Isogeny-Based Cryptography

Post-quantum crypto from elliptic curves

Jonathan Komada Eriksen

Elliptic curves

An **elliptic curve** is a smooth, projective curves of genus 1

Elliptic curves

An **elliptic curve** is a smooth, projective curves of genus 1

Elliptic curves

An **elliptic curve** is a smooth, projective curves of genus 1

Riemann-Roch

Every elliptic curve over k is isomorphic to a plane curve of the form

$$E/k : y^2 = x^3 + ax + b$$

Elliptic curves

An **elliptic curve** is a smooth, projective curves of genus 1

Riemann-Roch

Every elliptic curve over k is isomorphic to a plane curve of the form

$$E/k : y^2 = x^3 + ax + b$$

Point at infinity

$\{(x,y) \in \bar{k} \times \bar{k} \mid y^2 = x^3 + ax + b\} \cup \{O_E\}$

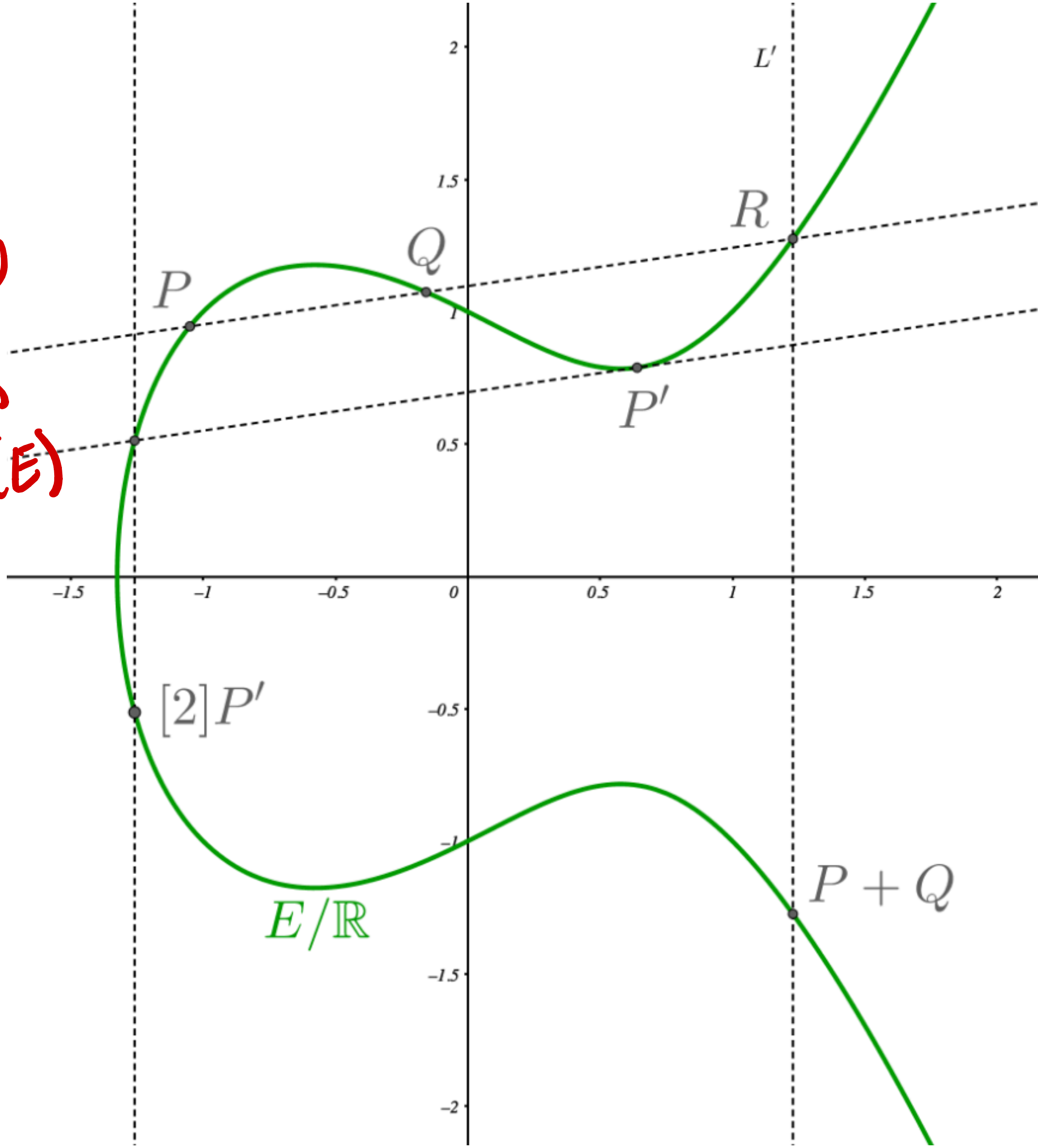
The addition law

Map given locally by rational functions from k(E)

There is a morphism

$$+ : E \times E \to E$$

Turning the points on E into an abelian group!



The addition law

Map given locally by rational functions from $k(E)$

There is a morphism

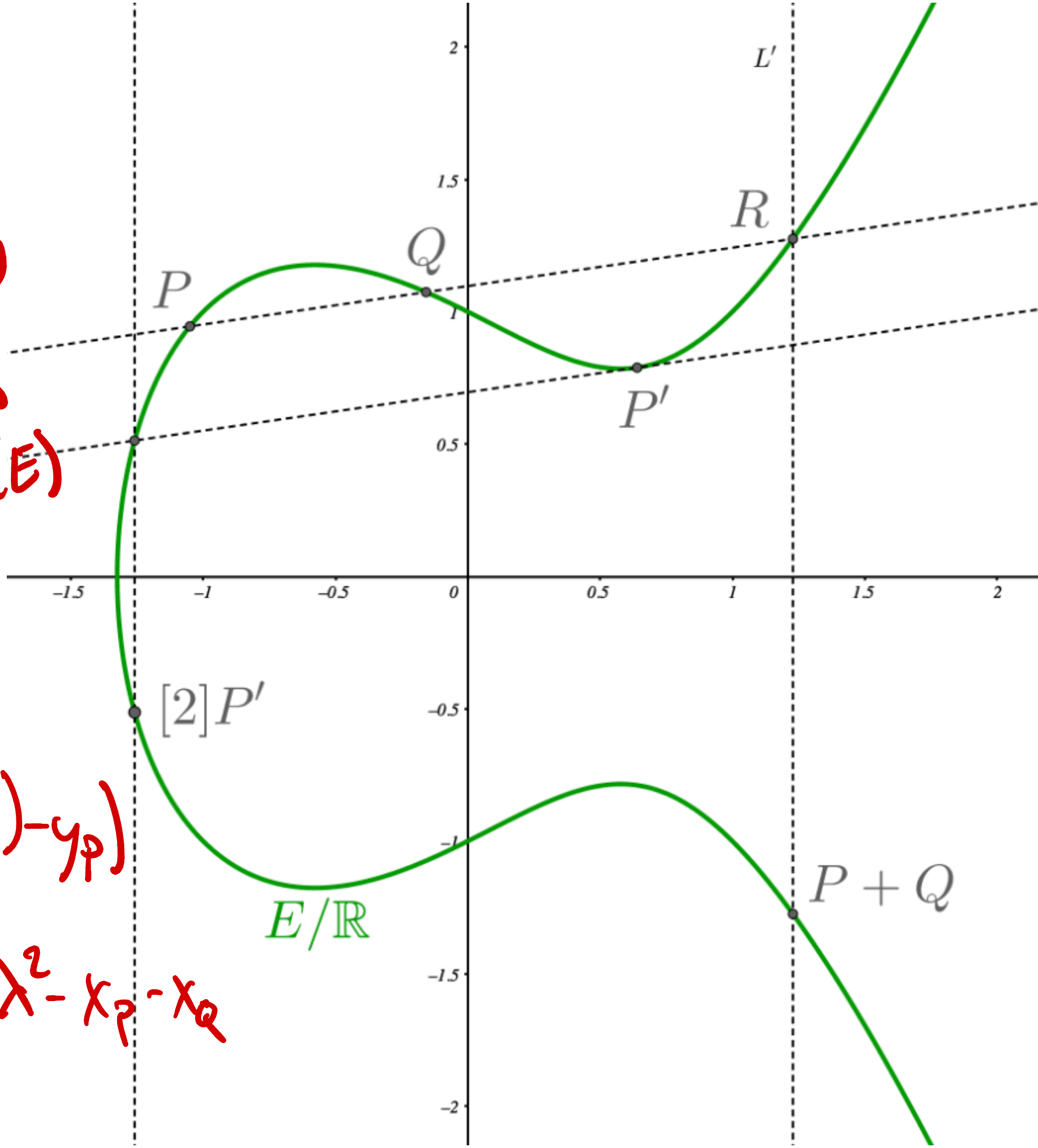
$$+ : E \times E \to E$$

Turning the points on E into an abelian group!

$(x_P, y_P) + (x_Q, y_Q) = (X, \lambda(x_P - X) - y_P)$

where

$\lambda = \frac{(y_P - y_Q)}{(x_P - x_Q)}$, $X = \lambda^2 - x_P - x_Q$



The addition law

There is a morphism

Map given locally by rational functions from $k(E)$

$$+ : E \times E \to E$$

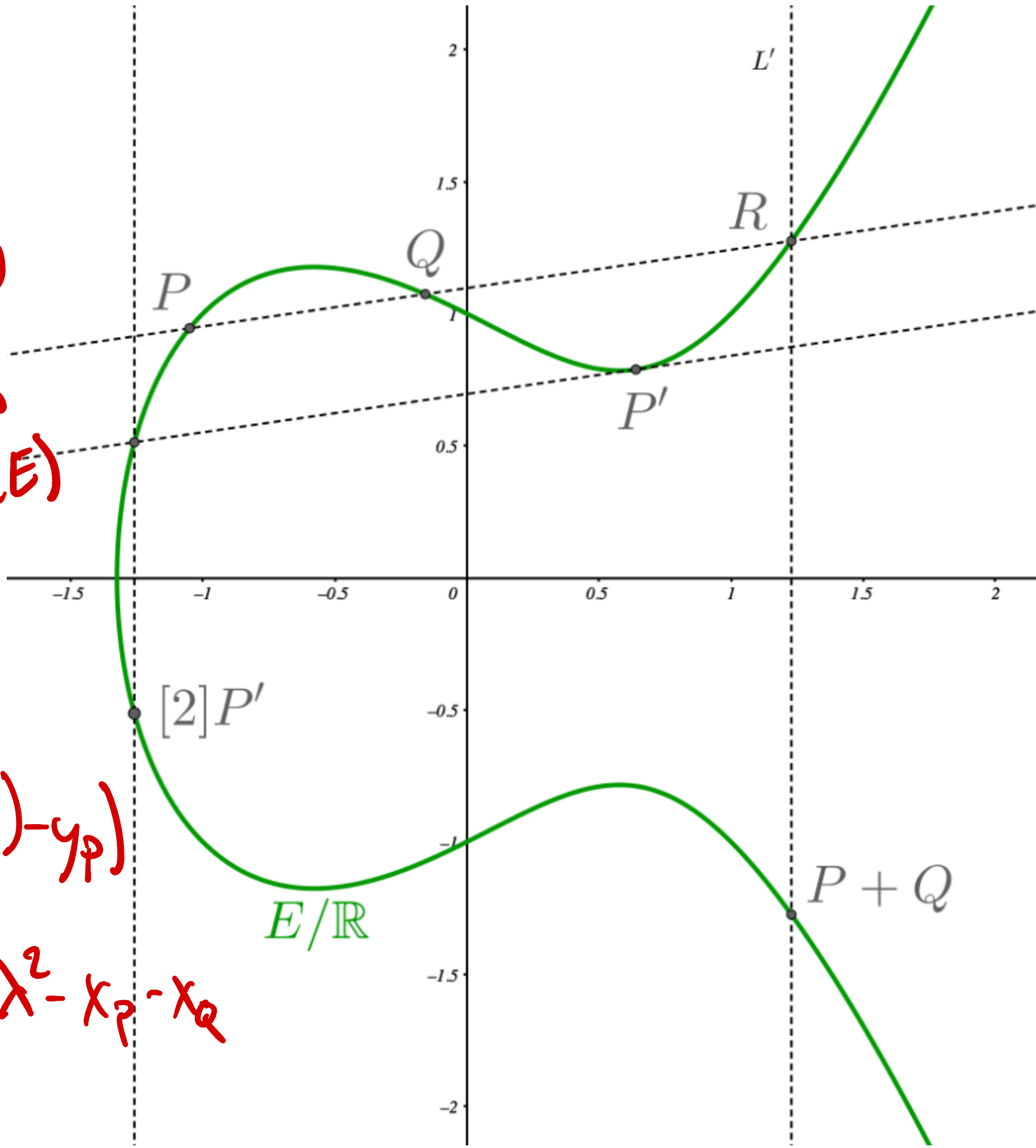
Turning the points on E into an abelian group!

$$(x_P, y_P) + (x_Q, y_Q) = (X, \lambda(x_P - X) - y_P)$$

where

$$\lambda = \frac{(y_P - y_Q)}{(x_P - x_Q)}, \quad X = \lambda^2 - x_P - x_Q$$

NB! $x_P \neq x_Q$

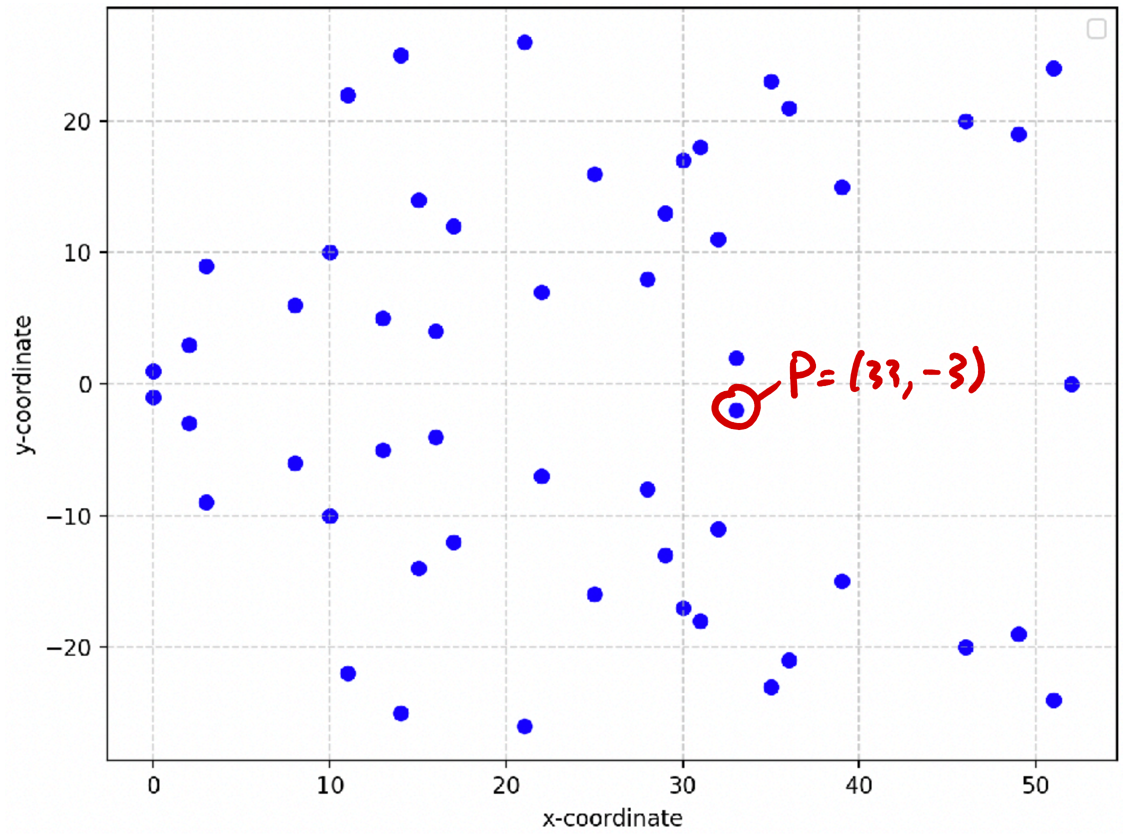


Classic ECC

Public : $E/\mathbb{F}_p$, $P \in E$

Switching to

$$E/\mathbb{F}_{53} : y^2 = x^3 + 1$$



Classic ECC

Public : $E/\mathbb{F}_p$, $P \in E$

Alice

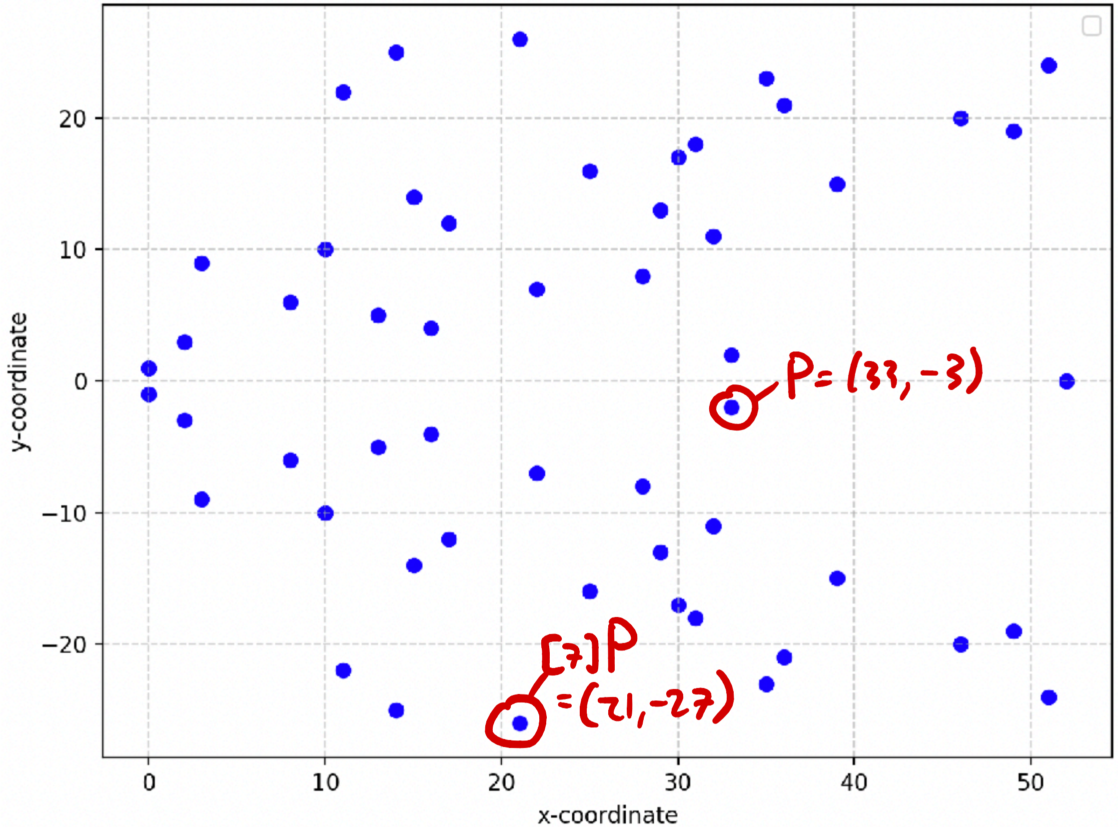
Bob

Secret $a \in \mathbb{Z}$

$[a]P$

Switching to

$$E/\mathbb{F}_{53} : y^2 = x^3 + 1$$



Classic ECC

Public : $E/\mathbb{F}_p$, $P \in E$

Alice

Secret $a \in \mathbb{Z}$

$[a]P$

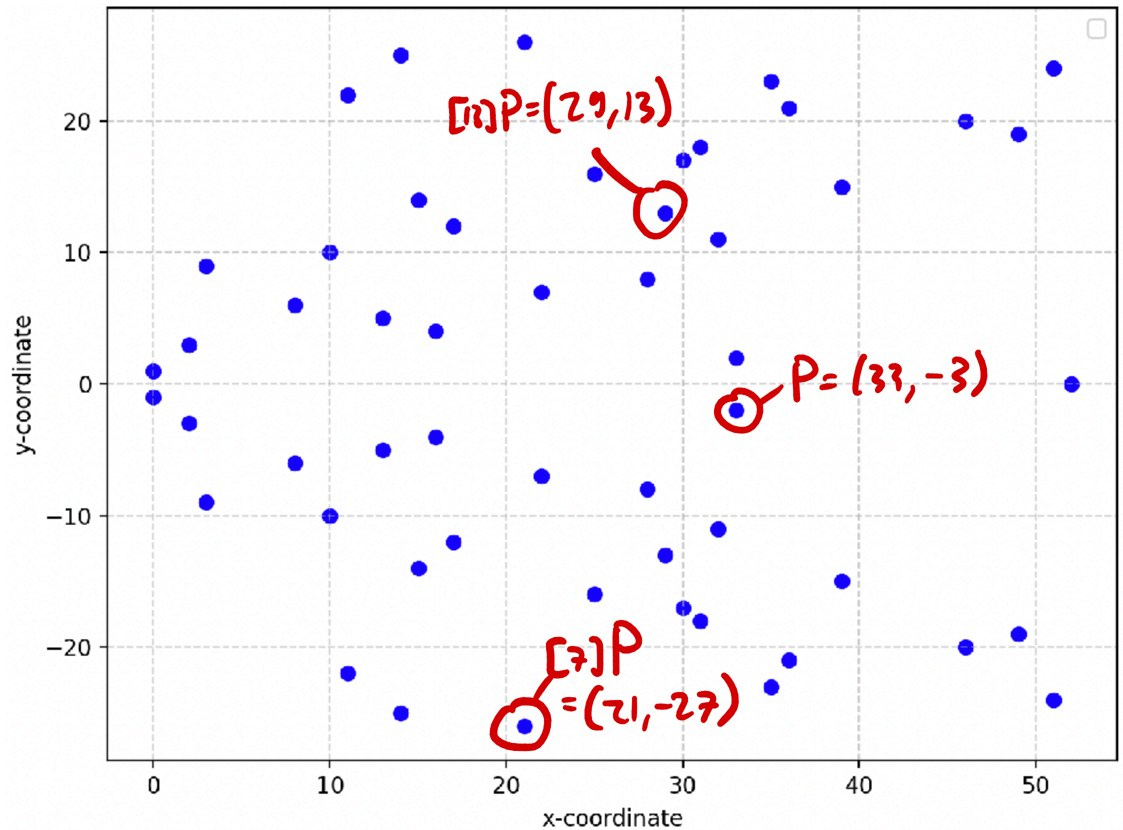
$[b]P$

Bob

Secret $b \in \mathbb{Z}$

Switching to

$$E/\mathbb{F}_{53} : y^2 = x^3 + 1$$



Classic ECC

Public: $E/\mathbb{F}_p$, $P \in E$

Alice

Secret $a \in \mathbb{Z}$

Bob

Secret $b \in \mathbb{Z}$

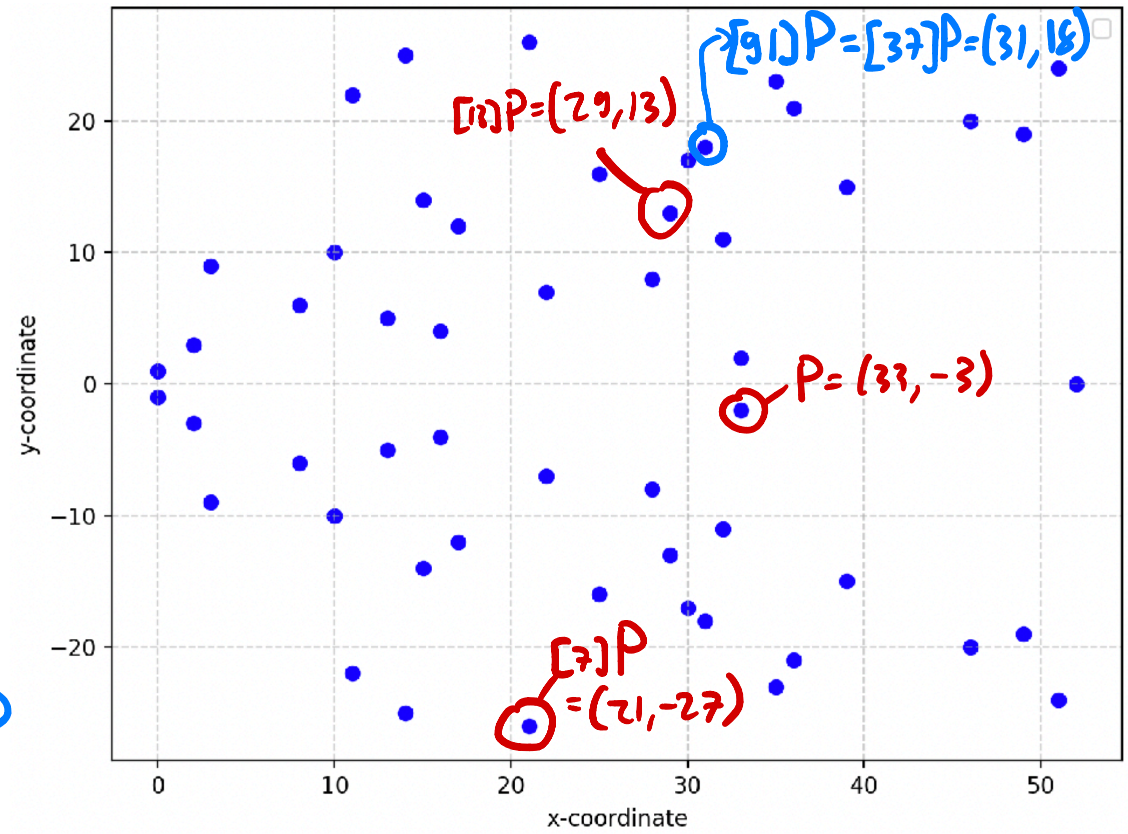
$\xrightarrow{[a]P}$

$\xleftarrow{[b]P}$

key $[a][b]P$ = key $[b][a]P$

Switching to

$$E/\mathbb{F}_{53} : y^2 = x^3 + 1$$



Isogenies

An **isogeny** is a morphism

$$\phi : E_1 \to E_2$$

With finite kernel, satisfying $\phi(0_{E_1}) = 0_{E_2}$

Isogenies

An **isogeny** is a morphism

$$\phi : E_1 \to E_2$$

With finite kernel, satisfying $\phi(0_{E_1}) = 0_{E_2}$

Thm: $\forall P, Q \in E_1$, $\phi(P+Q) = \phi(P) + \phi(Q)$!

Isogenies

An **isogeny** is a morphism

$$\phi : E_1 \to E_2$$

With finite kernel, satisfying $\phi(0_{E_1}) = 0_{E_2}$

Thm: $\forall P, Q \in E_1$, $\phi(P+Q) = \phi(P) + \phi(Q)$!

For (separable) isogenies, we have $\deg \phi = \#\ker \phi$

In fact, there is a bijection between
finite subgroups on E and **separable isogenies from E**

Isogenies

sufficient condition:
deg ϕ coprime to char(k)

An **isogeny** is a morphism

$$\phi : E_1 \to E_2$$

With finite kernel, satisfying $\phi(0_{E_1}) = 0_{E_2}$

Thm: $\forall P, Q \in E_1$, $\phi(P+Q) = \phi(P) + \phi(Q)$!

For (separable) isogenies, we have $\deg \phi = \# \ker \phi$

In fact, there is a bijection between
finite subgroups on E and **separable isogenies from E**

Isogenies

NB! Algorithm for computing ϕ given $\ker\phi < E$.

$(O(\sqrt{\#\ker\phi}))$

sufficient condition: $\deg\phi$ coprime to char(k)

An **isogeny** is a morphism

$$\phi : E_1 \to E_2$$

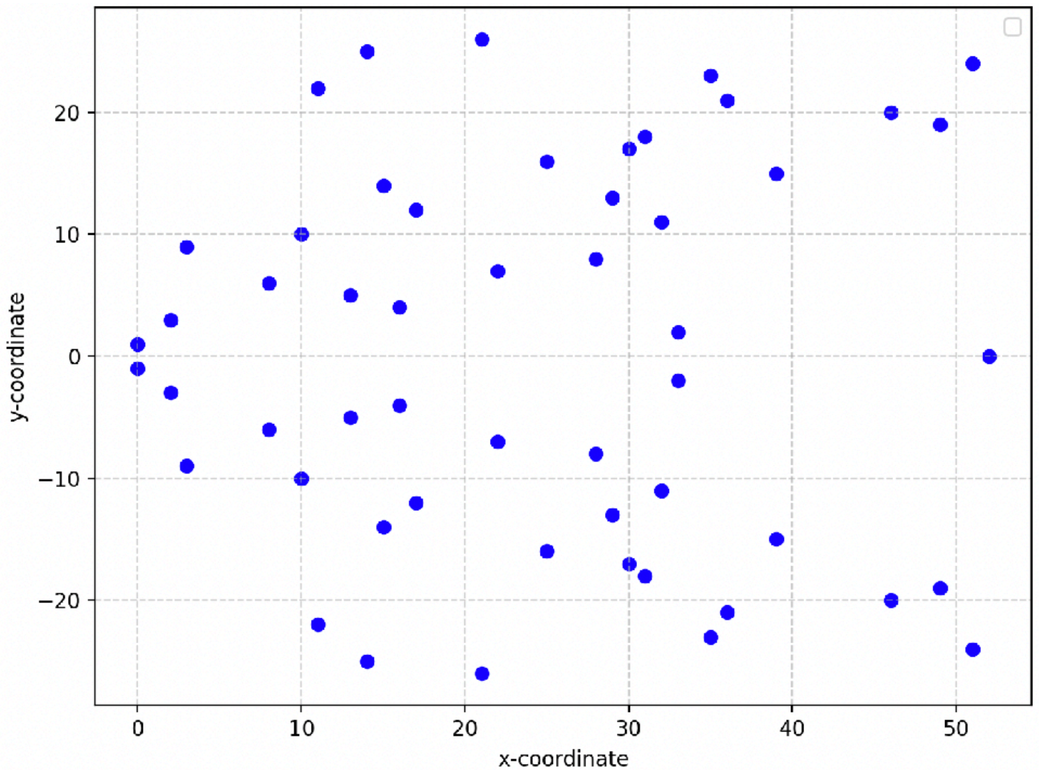
With finite kernel, satisfying $\phi(0_{E_1}) = 0_{E_2}$

Thm: $\forall P, Q \in E_1$, $\phi(P+Q) = \phi(P) + \phi(Q)$!

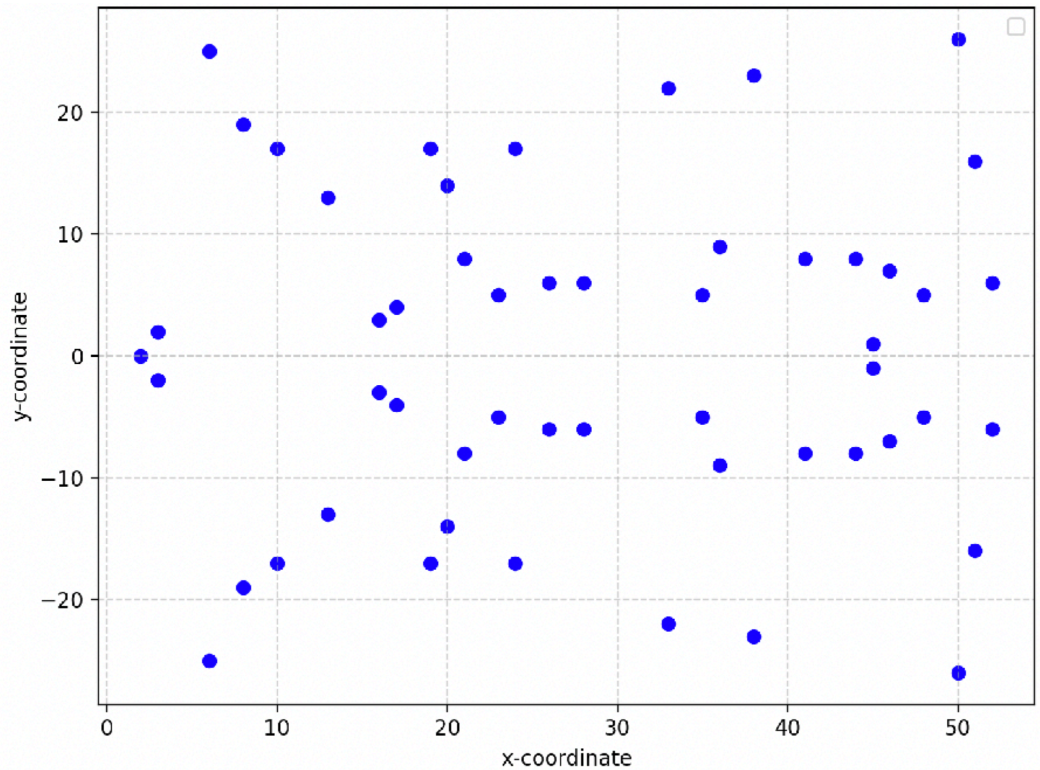
For (separable) isogenies, we have $\deg \phi = \#\ker\phi$

In fact, there is a bijection between
finite subgroups on E and **separable isogenies from E**

$$E_1 : y^2 = x^3 + 1$$

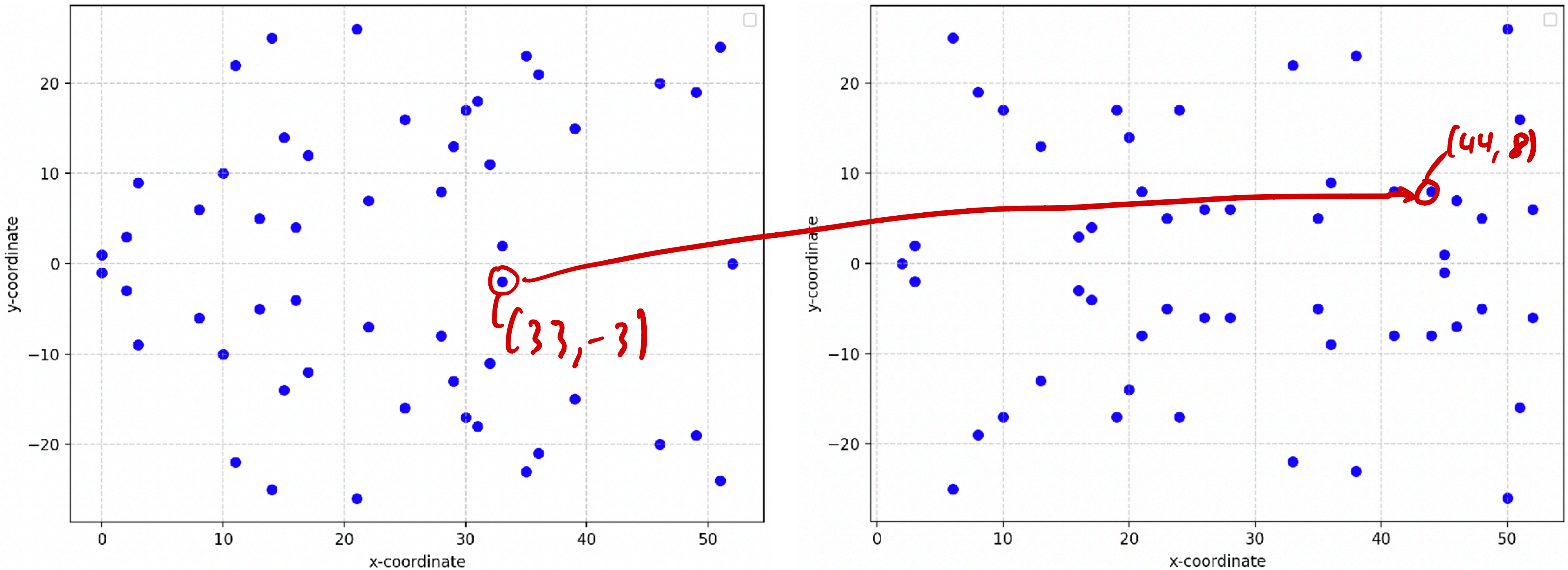


$$E_2 : y^2 = x^3 + 38x + 22$$



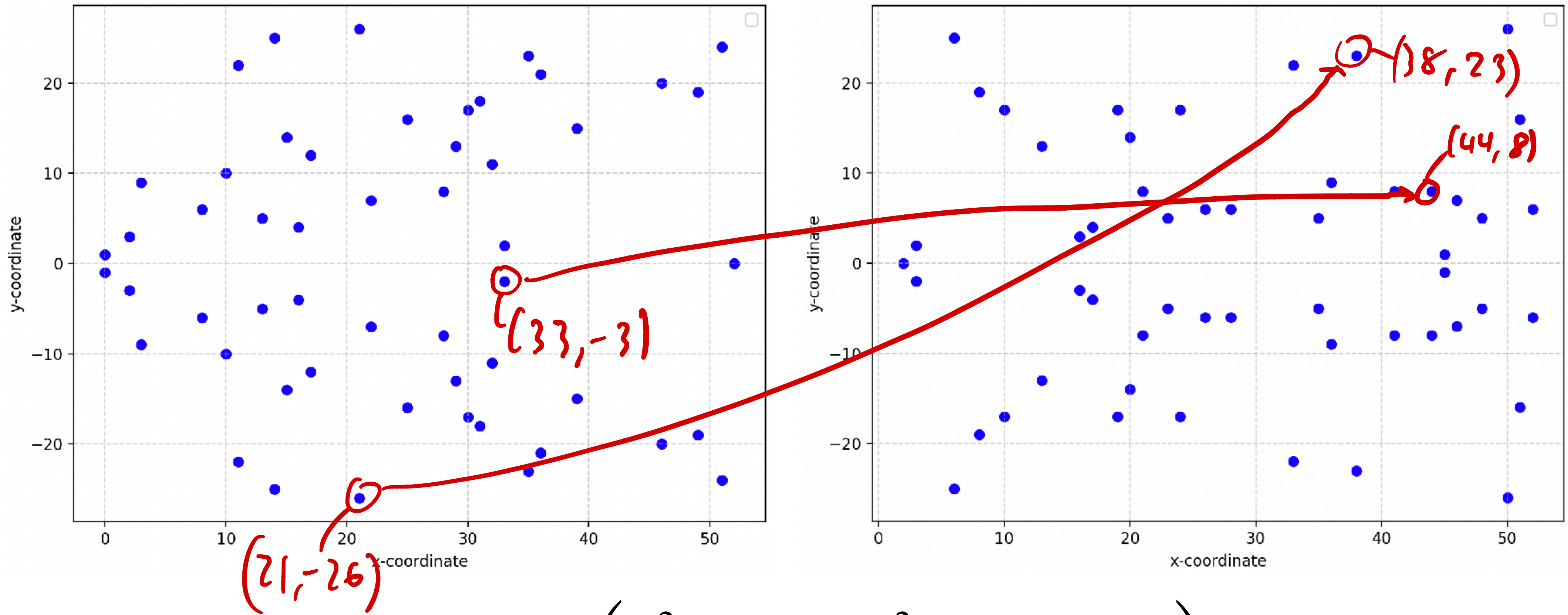
$$\phi((x, y)) = \left(\frac{x^2 + x + 3}{x + 1}, \frac{x^2 y + 2xy - 2y}{x^2 + 2x + 1} \right)$$

$$E_1 : y^2 = x^3 + 1 \qquad E_2 : y^2 = x^3 + 38x + 22$$



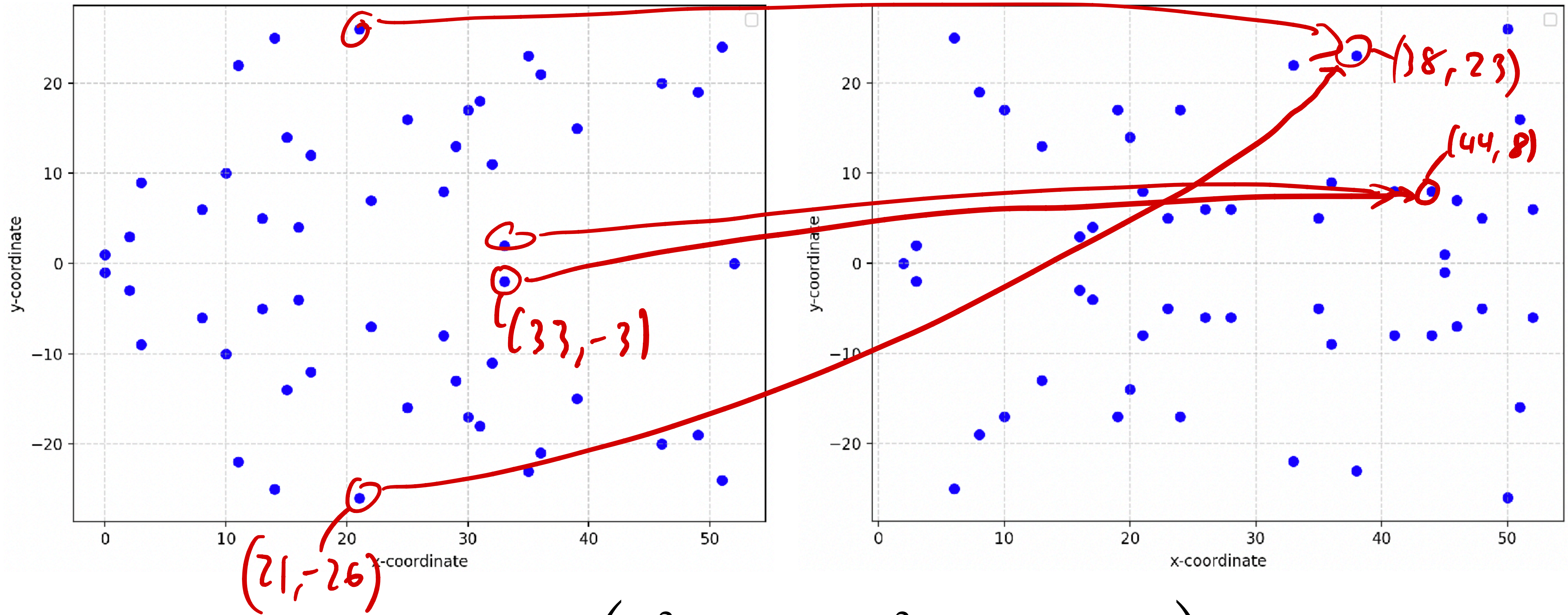
$$\phi((x,y)) = \left(\frac{x^2 + x + 3}{x + 1}, \frac{x^2y + 2xy - 2y}{x^2 + 2x + 1} \right)$$

$$E_1 : y^2 = x^3 + 1 \qquad E_2 : y^2 = x^3 + 38x + 22$$



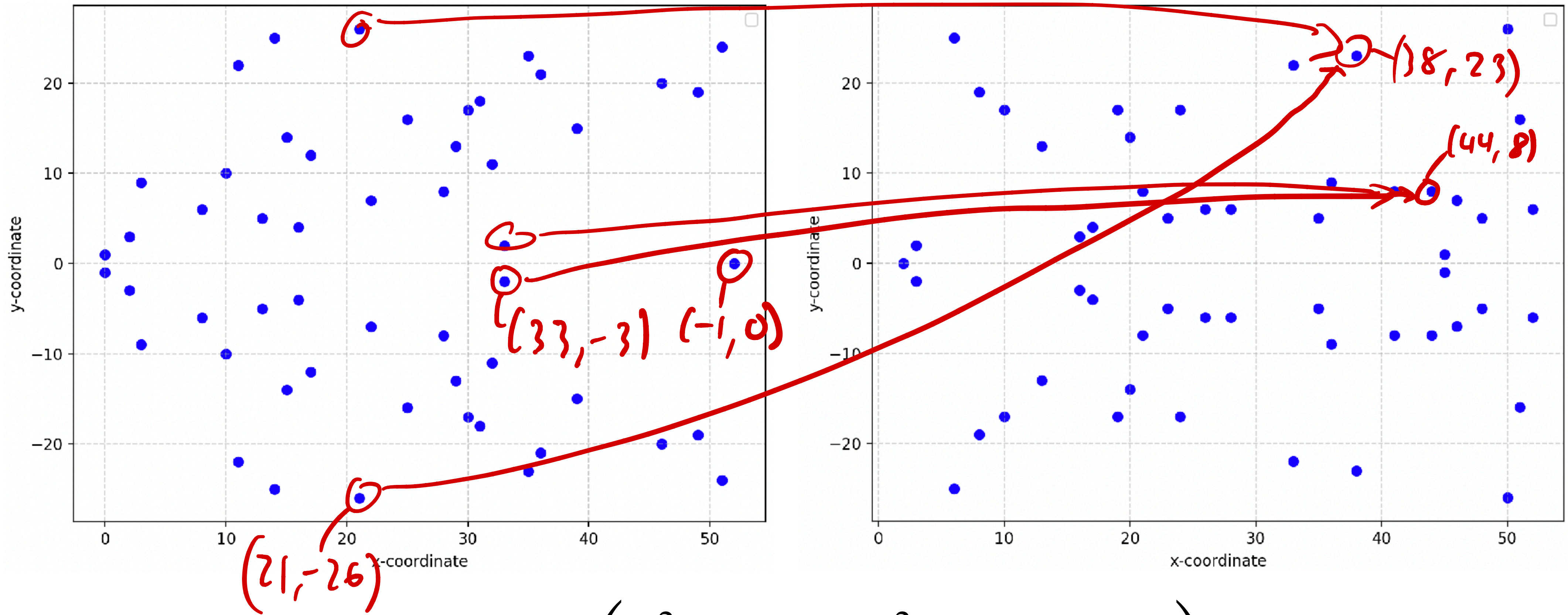
$$\phi((x,y)) = \left(\frac{x^2 + x + 3}{x + 1}, \frac{x^2y + 2xy - 2y}{x^2 + 2x + 1} \right)$$

$$E_1 : y^2 = x^3 + 1 \qquad\qquad E_2 : y^2 = x^3 + 38x + 22$$



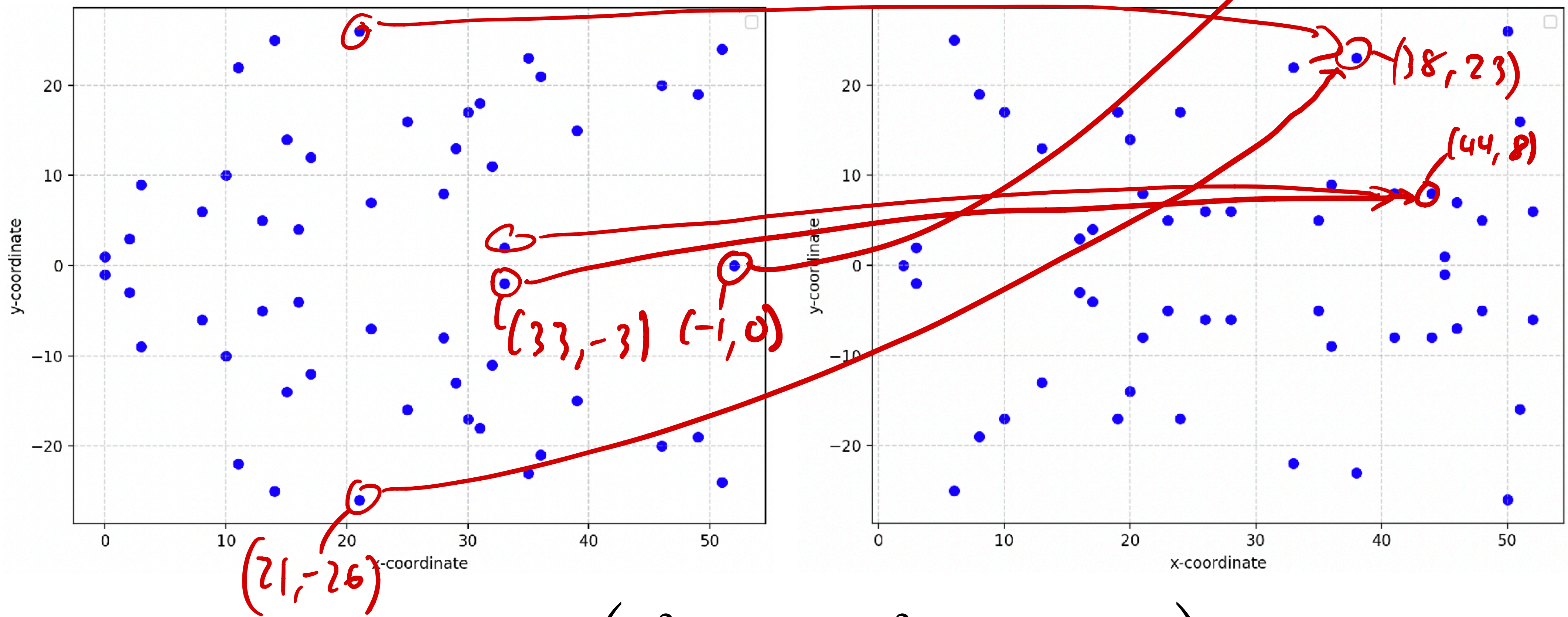
$$\phi((x,y)) = \left(\frac{x^2 + x + 3}{x + 1}, \frac{x^2y + 2xy - 2y}{x^2 + 2x + 1} \right)$$

$$E_1 : y^2 = x^3 + 1 \qquad E_2 : y^2 = x^3 + 38x + 22$$



$$\phi((x, y)) = \left(\frac{x^2 + x + 3}{x + 1}, \frac{x^2 y + 2xy - 2y}{x^2 + 2x + 1} \right)$$

$$E_1 : y^2 = x^3 + 1 \qquad\qquad E_2 : y^2 = x^3 + 38x + 22$$



$$\phi((x,y)) = \left(\frac{x^2 + x + 3}{x + 1}, \frac{x^2y + 2xy - 2y}{x^2 + 2x + 1} \right)$$

Other isogenies

$$[m]P = P + \ldots + P$$

$$\ker[m] = E[m] \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

(for $p \nmid m$)

Other isogenies

$$[m]P = P + \ldots + P$$

$$\ker[m] = E[m] \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

(for $p \nmid m$)

So $\deg [m] = m^2$

Other isogenies

$$[m]P = P + \ldots + P$$

$$\ker[m] = E[m] \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

(for $p \nmid m$)

So $\deg [m] = m^2$

(Note: $E(k)[m] \subseteq E[m]$, but not equal in general)

Other isogenies

$$[m]P = P + \ldots + P$$

$$\ker[m] = E[m] \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

→ (for $p \nmid m$)

So $\deg [m] = m^2$

(Note: $E(k)[m] \subseteq E[m]$, but not equal in general)

$$\pi((x, y)) = (x^p, y^p)$$

→ Frobenius (inseparable!)

Other isogenies

$$[m]P = P + \ldots + P$$

$$\ker[m] = E[m] \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$ (for $p \nmid m$)

So $\deg[m] = m^2$

(Note: $E(k)[m] \subseteq E[m]$, but not equal in general)

$$\pi((x, y)) = (x^p, y^p)$$ → Frobenius (inseparable!)

Notice: $[m] \in \mathrm{End}(E) = \{\phi : E \to E \mid \phi \text{ isogeny}\} \cup \{0\}$

If $E/\mathbb{F}_p$, we also have $\pi \in \mathrm{End}(E)$.

The endomorphism ring

($E/\mathbb{F}_p$, π frobenius on E)

$$\mathbb{Z}[\pi] \subseteq \mathrm{End}(E)$$

The endomorphism ring

($E/\mathbb{F}_p$, π frobenius on E)

$$\mathbb{Z}[\pi] \subseteq \mathrm{End}(E)$$

End(E) has a ring structure!

$$(\phi+\psi)(P) = \phi(P)+\psi(P)$$

$$(\phi\psi)(P) = \phi(\psi(P))$$

The endomorphism ring

($E/\mathbb{F}_p$, π frobenius on E)

$$\mathbb{Z}[\pi] \subseteq \mathrm{End}(E)$$

End(E) has a ring structure!

For

$$E/\mathbb{F}_{53} : y^2 = x^3 + 1$$

It turns out that $\pi^2 = [-p]$, thus

$$\iota : \mathbb{Z}\left[\sqrt{-p}\right] \hookrightarrow \mathrm{End}(E)$$

→ Ring-homomorphism

$$i(a + b\sqrt{-p}) = [a] + [b] \circ \pi$$

Imaginary quadratic orders

Numberfield $K \supset \mathbb{Q}$

$\mathbb{Z}[\sqrt{-n}]$ are examples of (imaginary quadratic) orders

f.g. $\mathbb{Z}$-module $\underline{O} \subset K$ with $\mathbb{Q} \otimes \underline{O} = K$

For quadratic number fields K, there is a **maximal order** $\mathfrak{O}_K$

Further, every order $\mathfrak{O}$ in K is of the form

$$\mathfrak{O} = \mathbb{Z} + f\mathfrak{O}_K$$

Imaginary quadratic orders

Numberfield $K \supset \mathbb{Q}$

$\mathbb{Z}[\sqrt{-n}]$ are examples of (imaginary quadratic) orders

f.g. $\mathbb{Z}$-module $\underline{O} \subset K$ with $\mathbb{Q} \otimes \underline{O} = K$

For quadratic number fields K, there is a **maximal order** $\mathfrak{O}_K$

Ring of integers (= Integral closure of $\mathbb{Z}$ in K)

Further, every order $\mathfrak{O}$ in K is of the form

$$\mathfrak{O} = \mathbb{Z} + f\mathfrak{O}_K$$

Imaginary quadratic orders

Numberfield $K \supset \mathbb{Q}$

$\mathbb{Z}[\sqrt{-n}]$ are examples of (imaginary quadratic) orders

f.g. $\mathbb{Z}$-module $\mathcal{O} \subset K$ with $\mathbb{Q} \otimes \mathcal{O} = K$

For quadratic number fields K, there is a **maximal order** $\mathfrak{O}_K$

Ring of integers (= Integral closure of $\mathbb{Z}$ in K)

Further, every order $\mathfrak{O}$ in K is of the form

$$\mathfrak{O} = \mathbb{Z} + f\mathfrak{O}_K$$

"conductor" of $\mathcal{O}$

The Class Group

For any ideal $\mathfrak{a} \subset \mathfrak{O}_K$, we can write

$$\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_r^{e_r}$$

In a unique way (up to ordering)

"unique factorisation of ideals"

($\mathcal{O}_K$ not UFD in general!)

The Class Group

For any ideal $\mathfrak{a} \subset \mathfrak{O}_K$, we can write

$$\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_r^{e_r}$$

In a unique way (up to ordering)

"unique factorisation of ideals"

(O_K not UFD in general)

Adding **fractional ideals** makes $I(\mathfrak{O}_K)$ into a group.

Free group gen. by all the prime ideals

The **class group** is defined as

$$cl(\mathfrak{O}_K) := I(\mathfrak{O}_K)/P(\mathfrak{O}_K)$$

Where $P(\mathfrak{O}_K) < I(\mathfrak{O}_K)$ is the subgroup of principal ideals

The Class Group

For any ideal $\mathfrak{a} \subset \mathfrak{O}_K$, we can write

$$\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_r^{e_r}$$

In a unique way (up to ordering)

"unique factorisation of ideals"
($\mathcal{O}_K$ not UFD in general)

Adding **fractional ideals** makes $I(\mathfrak{O}_K)$ into a group.

Free group gen. by all the prime ideals

The **class group** is defined as

$$cl(\mathfrak{O}_K) := I(\mathfrak{O}_K)/P(\mathfrak{O}_K)$$

Where $P(\mathfrak{O}_K) < I(\mathfrak{O}_K)$ is the subgroup of principal ideals

So $[\mathfrak{a}] = [\mathfrak{b}] \iff \alpha\mathfrak{a} = \mathfrak{b}$ for some $\alpha \in K$

Example

Can be computed using binary quadratic ~~forms~~ forms and Gauss composition.

Let $\pi^2 = -53$

$cl(\mathbb{Z}[\pi])$ can be given the representatives

$$[\langle 1 \rangle], [\langle 2, 1-\pi \rangle], [\langle 3, \pi - 1 \rangle], [\langle 13, \pi - 5 \rangle], [\langle 17, \pi - 7 \rangle], [\langle 23, \pi - 4 \rangle]$$

Example

Can be computed using binary quadratic forms and Gauss composition.

Let $\pi^2 = -53$

$cl(\mathbb{Z}[\pi])$ can be given the representatives

$$[\langle 1\rangle], [\langle 2,1-\pi\rangle], [\langle 3,\pi-1\rangle], [\langle 13,\pi-5\rangle], [\langle 17,\pi-7\rangle], [\langle 23,\pi-4\rangle]$$

$[\langle 1\rangle]$

$[\langle 23, \pi-4\rangle]$ $\qquad$ $[\langle 3, \pi-1\rangle]$

C_6

$[\langle 13, \pi-5\rangle]$ $\qquad$ $[\langle 17, \pi-7\rangle]$

$[\langle 2, \pi-1\rangle]$

Class Group Action

Given $\mathfrak{a} \subset \mathbb{Z}[\pi]$ we can define

$$E[\mathfrak{a}] = \{P \in E \mid \alpha(P) = 0_E, \forall \alpha \in \mathfrak{a}\}$$

And set $\phi_{\mathfrak{a}}$ to be **the** isogeny with kernel $E[\mathfrak{a}]$

Class Group Action

Given $\mathfrak{a} \subset \mathbb{Z}[\pi]$ we can define

$$E[\mathfrak{a}] = \{P \in E \mid \alpha(P) = 0_E, \forall \alpha \in \mathfrak{a}\}$$

And set $\phi_{\mathfrak{a}}$ to be **the** isogeny with kernel $E[\mathfrak{a}]$

$\mathfrak{a} = \langle 2, \pi - 1 \rangle$

$E[\mathfrak{a}] = \ker[2] \cap \ker(\pi - [1])$

Class Group Action

Given $\mathfrak{a} \subset \mathbb{Z}[\pi]$ we can define

$$E[\mathfrak{a}] = \{P \in E \mid \alpha(P) = 0_E, \forall \alpha \in \mathfrak{a}\}$$

And set $\phi_{\mathfrak{a}}$ to be **the** isogeny with kernel $E[\mathfrak{a}]$

$\mathfrak{a} = \langle 2, \pi - 1 \rangle$

$E[\mathfrak{a}] = \ker[2] \cap \ker(\pi - [1])$

$= E[2] \cap E(\mathbb{F}_p)$

$P \in \ker \pi - [1]$

$\Updownarrow$

$\pi(P) - P = 0$

$\pi(P) = P$

$\Updownarrow$

$P \in E(\mathbb{F}_p)$

Class Group Action

Given $\mathfrak{a} \subset \mathbb{Z}[\pi]$ we can define

$$E[\mathfrak{a}] = \{P \in E \mid \alpha(P) = 0_E, \forall \alpha \in \mathfrak{a}\}$$

And set $\phi_{\mathfrak{a}}$ to be **the** isogeny with kernel $E[\mathfrak{a}]$

$\mathfrak{a} = \langle 2, \pi - 1 \rangle$

$E[\mathfrak{a}] = \ker[2] \cap \ker(\pi - [1])$

$= E[2] \cap E(\mathbb{F}_p)$

$= E(\mathbb{F}_p)[2]$

$\Rightarrow \phi_{\mathfrak{a}}$ is the same isogeny we looked at before!

$P \in \ker \pi - [1]$

$\Updownarrow$

$\pi(P) - P = 0$

$\pi(P) = P$

$\Updownarrow$

$P \in E(\mathbb{F}_p)$

Class Group Action

$\phi_{\mathfrak{a}}$

$$y^2 = x^3 + 1$$

$$\downarrow$$

$$y^2 = x^3 + 38x + 22$$

Class Group Action

$\phi_{\mathfrak{a}}$

$$y^2 = x^3 + 1$$

$$y^2 = x^3 + 38x + 22$$

Class Group Action

ϕ_a ϕ_b, $b = \langle 3, \bar{\pi} - 1 \rangle$

$$y^2 = x^3 + 1$$

$$y^2 = x^3 + 26$$

$$y^2 = x^3 + 38x + 22$$

Class Group Action

ϕ_a ϕ_b, $b = \langle 3, \pi - 1 \rangle$

$$y^2 = x^3 + 1$$

$$y^2 = x^3 + 26$$

$$y^2 = x^3 + 32x + 6$$

$$y^2 = x^3 + 38x + 22$$

Class Group Action

ϕ_a ϕ_b , $b = \langle 3, \pi - 1 \rangle$

$$y^2 = x^3 + 1$$

$$y^2 = x^3 + 26$$

$$y^2 = x^3 + 32x + 6$$

$$y^2 = x^3 + 38x + 22$$

Class Group Action

$\phi_{\mathfrak{a}}$ $\phi_{\mathfrak{b}}$, $\mathfrak{b} = \langle 3, \pi - 1 \rangle$

$$y^2 = x^3 + 1$$

$$y^2 = x^3 + 22x + 5$$

$$y^2 = x^3 + 26$$

$$y^2 = x^3 + 24x + 42$$

$$y^2 = x^3 + 32x + 6$$

$$y^2 = x^3 + 38x + 22$$

Post-Quantum Diffie-Hellman??

Assume $\mathfrak{O} = \mathrm{End}(E)$, for an imaginary quadratic order $\mathfrak{O}$.
There is a free and transitive group action

$$\star : Cl(\mathfrak{O}) \times Ell \to Ell$$

$$\mathfrak{a} \star E = \phi_{\mathfrak{a}}(E)$$

E/k
with $\mathrm{End}(E) = \underline{\mathfrak{O}}$
(up to isomorphism)

Post-Quantum Diffie-Hellman??

Public: $E/\mathbb{F}_p$, $P \in E$

Alice

Secret $a \in \mathbb{Z}$

Bob

Secret $b \in \mathbb{Z}$

$[a]P$

$[b]P$

key $[a][b]P$ = key $[b][a]P$

$$y^2 = x^3 + 1$$

$$y^2 = x^3 + 22x + 5$$

$$y^2 = x^3 + 26$$

$$y^2 = x^3 + 24x + 42$$

$$y^2 = x^3 + 32x + 6$$

$$y^2 = x^3 + 38x + 22$$

Post-Quantum Diffie-Hellman??

Public : $E/\mathbb{F}_p$

Alice

Secret $[\mathfrak{a}] \in Cl(\mathbb{Z}[\pi])$

$\mathfrak{a} * E$

Bob

E

$$y^2 = x^3 + 1$$

$$y^2 = x^3 + 22x + 5 \qquad y^2 = x^3 + 26$$

$$y^2 = x^3 + 24x + 42 \qquad y^2 = x^3 + 32x + 6$$

$$y^2 = x^3 + 38x + 22$$

$\mathfrak{a} * E$, $\mathfrak{a} = \langle 2, \pi - 1 \rangle$

Post-Quantum Diffie-Hellman??

Public: $E/\mathbb{F}_p$

Alice

Secret $[\mathfrak{a}] \in cl(\mathbb{Z}[\pi])$

$\mathfrak{a} * E$

$\mathfrak{b} * E$

Bob

Secret $[\mathfrak{b}] \in cl(\mathbb{Z}[\pi])$

E

$$y^2 = x^3 + 1$$

$\mathfrak{b} = \langle 3, \pi - 1 \rangle$

$\mathfrak{b} * E$

$$y^2 = x^3 + 22x + 5$$

$$y^2 = x^3 + 26$$

$$y^2 = x^3 + 24x + 42$$

$$y^2 = x^3 + 32x + 6$$

$$y^2 = x^3 + 38x + 22$$

$\mathfrak{a} * E, \quad \mathfrak{a} = \langle 2, \pi - 1 \rangle$

Post-Quantum Diffie-Hellman??

Public: $E/\mathbb{F}_p$

Alice

secret $[\mathfrak{a}] \in cl(\mathbb{Z}[\pi])$

Bob

secret $[\mathfrak{b}] \in cl(\mathbb{Z}[\pi])$

$\mathfrak{a} * E$

$\mathfrak{b} * E$

key $\mathfrak{a} * (\mathfrak{b} * E)$ = key $\mathfrak{b} * (\mathfrak{a} * E)$

E

$$y^2 = x^3 + 1$$

$\mathfrak{b} = \langle 3, \pi - 1 \rangle$

$\mathfrak{b} * E$

$$y^2 = x^3 + 22x + 5$$

$$y^2 = x^3 + 26$$

$$y^2 = x^3 + 24x + 42$$

$\mathfrak{a} * \mathfrak{b} * E$

$$y^2 = x^3 + 32x + 6$$

$$y^2 = x^3 + 38x + 22$$

$\mathfrak{a} * E$, $\mathfrak{a} = \langle 2, \pi - 1 \rangle$

Confession: I've been lying...

$y^2 = x^3 + 1$

For our $E/\mathbb{F}_{53}$, $\mathbb{Z}[\pi] \subsetneq \mathrm{End}(E)$

$\zeta^3 = 1, \ \zeta \neq 1$

$$\omega((x, y)) = (\zeta x, -y)$$

$$\pi \circ \omega = -\omega \circ \pi$$

Confession: I've been lying...

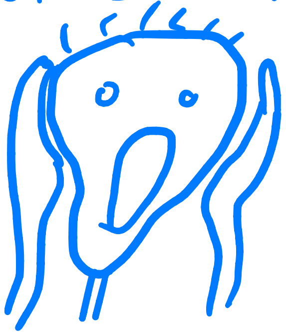
$y^2 = x^3 + 1$

For our $E/\mathbb{F}_{53}$, $\mathbb{Z}[\pi] \subsetneq \mathrm{End}(E)$

$\zeta^3 = 1$, $\zeta \neq 1$

$$\omega((x, y)) = (\zeta x, -y)$$

So $\mathrm{End}(E)$ is not commutative!



$$\pi \circ \omega = -\omega \circ \pi$$

Because $p \equiv 2 \pmod{3}$, so $\zeta \notin \mathbb{F}_p$

Quaternion Algebras

A quaternion algebra (over $\mathbb{Q}$) is something of the form

$$B = \mathbb{Q} + \mathbb{Q}\mathbf{i} + \mathbb{Q}\mathbf{j} + \mathbb{Q}\mathbf{k}$$

$a, b \in \mathbb{Q}^\times$

Satisfying

$$\mathbf{i}^2 = a, \quad \mathbf{j}^2 = b, \quad \mathbf{ij} = \mathbf{k} = -\mathbf{ji}$$

$\mathbb{Z}\langle \pi, \omega \rangle$ is a (maximal) order in a quaternion algebra!

Quaternion Algebras

A quaternion algebra (over $\mathbb{Q}$) is something of the form

$$B = \mathbb{Q} + \mathbb{Q}\mathbf{i} + \mathbb{Q}\mathbf{j} + \mathbb{Q}\mathbf{k}$$

$a, b \in \mathbb{Q}^\times$

Satisfying

$$\mathbf{i}^2 = a, \quad \mathbf{j}^2 = b, \quad \mathbf{ij} = \mathbf{k} = -\mathbf{ji}$$

$\mathbb{Z}\langle \pi, \omega \rangle$ is a (maximal) order in a quaternion algebra!

f.g. $\mathbb{Z}$-module $\mathcal{O}$ with $\mathbb{Q} \otimes \mathcal{O} = B$

B vs. K

(Positive definite) quaternion algebra | (Imaginary quadratic) number field

- Commutative
- Unique maximal order
- Class Group $C(\mathcal{O})$

$$= \{\mathfrak{a} \subseteq \mathcal{O}\}/\sim$$

where

$$\mathfrak{a} \sim \mathfrak{b} \Leftrightarrow \alpha\mathfrak{a} = \mathfrak{b} \text{ for } \alpha \in K$$

B vs. K

(Positive definite) quaternion algebra | (Imaginary quadratic) number field

- Non-commutative

- Commutative
- Unique maximal order
- Class Group $C(\mathcal{O})$

$$= \{\mathfrak{a} \subseteq \mathcal{O}\}/\sim$$

where

$$\mathfrak{a} \sim \mathfrak{b} \Leftrightarrow \alpha\mathfrak{a} = \mathfrak{b}$$

for $\alpha \in K$

B vs. K

(Non-commutative, so integral closure is not closed under multiplication!)

(Positive definite) quaternion algebra | (Imaginary quadratic) number field

- Non-commutative
- Many Maximal orders

- Commutative
- Unique maximal order
- Class Group $C(\mathcal{O})$

$$= \{\mathfrak{a} \subseteq \mathcal{O}\}/\sim$$

where

$$\mathfrak{a} \sim \mathfrak{b} \Leftrightarrow \alpha\mathfrak{a} = \mathfrak{b} \text{ for } \alpha \in K$$

B vs. K

(Positive definite) quaternion algebra	(Imaginary quadratic) number field
- Non-commutative	- Commutative
- Many Maximal orders	- Unique maximal order
- Class Set $(\mathcal{O})$ $= \{ I \subseteq \mathcal{O} \mid I \text{ left ideal} \} / \sim$ where $I \sim J \iff I\alpha = J$ for some $\alpha \in B$	- Class Group $(\mathcal{O})$ $= \{ \mathfrak{a} \subseteq \mathcal{O} \mid \mathfrak{a} \text{ ideal} \} / \sim$ where $\mathfrak{a} \sim \mathfrak{b} \iff \alpha\mathfrak{a} = \mathfrak{b}$ for $\alpha \in K$

B vs. K

Not a group, since multiplication of ideals is not well-behaved in general.

(Positive definite) quaternion algebra | (Imaginary quadratic) number field

- Non-commutative
- Many Maximal orders
- Class Set $(\mathcal{O})$ $= \{ I \subseteq \mathcal{O} \mid I \text{ left ideal} \} / \sim$

where $I \sim J \iff I\alpha = J$ for some $\alpha \in B$

- Commutative
- Unique maximal order
- Class Group $(\mathcal{O})$ $= \{ \mathfrak{a} \subseteq \mathcal{O} \mid \mathfrak{a} \text{ ideal} \} / \sim$

where $\mathfrak{a} \sim \mathfrak{b} \iff \alpha\mathfrak{a} = \mathfrak{b}$ for $\alpha \in K$

The Deuring Correspondence

Ob: Supersingular curves over $\overline{\mathbb{F}}_p$

Morphisms: Isogenies

Ob: Left $\mathcal{O}$-ideals

Morphisms: Left $\mathcal{O}$-module homomorphisms

Let $\mathrm{End}(E) = \mathcal{O} \subset B_{p,\infty}$.

There is an equivalence of categories

$$F : \mathrm{SS}_{\overline{\mathbb{F}}_p} \to \mathrm{LeftId}(\mathcal{O})$$

The Deuring Correspondence

Ob: Supersingular curves over $\overline{\mathbb{F}}_p$

Morphisms: Isogenies

Let $\mathrm{End}(E) = \mathcal{O} \subset B_{p,\infty}$.

Ob: Left $\mathcal{O}$-ideals

Morphisms: Left $\mathcal{O}$-module homomorphisms

There is an equivalence of categories

$$F : \mathrm{SS}_{\overline{\mathbb{F}}_p} \to \mathrm{LeftId}(\mathcal{O})$$

Any $\varphi : E \to E'$

$$E' \to \mathrm{Hom}(E', E)\varphi$$

The Deuring Correspondence

Ob: Supersingular curves over $\overline{\mathbb{F}}_p$

Morphisms: Isogenies

Let $\mathrm{End}(E) = \mathcal{O} \subset B_{p,\infty}$.

Ob: Left $\mathcal{O}$-ideals

Morphisms: Left $\mathcal{O}$-module homomorphisms

There is an equivalence of categories

$$F : \mathrm{SS}_{\overline{\mathbb{F}}_p} \to \mathrm{LeftId}(\mathcal{O})$$

Any $\varphi : E \to E'$

$$E' \to \mathrm{Hom}(E', E)\varphi$$

ϕ_I is the isogeny with kernel

$$\phi_I(E) \leftarrow I$$

$$E[I] = \{ P \in E \mid \alpha(P) = 0 \ \forall \alpha \in I \}$$

The Deuring Correspondence

Ob: Supersingular curves over $\overline{\mathbb{F}}_p$

Morphisms: Isogenies

Ob: Left $\mathcal{O}$-ideals

Morphisms: Left $\mathcal{O}$-module homomorphisms

Let $\mathrm{End}(E) = \mathcal{O} \subset B_{p,\infty}$.

There is an equivalence of categories

$$F : \mathrm{SS}_{\overline{\mathbb{F}}_p} \to \mathrm{LeftId}(\mathcal{O})$$

Any $\varphi : E \to E'$

$$E' \to \mathrm{Hom}(E', E)\varphi$$

ϕ_I is the isogeny with kernel

$$E[I] = \{ P \in E \mid \alpha(P) = 0 \ \forall \alpha \in I \}$$

$$\phi_I(E) \leftarrow I$$

$$\deg \Phi_I = n(I)$$

$$\mathrm{End}(E') = \mathcal{O}_R(I)$$

Application 1: Generate a supersingular curve with $\mathrm{End}(E) = \mathcal{O}$

Goal: Let $\mathcal{O} \subset B_{p,\infty}$ be a maximal order.

Find $E/\overline{\mathbb{F}}_p$ with $\mathrm{End}(E) = \mathcal{O}$

Application 1: Generate a supersingular curve with $\mathrm{End}(E) = \mathcal{O}$

Goal: Let $\mathcal{O} \subset B_{p,\infty}$ be a maximal order.
Find $E/\overline{\mathbb{F}}_p$ with $\mathrm{End}(E) = \mathcal{O}$

Step 1: Fix E_0 with $\mathrm{End}(E_0) = \mathcal{O}_0$ known.

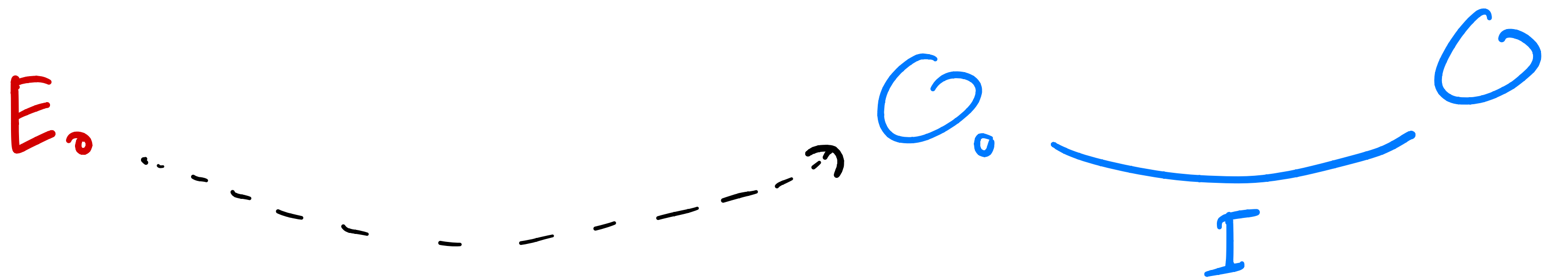
$$E_0 \dashrightarrow \mathcal{O}_0$$

Application 1: Generate a supersingular curve with $\mathrm{End}(E) = \mathcal{O}$

Goal: Let $\mathcal{O} \subset B_{p,\infty}$ be a maximal order.

Find $E/\overline{\mathbb{F}}_p$ with $\mathrm{End}(E) = \mathcal{O}$

Step 2: Compute a left $\mathcal{O}_0$-ideal with $\mathcal{O}_R(I) = \mathcal{O}$

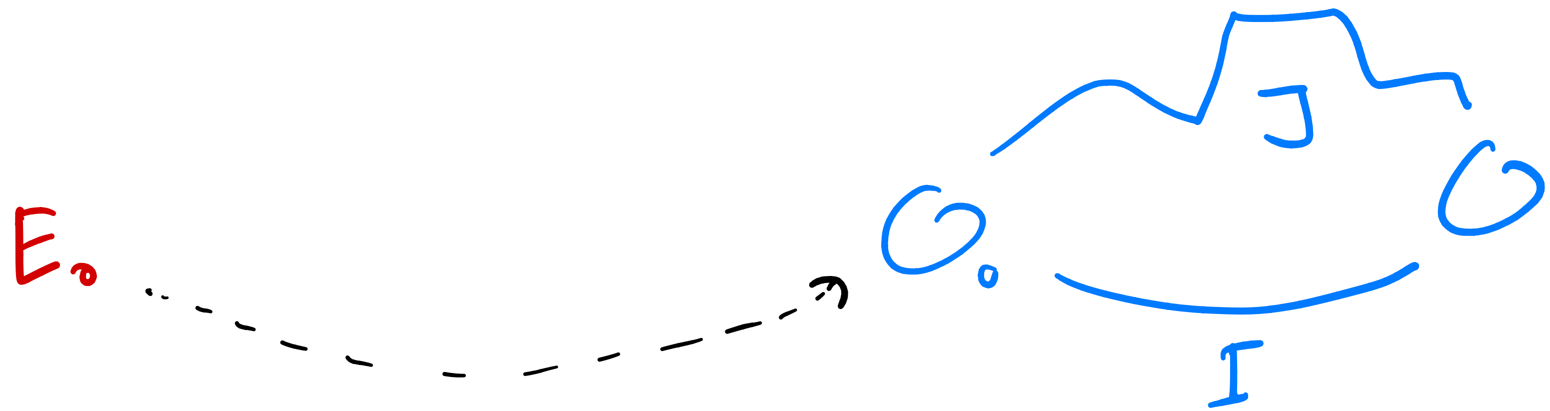


Application 1: Generate a supersingular curve with $\mathrm{End}(E) = \mathcal{O}$

Goal: Let $\mathcal{O} \subset B_{p,\infty}$ be a maximal order.
Find $E/\overline{\mathbb{F}}_p$ with $\mathrm{End}(E) = \mathcal{O}$

(every prime $\ell \mid n(J)$) / very small)

Step 3: Compute $J \sim I$ with $n(J)$ smooth

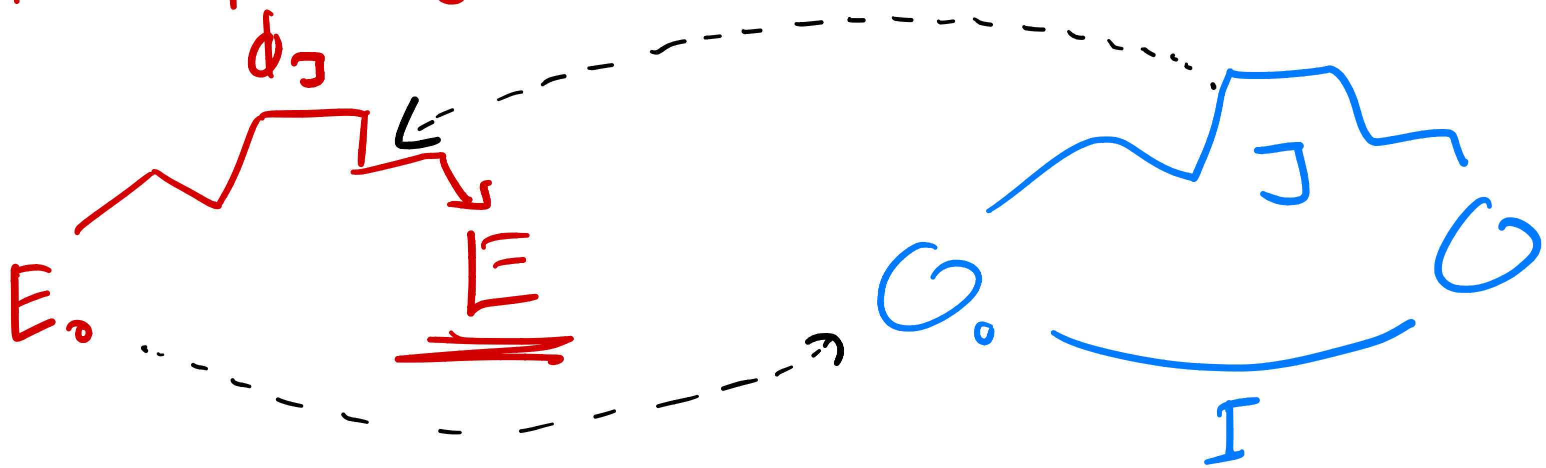


Application 1: Generate a supersingular curve with $\mathrm{End}(E) = \mathcal{O}$

Goal: Let $\mathcal{O} \subset B_{p,\infty}$ be a maximal order.

Find $E/\overline{\mathbb{F}}_p$ with $\mathrm{End}(E) = \mathcal{O}$

Final step: Compute ϕ_J, set $E = \phi_J(E_0)$



Application: SQIsign

Alice Bob

Goal: Prove that you know $\mathrm{End}(E_{pk})$ (without revealing it)

$$E_{pk} \xrightarrow{\text{Secret}} \mathcal{O}_{pk}$$

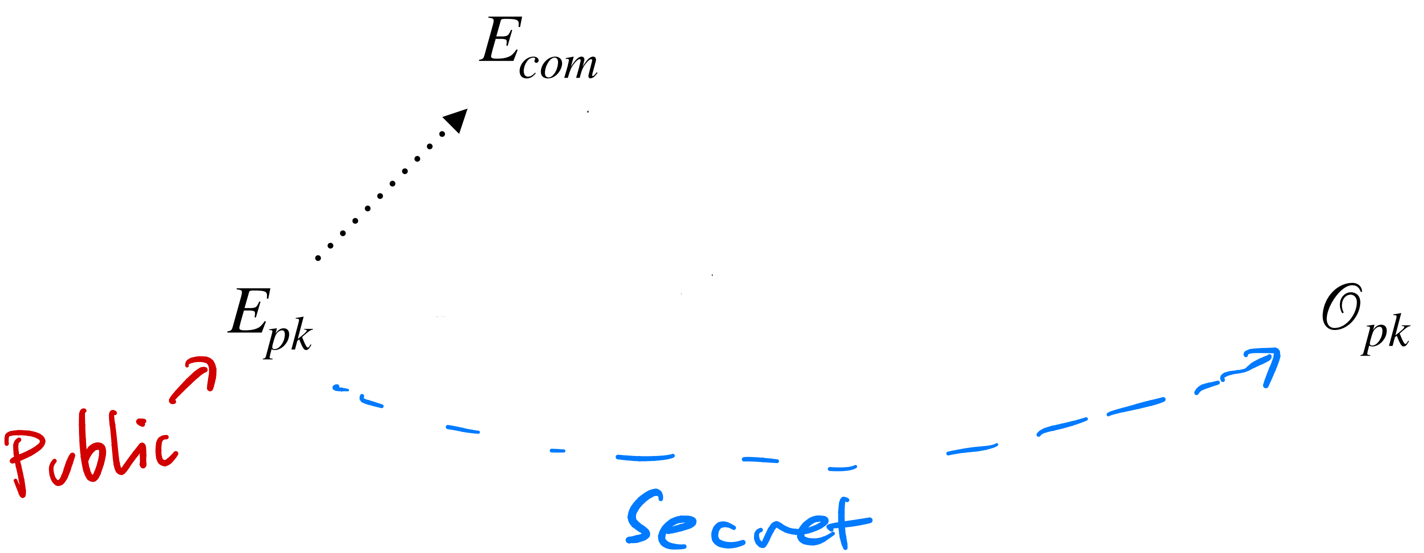
Public

Application: SQIsign

Alice Bob

E_{com}

Goal: Prove that you know $\mathrm{End}(E_{pk})$ (without revealing it)



Application: SQIsign

Goal: Prove that you know $\mathrm{End}(E_{pk})$ (without revealing it)

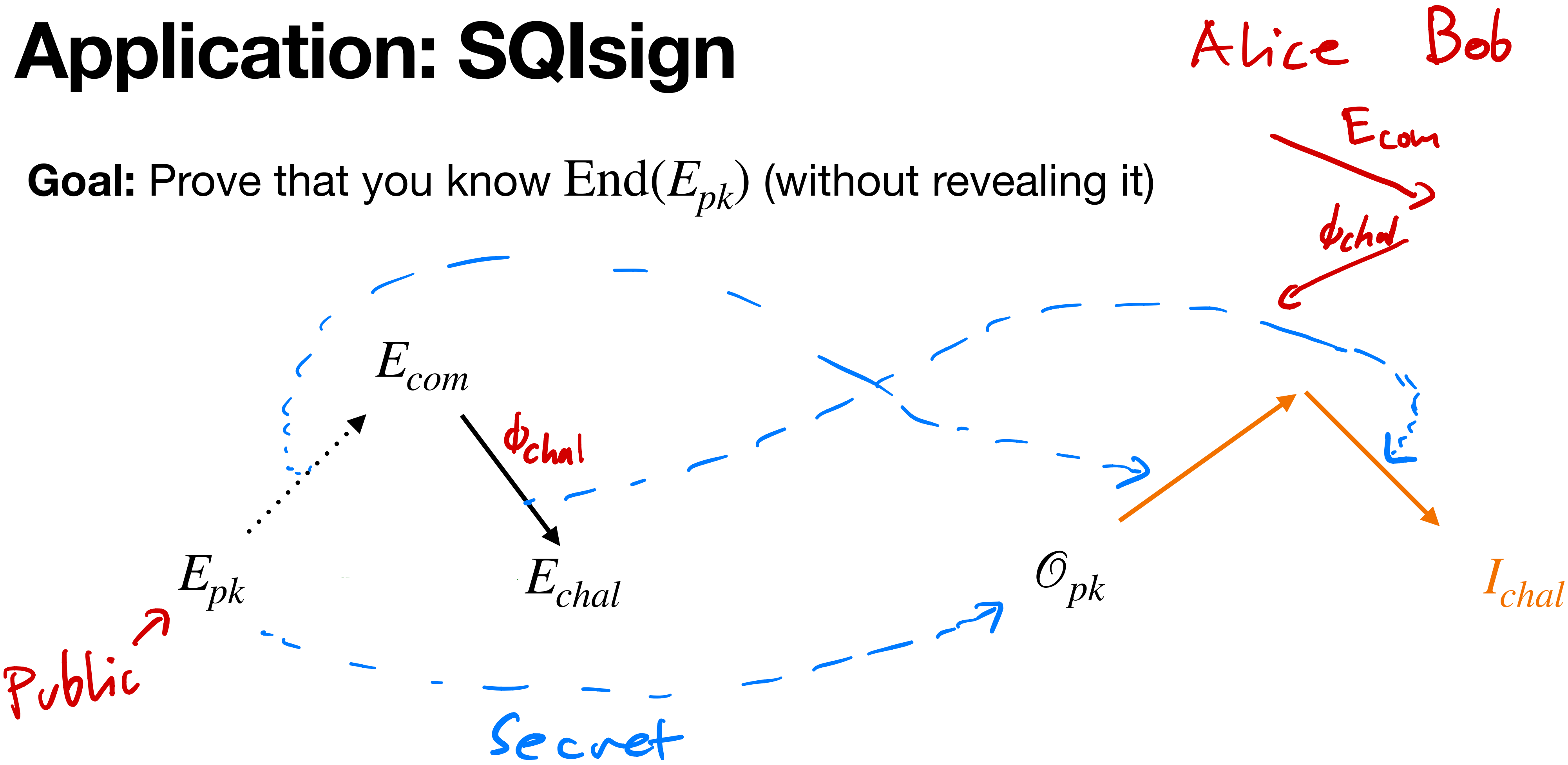
$$\begin{tikzcd} & E_{com} \arrow[dr, "\phi_{chal}"] & & \\ E_{pk} \arrow[ur, dotted] \arrow[rrr, dashed, bend right, "\text{Secret}"'] & & E_{chal} & \mathcal{O}_{pk} \end{tikzcd}$$

Public

$$\begin{tikzcd} \text{Alice} \arrow[r, shift left, "E_{com}"] & \text{Bob} \arrow[l, shift left, "\phi_{chal}"] \end{tikzcd}$$

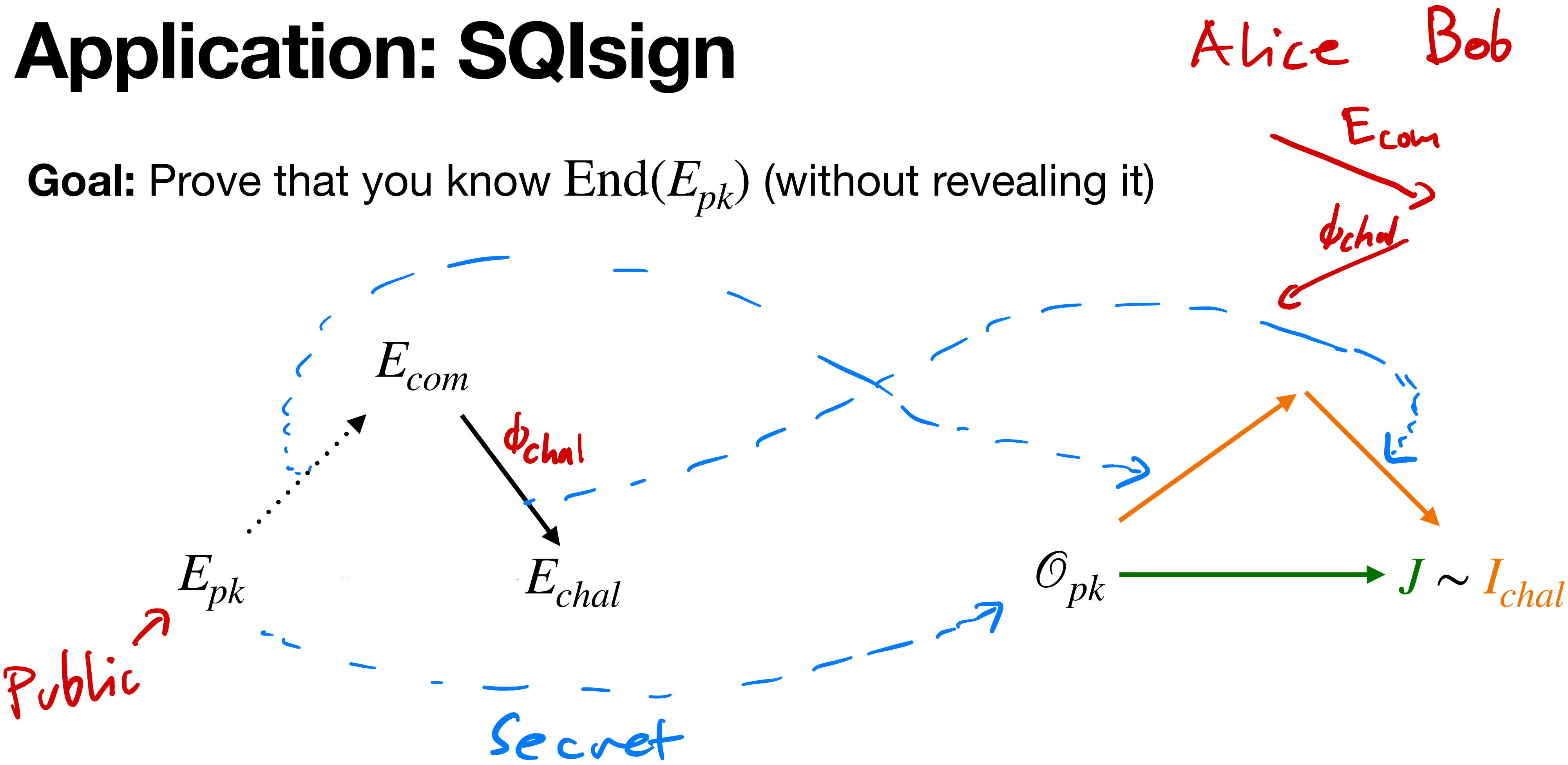
Application: SQIsign

Goal: Prove that you know $\mathrm{End}(E_{pk})$ (without revealing it)



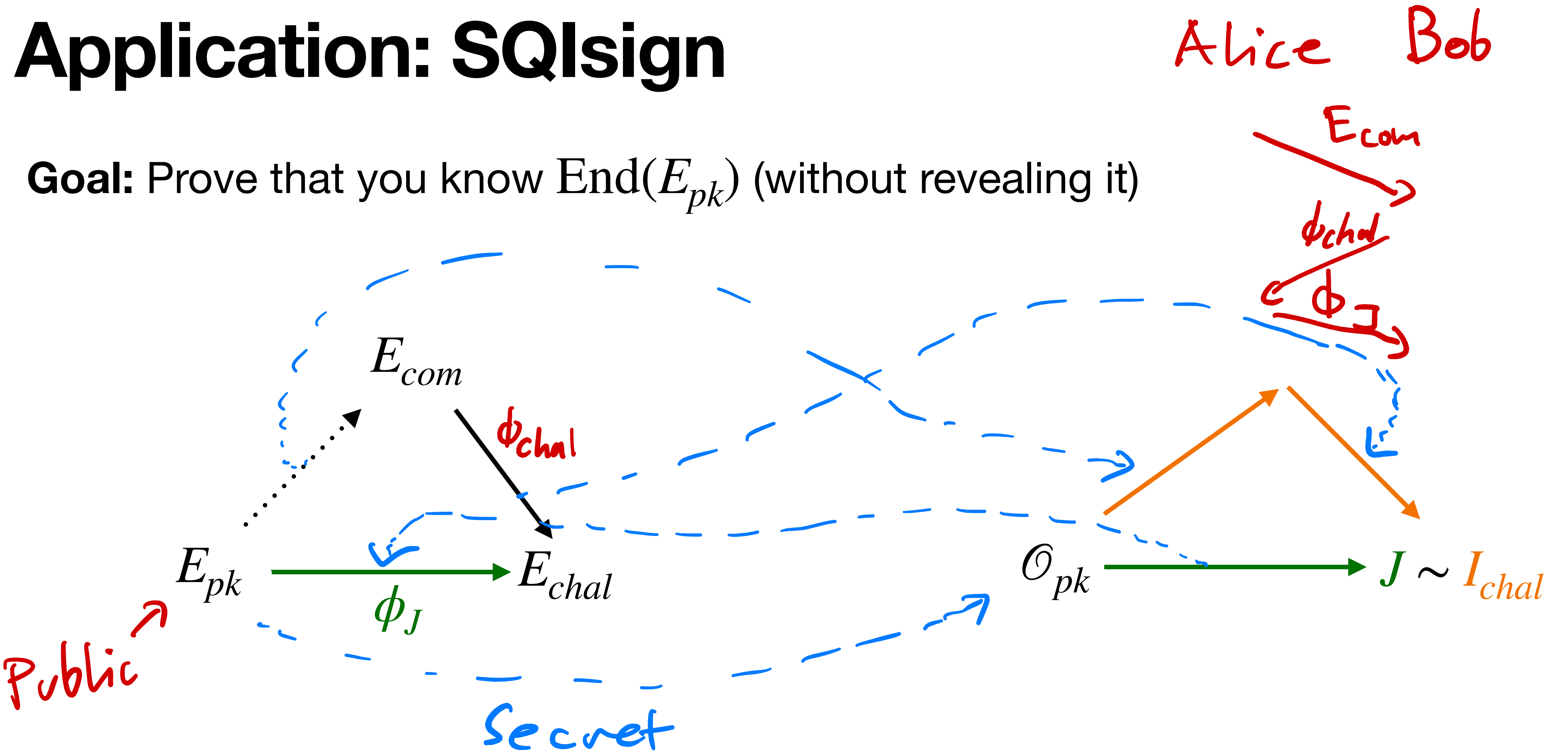
Application: SQIsign

Goal: Prove that you know $\mathrm{End}(E_{pk})$ (without revealing it)



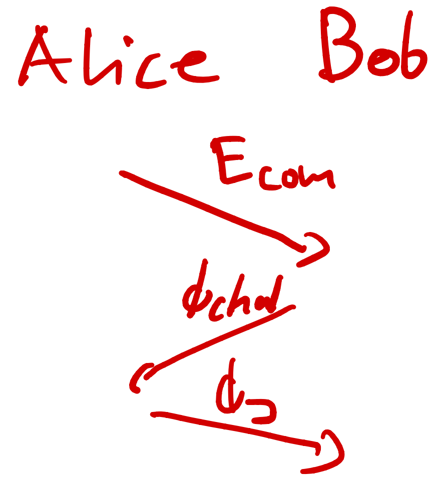
Application: SQIsign

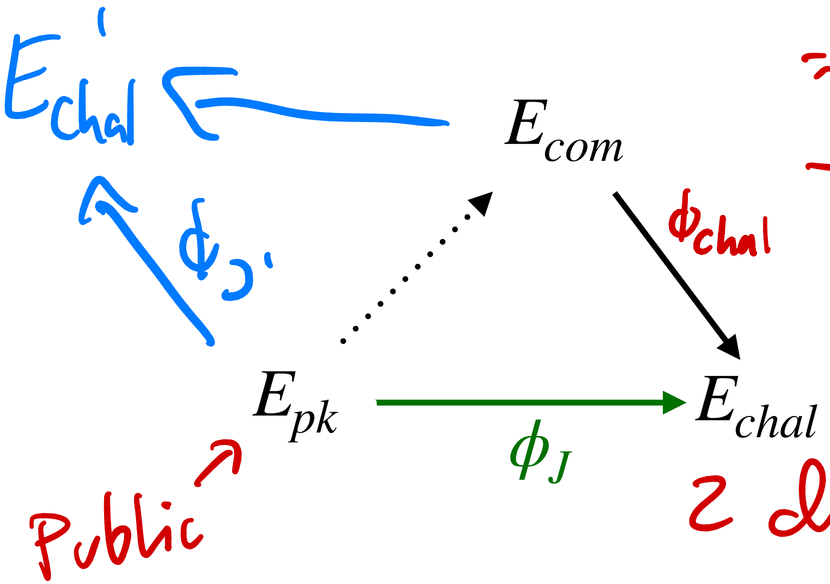
Goal: Prove that you know $\mathrm{End}(E_{pk})$ (without revealing it)



Application: SQIsign

Goal: Prove that you know $\mathrm{End}(E_{pk})$ (without revealing it)

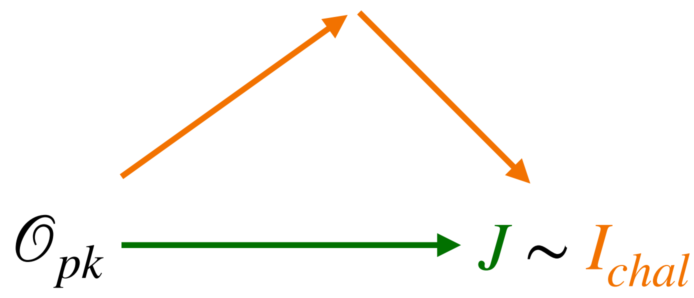




"Soundness"

Intuitively:

Answering 2 different chal's reveals an endomorphism of E_{pk}



Application: SQIsign

Goal: Prove that you know $\mathrm{End}(E_{pk})$ (without revealing it)

$$\begin{tikzcd}
 & & E_{com} \arrow[d, "\phi_{chal}"] \\
E_{pk} \arrow[rr, "\phi_J"'] & & E_{chal}
\end{tikzcd}$$

Public

Alice Bob

$$\begin{tikzcd}
\text{Alice} \arrow[r, "E_{com}"] & \text{Bob} \arrow[l, bend left, "\phi_{chal}"] \\
\text{Alice} \arrow[r, "\phi_J"] & \text{Bob}
\end{tikzcd}$$

"zero-knowledge"

Intuitively:
The only information revealed is a random isogeny.

Current Trends and Open Problems

Abelian Varieties

An **abelian variety** is a smooth, projective ~~curves of genus 1~~
variety, with a "group structure"

Abelian Varieties

An **abelian variety** is a smooth, projective ~~curves of genus 1~~ variety, with a "group structure"

$+ : A \times A \to A, \quad - : A \to A, \quad 0_A \in A$

Abelian Varieties

An **abelian variety** is a smooth, projective ~~curves of genus 1~~ variety, with a "group structure"

$m : A \times A \to A, \quad i : A \to A, \quad O_A \in A$

Identity:

$$\begin{tikzcd} \{O_A\} \times A \arrow[r, "O_A \times id_A"] \arrow[dr, "\pi_2"'] & A \times A \arrow[d, "m"] \\ & A \end{tikzcd}$$

(And same for $A \times O_A$)

Abelian Varieties

An **abelian variety** is a smooth, projective ~~curves of genus 1~~ variety, with a "group structure"

$m : A \times A \to A, \quad i : A \to A, \quad 0_A \in A$

Identity:
$$\begin{tikzcd} \{0_A\} \times A \arrow[r, "0_A \times id_A"] \arrow[dr, "\pi_2"'] & A \times A \arrow[d, "m"] \\ & A \end{tikzcd}$$

(And same for $A \times 0_A$)

Inverse:
$$\begin{tikzcd} A \arrow[r, "id_A \times i"] \arrow[d] & A \times A \arrow[d, "m"] \\ \{0_A\} \arrow[r] & A \end{tikzcd}$$

(And same for $i \times id_A$)

Abelian Varieties

An **abelian variety** is a smooth, projective ~~curves of genus 1~~ variety, with a "group structure"

$m: A \times A \to A$, $i: A \to A$, $0_A \in A$

Associativity:

$$\begin{tikzcd} A \times A \times A \arrow[r, "m \times id_A"] \arrow[d, "id_A \times m"'] & A \times A \arrow[d, "m"] \\ A \times A \arrow[r, "m"] & A \end{tikzcd}$$

Abelian Varieties

An **abelian variety** is a smooth, projective ~~curves of genus 1~~ variety, with a "group structure"

Hard to write down explicit examples !!

$A \not\subseteq \mathbb{P}^3$ (In general, $A \hookrightarrow \mathbb{P}^5$)

Dimension 2: Defining equations have high degree !!

Abelian Varieties

An **abelian variety** is a smooth, projective ~~curves of genus 1~~ variety, with a "group structure"

Hard to write down explicit examples !!

$A \not\subseteq \mathbb{P}^3$ (In general, $A \hookrightarrow \mathbb{P}^5$)

Defining equations have high degree !!

Dimension 2:
All Abelian surfaces are either products of elliptic curves, $\rightsquigarrow E \times E'$
or jacobians of genus 2 curves $\rightsquigarrow J(C)$

(can work with divisors on C)

Abelian Varieties

An **abelian variety** is a smooth, projective ~~curves of genus 1~~ variety, with a "group structure"

Hard to write down explicit examples !!

$A \not\subset \mathbb{P}^3$ (In general, $A \hookrightarrow \mathbb{P}^5$)

Defining equations have high degree !!

Dimension 2:
All Abelian surfaces are either products of elliptic curves,
or jacobians of genus 2 curves

Dimension 4+: products and jacobians no longer enough

Abelian Varieties → Why so useful?

Pre-2021: Could only compute ϕ if $\deg \phi$ was **smooth**

$$\phi : E \xrightarrow{\phi_1} E_1 \xrightarrow{\phi_2} \cdots\cdots \xrightarrow{\phi_r} E_r,$$

ϕ_i all have small degree.

Abelian Varieties

Pre-2021: Could only compute ϕ if $\deg \phi$ was **smooth**

$\phi : E \xrightarrow{\phi_1} E_1 \xrightarrow{\phi_2} \cdots\cdots \xrightarrow{\phi_r} E_r$, ϕ_i all have small degree.

Post-2021: Can compute ϕ of **any degree** by embedding into an isogeny in higher dimension.

Abelian Varieties

Pre-2021: Could only compute ϕ if $\deg \phi$ was **smooth**

$$\phi : E \xrightarrow{\phi_1} E_1 \xrightarrow{\phi_2} \cdots \cdots \longrightarrow_{\phi_r} E_r,$$

ϕ_i all have small degree.

Post-2021: Can compute ϕ of **any degree** by embedding into an isogeny in higher dimension.

$$\Phi : E \times E' \longrightarrow F \times F' \qquad \Phi = \begin{pmatrix} \phi & \psi \\ \psi' & \phi' \end{pmatrix}$$

$$\begin{tikzcd} E \arrow[r, "\phi"] \arrow[dr, "\psi'"'] & F \\ E' \arrow[ur, "\psi"] \arrow[r, "\phi'"'] & F' \end{tikzcd}$$

Abelian Varieties

Pre-2021: Could only compute ϕ if $\deg \phi$ was **smooth**

$\phi : E \xrightarrow{\phi_1} E_1 \xrightarrow{\phi_2} \cdots\cdots \xrightarrow{\phi_r} E_r$, ϕ_i all have small degree.

Post-2021: Can compute ϕ of **any degree** by embedding into an isogeny in higher dimension.

$$\begin{tikzcd} E \arrow[r, "\phi"] \arrow[dr, "\psi'" near start] & F \\ E' \arrow[ur, "\psi" near start] \arrow[r, "\phi'"'] & F' \end{tikzcd}$$

$\Phi : E \times E' \to F \times F'$ $\quad \Phi = \begin{pmatrix} \phi & \psi \\ \psi' & \phi' \end{pmatrix}$

when $\hat{\psi}' \circ \phi = \hat{\phi}' \circ \psi$, $\boxed{\deg \Phi = \deg \Phi + \deg \psi}$

Abelian Varieties

Pre-2021: Could only compute ϕ if $\deg \phi$ was **smooth**

$\phi : E \xrightarrow{\phi_1} E_1 \xrightarrow{\phi_2} \cdots\cdots \xrightarrow{\phi_r} E_r,$ ϕ_i all have small degree.

Post-2021: Can compute ϕ of **any degree** by embedding into an isogeny in higher dimension.

$\Phi : E \times E' \to F \times F'$ $\quad \Phi = \begin{pmatrix} \phi & \psi \\ \psi' & \phi' \end{pmatrix}$

For $\deg \Phi$ smooth we can compute

$\phi : E \xrightarrow{(id, 0)} E \times E' \xrightarrow{\Phi} F \times F' \xrightarrow{\pi_1} F$

when $\widehat{\psi}' \circ \phi = \widehat{\phi}' \circ \psi,$ $\boxed{\deg \Phi = \deg \Phi + \deg \psi}$

Example 1: SQIsign

Before: The response ϕ_J had to have smooth degree.
This complicated things **immensely**

$$\begin{tikzcd} & E_{com} \arrow[dr] & \\ E_{pk} \arrow[ur, dotted] \arrow[rr, "\phi_J"'] & & E_{chal} \end{tikzcd} \qquad \begin{tikzcd} & {} \arrow[dr] & \\ \mathcal{O}_{pk} \arrow[ur] \arrow[rr] & & J \sim I_{chal} \end{tikzcd}$$

Now: Return any ϕ_J embedded in dimension 2.

Result: SQIsign really looking promising for standardisation?

Example 1: Group Actions

Before: Could only compute this group action for ideals of smooth norm.

$$\star : Cl(\mathfrak{O}) \times Ell \to Ell$$
$$\mathfrak{a} \star E = \phi_{\mathfrak{a}}(E)$$

Now (one month ago): Compute this action for any ideal by embedding in dimension 4.

Result: Way more Diffie-Hellman based protocols immediately get post-quantum analogues

Open problems - Abelian Varieties

Algorithmic tools missing

Computing (polarized) isogenies

→ Dim 1 (Elliptic Curves) — Well known

Open problems - Abelian Varieties

Algorithmic tools missing

Computing (polarized) isogenies

→ Dim 1 (Elliptic Curves) — Well known

→ Dim 2 — Some work, only efficient for <u>very</u> small deg ϕ

Open problems - Abelian Varieties

Algorithmic tools missing

Computing (polarized) isogenies

→ Dim 1 (Elliptic Curves) — Well known

→ Dim 2 — Some work, only efficient for <u>very</u> small deg ϕ

→ Dim 3/4 — Some work on deg $\phi = 2$

Open problems - Abelian Varieties

Algorithmic tools missing

Computing (polarized) isogenies

→ Dim 1 (Elliptic Curves) — Well known

→ Dim 2 — Some work, only efficient for <u>very</u> small deg ϕ

→ Dim 3/4 — Some work on deg $\phi = 2$

→ Dim d — ¯_(ツ)_/¯

Open problems - Abelian Varieties

Algorithmic tools missing

Increased understanding of their isogeny graphs etc.

Open problems - Abelian Varieties

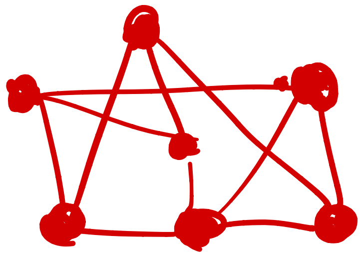
Algorithmic tools missing

Fix prime ℓ

Increased understanding of their isogeny graphs etc.

$G_\ell(\mathbb{F}_p)$ has vertecies $= \left(\begin{array}{l} \text{isomorphism} \\ \text{classes of } E/\mathbb{F}_p \end{array} \right)$

edges = isogenies of deg $\phi = \ell$



Open problems - Abelian Varieties

Algorithmic tools missing

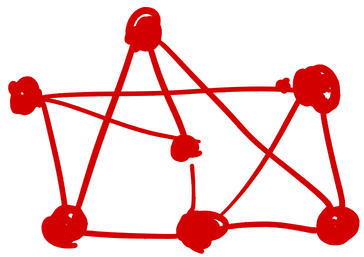
Lots of work for such graphs in dimension 1

Fix prime ℓ

Increased understanding of their isogeny graphs etc.

$G_\ell(\mathbb{F}_p)$ has vertecies $= \left(\begin{array}{l} \text{isomorphism} \\ \text{classes of } E/\mathbb{F}_p \end{array} \right)$

edges $=$ isogenies of $\deg \phi = \ell$



Other open problems

... that no one knows how to solve, but we need

(or any smooth number really)

Finding equivalent, smooth, quaternion ideals

Given $I \subseteq \mathcal{O} \subseteq B_{p,\infty}$ left ideal,

find $J \sim I$ with $n(J) = 2^e$

Other open problems

... that no one knows how to solve, but we need

Finding equivalent, smooth, quaternion ideals

Given $I \subseteq \mathcal{O} \subseteq B_{p,\infty}$ left ideal,

find $J \sim I$ with $n(J) = 2^e$

"KLPT" $\rightsquigarrow$ Solves for $2^e \approx p^3$

Expect solutions to exist when $2^e \gtrsim p$

Other open problems

... that no one knows how to solve, but we need

Generate random supersingular elliptic curves,
without learning their endomorphism ring

Current way to gen. SS curve over $\mathbb{F}_p$:

Other open problems

... that no one knows how to solve, but we need

Generate random supersingular elliptic curves,
without learning their endomorphism ring

Current way to gen. SS curve over $\mathbb{F}_p$:

- Find small D so that p inert in $\mathbb{Q}(\sqrt{-D})$

Other open problems

... that no one knows how to solve, but we need

Generate random supersingular elliptic curves,
without learning their endomorphism ring

Current way to gen. SS curve over $\mathbb{F}_p$:

- Find small D so that p inert in $\mathbb{Q}(\sqrt{-D})$
- Compute a root j_0 of $H_{-D}(x)$ over $\mathbb{F}_p$

Hilbert Class Polynomial

Other open problems

... that no one knows how to solve, but we need

Generate random supersingular elliptic curves,
without learning their endomorphism ring

Hilbert Class Polynomial

Current way to gen. SS curve over $\mathbb{F}_p$:

- Find small D so that p inert in $\mathbb{Q}(\sqrt{-D})$
- Compute a root j_0 of $H_{-D}(x)$ over $\overline{\mathbb{F}_p}$
- Compute a random isogeny $E_0 \longrightarrow \underline{\underline{E}}$

$\hookrightarrow j(E_0) = j_0$

Other open problems

... that no one knows how to solve, but we need

Generate random supersingular elliptic curves,
without learning their endomorphism ring

Current way to gen. SS curve over $\mathbb{F}_p$:

- Find small D so that p inert in $\mathbb{Q}(\sqrt{-D})$
- Compute a root j_0 of $H_{-D}(x)$ over $\mathbb{F}_p$
- Compute a random isogeny $E_0 \longrightarrow \underline{\underline{E}}$

Hilbert Class Polynomial

$\hookrightarrow j(E_0) = j_0$

Problem: This reveals $\mathrm{End}(E)$!

Thank you!

Questions?