Drinfeld Modules vs Isogeny-based Crypto

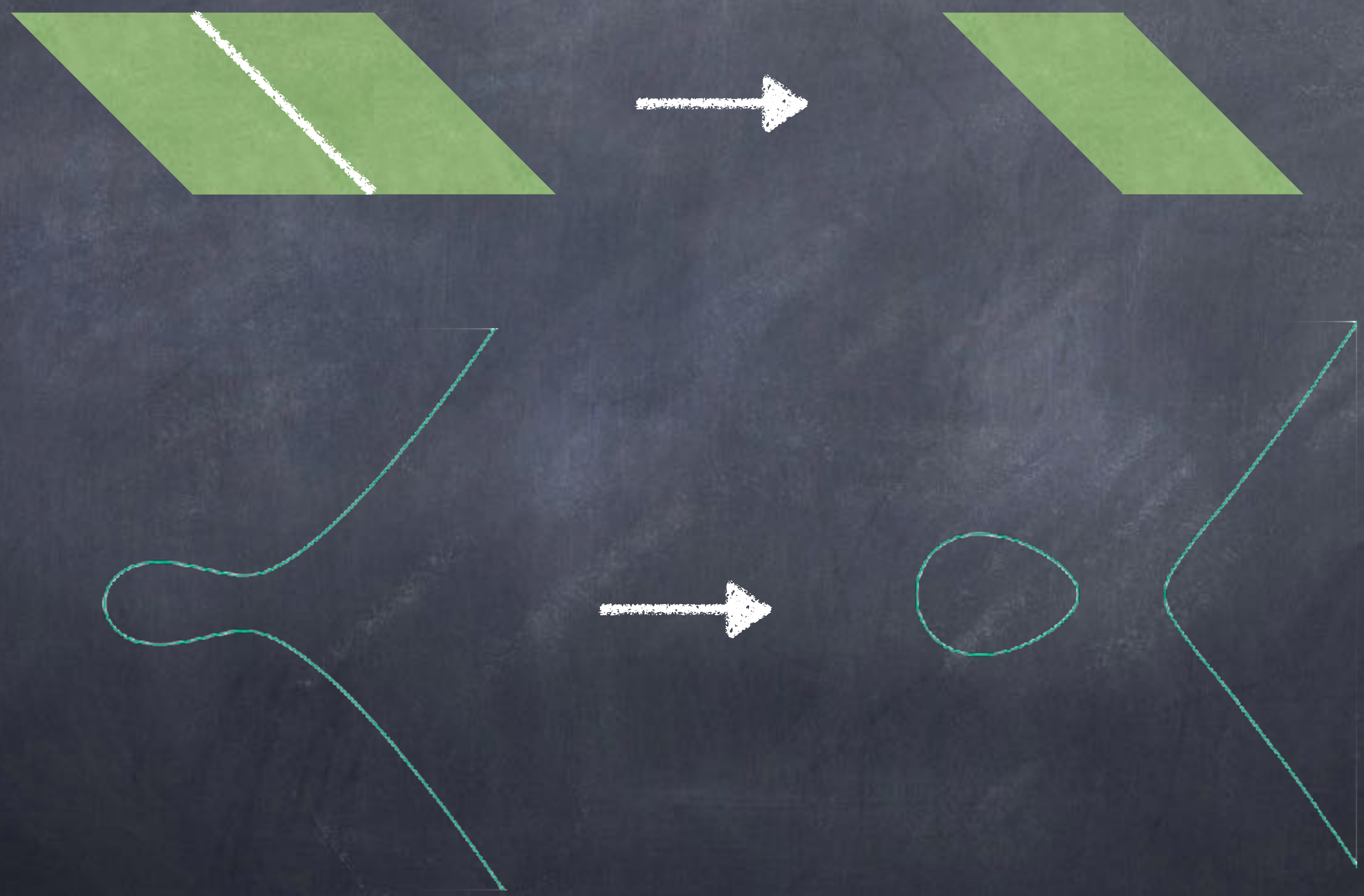
Simons Institute - Feb 24, 2020

Antoine Joux
(joint work with Anand K. Naranayan)

Isog-based Crypto

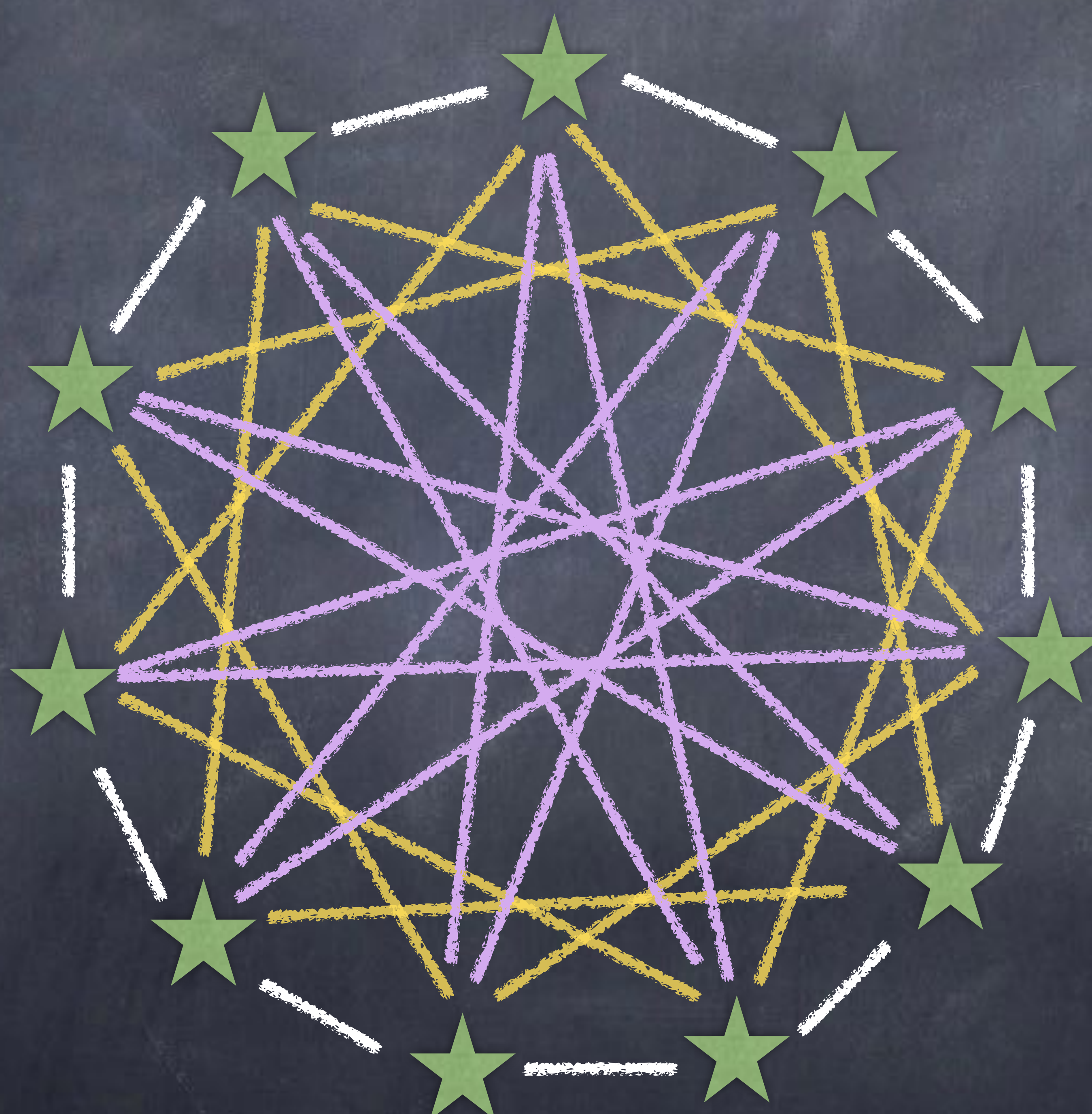
- Focuses about maps (isogenies) between curves
- No emphasis on points
- Paths in the isogeny graph

Isogenies of EC

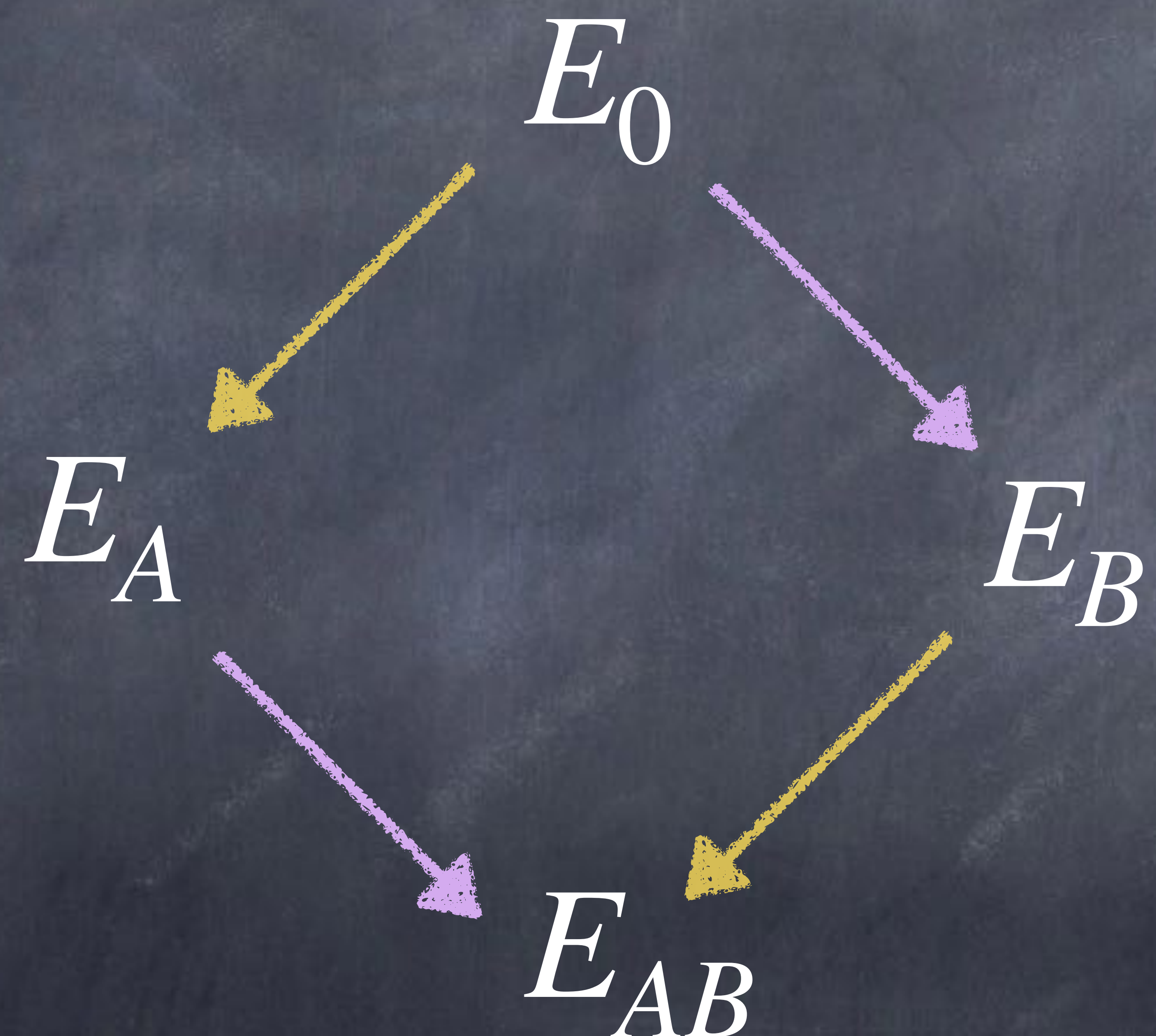


Isogeny graph

Isogeny graph



Isog Key Exchange



Drinfeld Modules (of rank 2)

- « Analogues » of EC
- Many similarities
- Exception: no natural « points »

Drinfeld Modules Setting

$$\mathbb{F}_q[x] \xrightarrow{\gamma} K = \mathbb{F}_{q^n}$$

q Frobenius: $K \xrightarrow{\tau} K$

$K\langle\tau\rangle$ Ring of skewed polynomials

Elts of $K\langle\tau\rangle$ give endomorphisms

$$j_\phi = g_\phi^{q+1}/\Delta_\phi$$

$$\mathbb{F}_q[x] \xrightarrow{\phi/K} K\langle\tau\rangle$$

$$x \longrightarrow \gamma(x) + g_\phi\tau + \Delta_\phi\tau^2$$

$K = \mathbb{F}_{q^n}$ defined as $\mathbb{F}_q[x]/f(x)$

$$\tau^{2n} - \phi(t_\phi(x))\tau^n + \epsilon_\phi\phi(f) = 0$$

$t_\phi(x)$ is called the Trace of ϕ/K

ϕ/K supersingular is $t_\phi(x) = 0$

Drinfeld Modules
Isogeny

$\iota \in K\langle\tau\rangle$ isogeny $\phi/K \longrightarrow \psi/K$

iff $\iota \circ \phi = \psi \circ \iota$

We just need to check on x

Example

Field: $K = \mathbb{F}_{p^p} = \mathbb{F}_p[x]/(x^p - x + 1) = \mathbb{F}_p[\omega]$

Supersing Module: ϕ/K with $\phi(x) = x + \tau^2$

$$\tau^{2n} + \epsilon_\phi \phi(f) = 0$$

In fact $\phi(f) = \tau^{2n}$

Thus $$\prod_{\alpha \in \mathbb{F}_p} \phi(x - \alpha) = \tau^{2n} - 1$$

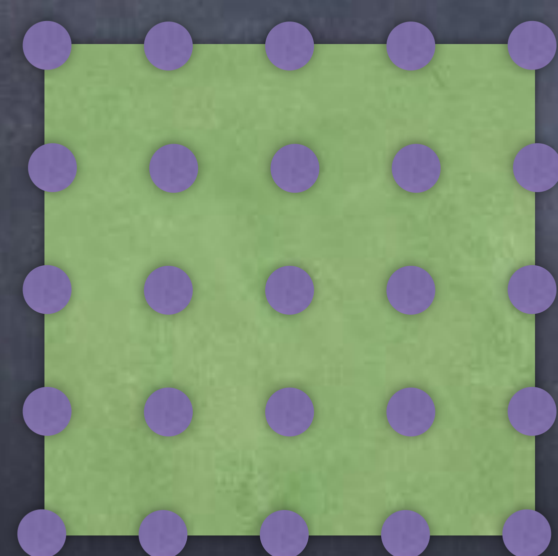
Example

Low-Degree Isogenies from Torsion

$$\phi_{x+\alpha} = \phi(x+\alpha) = x + \alpha + \tau^2$$

$$\phi_{x+\alpha}(Y) = 0 \iff Y^{p^2} + (\omega + \alpha)Y = 0$$

V-space



Each line gives:

$Y^p - \theta Y = 0$ with $\theta \in \mathbb{F}_{p^{2p}}$

Isogeny: $\iota = \tau - \theta$

Example

Isogeny: $\iota = \tau - \theta$

Dual: $\hat{\imath} = \tau - (\omega + \alpha)/\theta$

We have: $\hat{\imath} \circ \iota = \phi(x) + \alpha$ Let $\psi = \iota \circ \hat{\imath} - \alpha$

$$\hat{\imath} \circ \iota \circ \hat{\imath} - \alpha\hat{\imath} = \phi \circ \hat{\imath} = \hat{\imath} \circ \psi$$

Thus: Low-Degree isogeny

Example

$$\phi(x) = \omega + g_\phi \tau + \tau^2$$

$$\xleftarrow{\ \iota^-\ } \quad \phi/K \quad \xrightarrow{\ \iota^+\ }$$

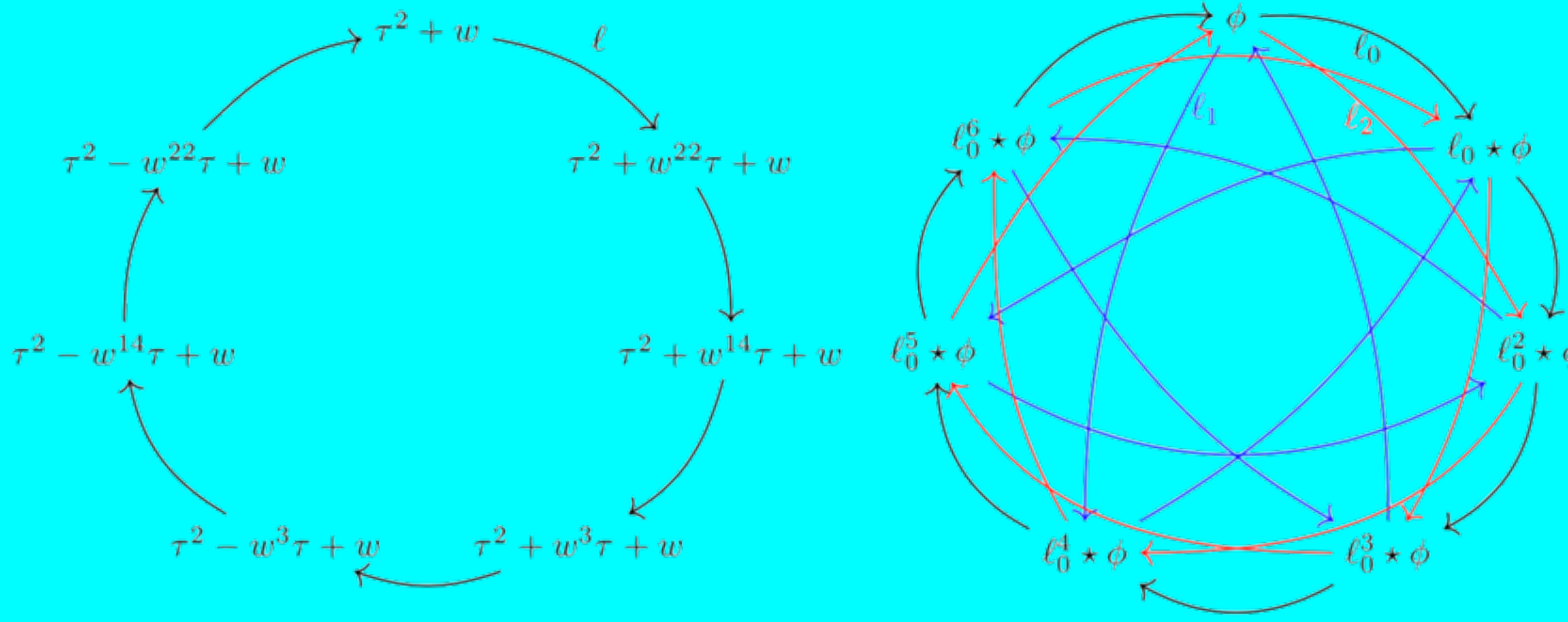
$\iota^+ = \tau - \theta^+$ where

$$Y^p - \theta^+ Y = \gcd(Y^{p^2} + g_\phi Y^p + (\omega + \alpha)Y, Y^{p^p} - Y)$$

$\iota^- = \tau - \theta^-$ where

$$Y^p - \theta^- Y = \gcd(Y^{p^2} + g_\phi Y^p + (\omega + \alpha)Y, Y^{p^p} + Y)$$

Example



$\tau^2 + w$
ℓ
$\tau^2 + w^{22}\tau + w$
$\tau^2 + w^{14}\tau + w$
$\tau^2 + w^3\tau + w$
$\tau^2 - w^3\tau + w$
$\tau^2 - w^{14}\tau + w$
$\tau^2 - w^{22}\tau + w$
ϕ
ℓ_0
ℓ_1
ℓ_2
$\ell_0 \star \phi$
$\ell_0^2 \star \phi$
$\ell_0^3 \star \phi$
$\ell_0^4 \star \phi$
$\ell_0^5 \star \phi$
$\ell_0^6 \star \phi$

$p = 3$

Adapting (C)SIDH

$(p+1)$ isogs $\iota = \tau - \theta$ for each $x + \alpha$

SIDH	CSIDH
All values θ	Only $\theta \in \mathbb{F}_{p^p}$ and dual
Non commutative	Isogs (α, θ) commutes
Need A/B split	
Need Ker images	
Larger graph	Smaller graph

Base of the attack

Given ϕ/K and ψ/K

Find $\iota \circ \phi = \psi \circ \iota$

Where: $$\iota = \sum_{k=0}^{D} i_k \tau^k$$

For SIDH: Simple linear algebra !

Conclusion