphi_{\mathfrak{a}}(P)$ for some λ.

$f, f' =$ self-pairings on G, G' compatible with all $\mathcal{O}$-oriented isogenies $\varphi\colon E \to E'$.

- Compute $f'(P') = f(P)^{\lambda^2 \deg(\varphi_{\mathfrak{a}})}$.
- Deduce λ by comparing $f(P)$ and $f'(P')$.

$\varphi_{\mathfrak{a}}(P)$ → SIDH attack → $\varphi_{\mathfrak{a}}$

Possible problems:

- f and f' might not exist!
- Computing f and f' might be inefficient.

OUR MAIN RESULT

From [Cas+23a, Prop. 4.8 and §5]:

Define $m = \ell^{2r} \cdot \mathrm{gcd}(2, \ell)$ and $p = \mathrm{char}(\mathbb{F}_q)$.
Let $\Delta_{\mathcal{O}}$ be the discriminant of $\mathcal{O}$.
Then f and f' exist if and only if

- $p \nmid m$,
- $m \mid \Delta_{\mathcal{O}}$,
- writing $\Delta_{\mathcal{O}} = -2^r n$ for n odd, we have:
  - if $r = 2$ then $m \mid \Delta_{\mathcal{O}}/2$,
  - if $r \geq 3$ then $m \mid \Delta_{\mathcal{O}}/4$.

Our main result

From [Cas+23a, Prop. 4.8 and §5]:

Define $m = \ell^{2r} \cdot \mathrm{gcd}(2, \ell)$ and $p = \mathrm{char}(\mathbb{F}_q)$.
Let $\Delta_{\mathcal{O}}$ be the discriminant of $\mathcal{O}$.
Then f and f' exist if and only if

- $p \nmid m$,
- $m \mid \Delta_{\mathcal{O}}$,
- writing $\Delta_{\mathcal{O}} = -2^r n$ for n odd, we have:
    - if $r = 2$ then $m \mid \Delta_{\mathcal{O}}/2$,
    - if $r \geq 3$ then $m \mid \Delta_{\mathcal{O}}/4$.

Good news: CSIDH is not affected by our attack
(since $\Delta_{\mathcal{O}} = -4p$)

Computing self-pairings (when they exist!)

For the values of m allowed by our main result, $f(P)$ can be computed as follows...

	Frobenius-oriented	General case
Tool	Frey–Rück Tate pairing	Weil pairing on large extension of $\mathbb{F}_q$
Time complexity	$O(\log^2 m \log^{1+\varepsilon} q)$	$O(\Delta_{\mathcal{O}}^{2+\varepsilon} m^{2+\varepsilon} \log^{1+\varepsilon} q)$ often: $O(m^{4+\varepsilon} \log^{1+\varepsilon} q)$

Which choices of $\mathcal{O}$ should be avoided?

For sure: $\Delta_{\mathcal{O}}$ with a factor ℓ^{2r} for some small prime ℓ, in the Frobenius-oriented case.

Probably: $\Delta_{\mathcal{O}}$ with a factor ℓ^{2r} for some smooth integer ℓ, in the Frobenius-oriented case.

To feel 100% safe from our attack: $\Delta_{\mathcal{O}}$ with many small factors.

Open problems

- Can we compute self-pairings more efficiently in the non-Frobenius-oriented case?

Open problems

- Can we compute self-pairings more efficiently in the non-Frobenius-oriented case?
- In the Frobenius-oriented case, our attack can be generalized to any smooth ℓ (not necessarily prime). The expected running time of the resulting attack is subexponential [Cas+23a, Prop. 6.5]. Is it possible to give a sharper estimate?

Open problems

- Can we compute self-pairings more efficiently in the non-Frobenius-oriented case?
- In the Frobenius-oriented case, our attack can be generalized to any smooth ℓ (not necessarily prime). The expected running time of the resulting attack is subexponential [Cas+23a, Prop. 6.5]. Is it possible to give a sharper estimate?
- Can we exploit self-pairings of order $< \deg(\varphi_{\mathfrak{a}})$ to perform some attack?

Open problems

- Can we compute self-pairings more efficiently in the non-Frobenius-oriented case?
- In the Frobenius-oriented case, our attack can be generalized to any smooth ℓ (not necessarily prime). The expected running time of the resulting attack is subexponential [Cas+23a, Prop. 6.5]. Is it possible to give a sharper estimate?
- Can we exploit self-pairings of order $< \deg(\varphi_{\mathfrak{a}})$ to perform some attack?
- A few extra values of *m* are allowed if we only require *f* to be compatible with $\mathcal{O}$-oriented isogenies *of degree coprime with m* [Cas+23b, Prop. A.1]. Is there an effective construction for these extra cases?

Thank you for your attention!

[CD23] W. Castryck and T. Decru. "An Efficient Key Recovery Attack on SIDH". In: *Advances in Cryptology – EUROCRYPT 2023*. Ed. by C. Hazay and M. Stam. Cham: Springer Nature Switzerland, 2023, pp. 423–447.

[Cas+23a] W. Castryck, M. Houben, S.-P. Merz, M. Mula, S. van Buuren, and F. Vercauteren. "Weak Instances of Class Group Action Based Cryptography via Self-pairings". In: *Advances in Cryptology – CRYPTO 2023*. Ed. by H. Handschuh and A. Lysyanskaya. Cham: Springer Nature Switzerland, 2023, pp. 762–792.

[Cas+23b] W. Castryck, M. Houben, S.-P. Merz, M. Mula, S. van Buuren, and F. Vercauteren. *Weak instances of class group action based cryptography via self-pairings*. Full version on ePrint Archive available at https://eprint.iacr.org/2023/549. 2023.

Essential bibliography II

[Cas+18] W. Castryck, T. Lange, C. Martindale, L. Panny, and J. Renes. *CSIDH: An Efficient Post-Quantum Commutative Group Action*. Ed. by T. Peyrin and S. Galbraith. Cham, 2018.

[CK20] L. Colò and D. Kohel. “Orienting supersingular isogeny graphs”. In: *J. Math. Cryptol.* 14.1 (2020), pp. 414–437.

[Cou06] J.-M. Couveignes. *Hard Homogeneous Spaces*. Cryptology ePrint Archive, Report 2006/291. 2006. URL: `https://eprint.iacr.org/2006/291`.

[Mai+23] L. Maino, C. Martindale, L. Panny, G. Pope, and B. Wesolowski. “A Direct Key Recovery Attack on SIDH”. In: *Advances in Cryptology – EUROCRYPT 2023*. Ed. by C. Hazay and M. Stam. Cham: Springer Nature Switzerland, 2023, pp. 448–471.

Essential bibliography III

[Rob23] D. Robert. “Breaking SIDH in Polynomial Time”. In: *Advances in Cryptology – EUROCRYPT 2023*. Ed. by C. Hazay and M. Stam. Cham: Springer Nature Switzerland, 2023, pp. 472–503.

[RS06] A. Rostovtsev and A. Stolbunov. *Public-key cryptosystem based on isogenies*. Cryptology ePrint Archive, Report 2006/145. `https://eprint.iacr.org/2006/145`. 2006.

Appendix 1: Pairings

Weil pairing

$p =$ a (large) prime. $\quad n =$ positive integer coprime with p.

$\mu_n = n$-th roots of unity in $\overline{\mathbb{F}_p}$. $\quad \mathbb{F}_q =$ a finite field containing μ_n.

$E =$ an EC defined over $\mathbb{F}_q$. $\quad E[n] =$ group of points of n-torsion of E

Weil pairing

$p =$ a (large) prime. $n =$ positive integer coprime with p.

$\mu_n = n$-th roots of unity in $\overline{\mathbb{F}_p}$. $\mathbb{F}_q =$ a finite field containing μ_n.

$E =$ an EC defined over $\mathbb{F}_q$. $E[n] =$ group of points of n-torsion of E

The *n-Weil pairing* is a map

$$e(\,\cdot\,,\,\cdot\,) = e_{E,n}(\,\cdot\,,\,\cdot\,)\colon \quad E[n] \times E[n] \to \mu_n$$

which is

- Bilinear: $e(P+R, Q) = e(P,Q)e(R,Q)$ for all $P, Q, R \in E[n]$.
- Nondegenerate: if $e(P,Q) = 1$ for all $Q \in E[n]$, then $P = O$.
- Alternating: $e(P,Q) = e(Q,P)^{-1}$ for all $P, Q \in E[n]$.
- Compatible with *every* isogeny: if $\varphi\colon E \to E'$ is an isogeny, then

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

The power of pairings

Consider a (secret) isogeny

$$\varphi\colon E \to E'.$$

What can be done with pairings?

Let P, Q be generators of $E[n]$.

- Given $\varphi(P), \varphi(Q)$ $\rightsquigarrow$ recover $\deg(\varphi) \bmod n$.

Consider a (secret) isogeny

$$\varphi\colon E \to E'.$$

What can be done with pairings?

Let P, Q be generators of $E[n]$.

- Given $\varphi(P), \varphi(Q)$ $\rightsquigarrow$ recover $\deg(\varphi) \bmod n$.
- Given $\varphi(P)$ and $\deg(\varphi)$, if $n^2 > \deg(\varphi)$ $\rightsquigarrow$ recover φ itself! (using SIDH attack)

Appendix 2: Orientations

What happens if we use supersingular elliptic curves?

Problem: if E is supersingular, then $\mathrm{End}(E)$ is NOT an imaginary quadratic order!

Bad news

$\mathrm{End}(E)$ is non-commutative, $\mathrm{Cl}(\mathrm{End}(E))$ is not even a group.

What happens if we use supersingular elliptic curves?

Problem: if E is supersingular, then $\mathrm{End}(E)$ is NOT an imaginary quadratic order!

Bad news

$\mathrm{End}(E)$ is non-commutative, $\mathrm{Cl}(\mathrm{End}(E))$ is not even a group.

Good news

For each non-scalar $\tau \in \mathrm{End}(E)$, $\mathcal{O}_\tau = \{\sigma \in \mathrm{End}(E) \mid \sigma \circ \tau = \tau \circ \sigma\}$ is an imaginary quadratic order.

What happens if we use supersingular elliptic curves?

Problem: if E is supersingular, then $\mathrm{End}(E)$ is NOT an imaginary quadratic order!

Bad news

$\mathrm{End}(E)$ is non-commutative, $\mathrm{Cl}(\mathrm{End}(E))$ is not even a group.

Good news

For each non-scalar $\tau \in \mathrm{End}(E)$, $\mathcal{O}_\tau = \{\sigma \in \mathrm{End}(E) \mid \sigma \circ \tau = \tau \circ \sigma\}$ is an imaginary quadratic order.

Given $\mathcal{O} = \mathbb{Z}[\sqrt{-d}]$, we say that (E, ι) is an *$\mathcal{O}$-oriented elliptic curve* if there is an injective ring homomorphism

$$\iota \colon \mathcal{O} \hookrightarrow \mathrm{End}(E).$$

Conclusion: given an $\mathcal{O}$-orientation (E, ι), the subring $\iota(\mathcal{O}) \subseteq \mathrm{End}(E)$ is an imaginary quadratic order.

Appendix 3: Applications of self-pairings

The power of self-pairings

$$S = \{\text{elliptic curves over } \mathbb{F}_q \text{, oriented by their Frobenius}\}.$$
$$\mathrm{Cl}(\mathcal{O}) = \text{class group corresponding to the Frobenius orientation.}$$

Consider some orbit of the action of $\mathrm{Cl}(\mathcal{O})$ on S.

The power of self-pairings

$$S = \{\text{elliptic curves over } \mathbb{F}_q\text{, oriented by their Frobenius}\}.$$
$$\mathrm{Cl}(\mathcal{O}) = \text{class group corresponding to the Frobenius orientation.}$$

Consider some orbit of the action of $\mathrm{Cl}(\mathcal{O})$ on S.

What can be done with self-pairings?

- Given E and $[\mathfrak{a}]E$, recover $\mathfrak{a}$ if $\Delta_{\mathcal{O}}$ has a factor ℓ^{2r} and $N(\mathfrak{a}) < \ell^{2r}$. [1, Prop. 6.3]

THE POWER OF SELF-PAIRINGS

$$S = \{\text{elliptic curves over } \mathbb{F}_q, \text{ oriented by their Frobenius}\}.$$
$$\mathrm{Cl}(\mathcal{O}) = \text{class group corresponding to the Frobenius orientation.}$$

Consider some orbit of the action of $\mathrm{Cl}(\mathcal{O})$ on S.

What can be done with self-pairings?

- Given E and $[\mathfrak{a}]E$, recover $\mathfrak{a}$ if $\Delta_{\mathcal{O}}$ has a factor ℓ^{2r} and $N(\mathfrak{a}) < \ell^{2r}$. [1, Prop. 6.3]
- If q is 1 mod 4 and trace of Frobenius is 0 mod 4, breaking the *DDH problem*:

Distinguish the tuple	$(E, [\mathfrak{a}]E, [\mathfrak{b}]E, [\mathfrak{a}\mathfrak{b}]E)$
from the tuple	$(E, [\mathfrak{a}]E, [\mathfrak{b}]E, [\mathfrak{c}]E)$.

THE POWER OF SELF-PAIRINGS

$$S = \{\text{elliptic curves over } \mathbb{F}_q, \text{ oriented by their Frobenius}\}.$$
$$\mathrm{Cl}(\mathcal{O}) = \text{class group corresponding to the Frobenius orientation.}$$

Consider some orbit of the action of $\mathrm{Cl}(\mathcal{O})$ on S.

What can be done with self-pairings?

- Given E and $[\mathfrak{a}]E$, recover $\mathfrak{a}$ if $\Delta_{\mathcal{O}}$ has a factor ℓ^{2r} and $N(\mathfrak{a}) < \ell^{2r}$. [1, Prop. 6.3]
- If q is 1 mod 4 and trace of Frobenius is 0 mod 4, breaking the *DDH problem*:

  Distinguish the tuple $(E, [\mathfrak{a}]E, [\mathfrak{b}]E, [\mathfrak{a}\mathfrak{b}]E)$

  from the tuple $(E, [\mathfrak{a}]E, [\mathfrak{b}]E, [\mathfrak{c}]E)$.

- Walking the ℓ-isogeny volcano.

The hoped-for power of self-pairings

$S = \{$elliptic curves over $\mathbb{F}_q$, oriented by ~~their Frobenius~~ some endomorphism$\}$.

$\mathrm{Cl}(\mathcal{O}) =$ class group corresponding to the ~~Frobenius~~ orientation.

Consider some orbit of the action of $\mathrm{Cl}(\mathcal{O})$ on S.

The hoped-for power of self-pairings

$$S = \{\text{elliptic curves over } \mathbb{F}_q\text{, oriented by } \sout{\text{their Frobenius}}\ \text{some endomorphism}\}.$$

$$\mathrm{Cl}(\mathcal{O}) = \text{class group corresponding to the } \sout{\text{Frobenius}}\ \text{orientation.}$$

Consider some orbit of the action of $\mathrm{Cl}(\mathcal{O})$ on S.

What ~~can~~ might be done with self-pairings?

- Given E and $[\mathfrak{a}]E$, recover $\mathfrak{a}$ if $\Delta_{\mathcal{O}}$ has a factor ℓ^r and $N(\mathfrak{a}) < \ell^r$.

The hoped-for power of self-pairings

$$S = \{\text{elliptic curves over } \mathbb{F}_q, \text{ oriented by } \sout{\text{their Frobenius}}$$
$$\text{some endomorphism}\}.$$
$$\mathrm{Cl}(\mathcal{O}) = \text{class group corresponding to the } \sout{\text{Frobenius}} \text{ orientation.}$$

Consider some orbit of the action of $\mathrm{Cl}(\mathcal{O})$ on S.

What ~~can~~ might be done with self-pairings?

- Given E and $[\mathfrak{a}]E$, recover $\mathfrak{a}$ if $\Delta_{\mathcal{O}}$ has a factor ℓ^r and $N(\mathfrak{a}) < \ell^r$.
- Breaking the DDH problem,~~if q is 1 mod 4 and trace of Frobenius is 0 mod 4,~~ (under suitable assumptions on $\Delta_{\mathcal{O}}$).

The hoped-for power of self-pairings

$$S = \{\text{elliptic curves over } \mathbb{F}_q, \text{ oriented by } \sout{\text{their Frobenius}}\ \text{some endomorphism}\}.$$

$$\mathrm{Cl}(\mathcal{O}) = \text{class group corresponding to the } \sout{\text{Frobenius}} \text{ orientation.}$$

Consider some orbit of the action of $\mathrm{Cl}(\mathcal{O})$ on S.

What ~~can~~ might be done with self-pairings?

- Given E and $[\mathfrak{a}]E$, recover $\mathfrak{a}$ if $\Delta_{\mathcal{O}}$ has a factor ℓ^r and $N(\mathfrak{a}) < \ell^r$.
- Breaking the DDH problem,~~if q is 1 mod 4 and trace of Frobenius is 0 mod 4,~~ (under suitable assumptions on $\Delta_{\mathcal{O}}$).
- Walking the ℓ-isogeny volcano.

Appendix 4: Our main result (full version)

Self-pairings compatible with all oriented endomorphisms

From [Cas+23b, Prop. 4.8].

Proposition 1

$\mathcal{O}$ = imaginary quadratic order. *$\Delta_{\mathcal{O}}$ = discriminant of $\mathcal{O}$.*

E = $\mathcal{O}$-oriented EC over $\mathbb{F}_q$. *G = cyclic subgroup of E.*

f = self-pairing $G \to \mathbb{F}_q^*$. *$m = \#\langle f(G)\rangle$.*

Assume that f is compatible with $\mathcal{O}$-oriented endomorphisms. Then

- $\mathrm{char}(\mathbb{F}_q) \nmid m$,
- $m \mid \Delta_{\mathcal{O}}$,
- *Writing $\Delta_{\mathcal{O}} = -2^r n$ for n odd, we have:*
  - *if $r = 2$ then $m \mid \Delta_{\mathcal{O}}/2$,*
  - *if $r \geq 3$ then $m \mid \Delta_{\mathcal{O}}/4$.*

Self-pairings compatible with (most!) oriented endomorphisms

From [Cas+23b, Prop. A.1].

Proposition 2

$\mathcal{O}$ = *imaginary quadratic order.* $\Delta_{\mathcal{O}}$ = *discriminant of* $\mathcal{O}$.

E = $\mathcal{O}$*-oriented EC over* $\mathbb{F}_q$. G = *cyclic subgroup of* E.

f = *self-pairing* $G \to \mathbb{F}_q^*$. $m = \#\langle f(G) \rangle$.

Assume that f *is compatible with* $\mathcal{O}$*-oriented endomorphisms of norm coprime with* m*. Then*

- $\mathrm{char}(\mathbb{F}_q) \nmid m$,
- ~~$m \mid \Delta_{\mathcal{O}}$,~~
- *Writing* $\Delta_{\mathcal{O}} = -2^r n$ *for* n *odd, we have:*
    - *if* $r = 0$ *and* $n \equiv 3 \bmod 8$ *then* $m \mid \Delta_{\mathcal{O}}$,
    - *if* $r = 2$ *and* $n \equiv 3 \bmod 4$ *then* $m \mid \Delta_{\mathcal{O}}/2$,
    - *if* $r = 3, 4$ *then* $m \mid \Delta_{\mathcal{O}}/4$,
    - *if* $r = 0$ *and* $n \equiv 7 \bmod 8$ *then* $m \mid 2\Delta_{\mathcal{O}}$,
    - *if* $r = 2$ *and* $n \equiv 1 \bmod 4$ *then* $m \mid \Delta_{\mathcal{O}}$,
    - *if* $r \geq 5$ *then* $m \mid \Delta_{\mathcal{O}}/2$.