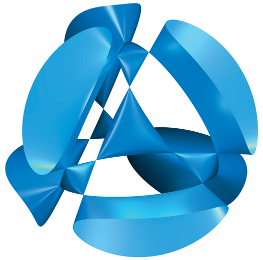
Computing supersingular isogenies on Kummer surfaces

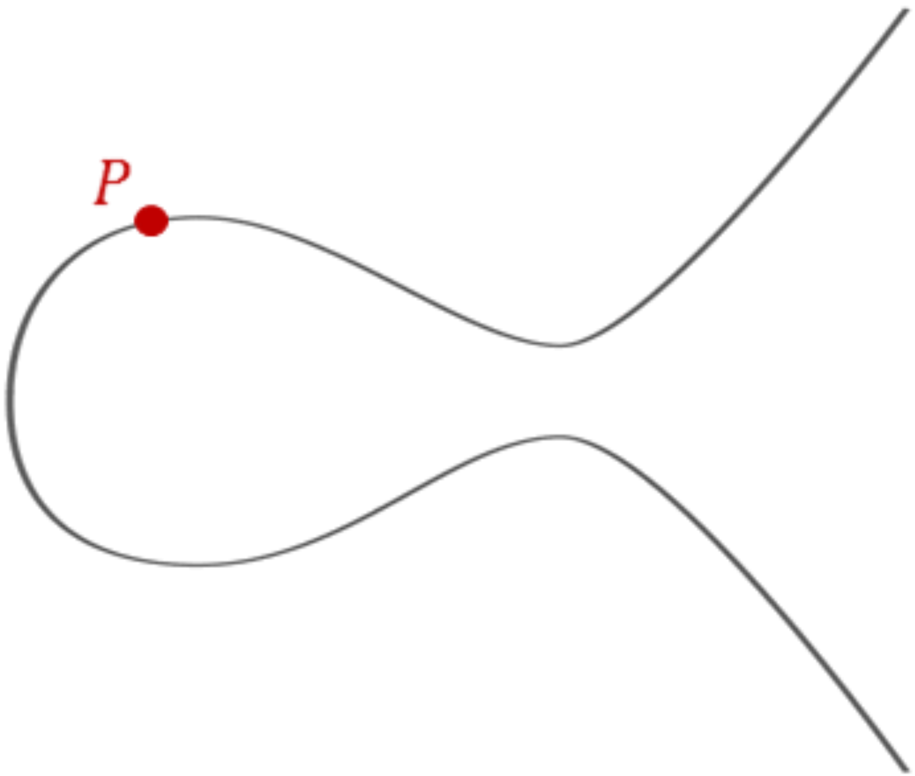
Craig Costello

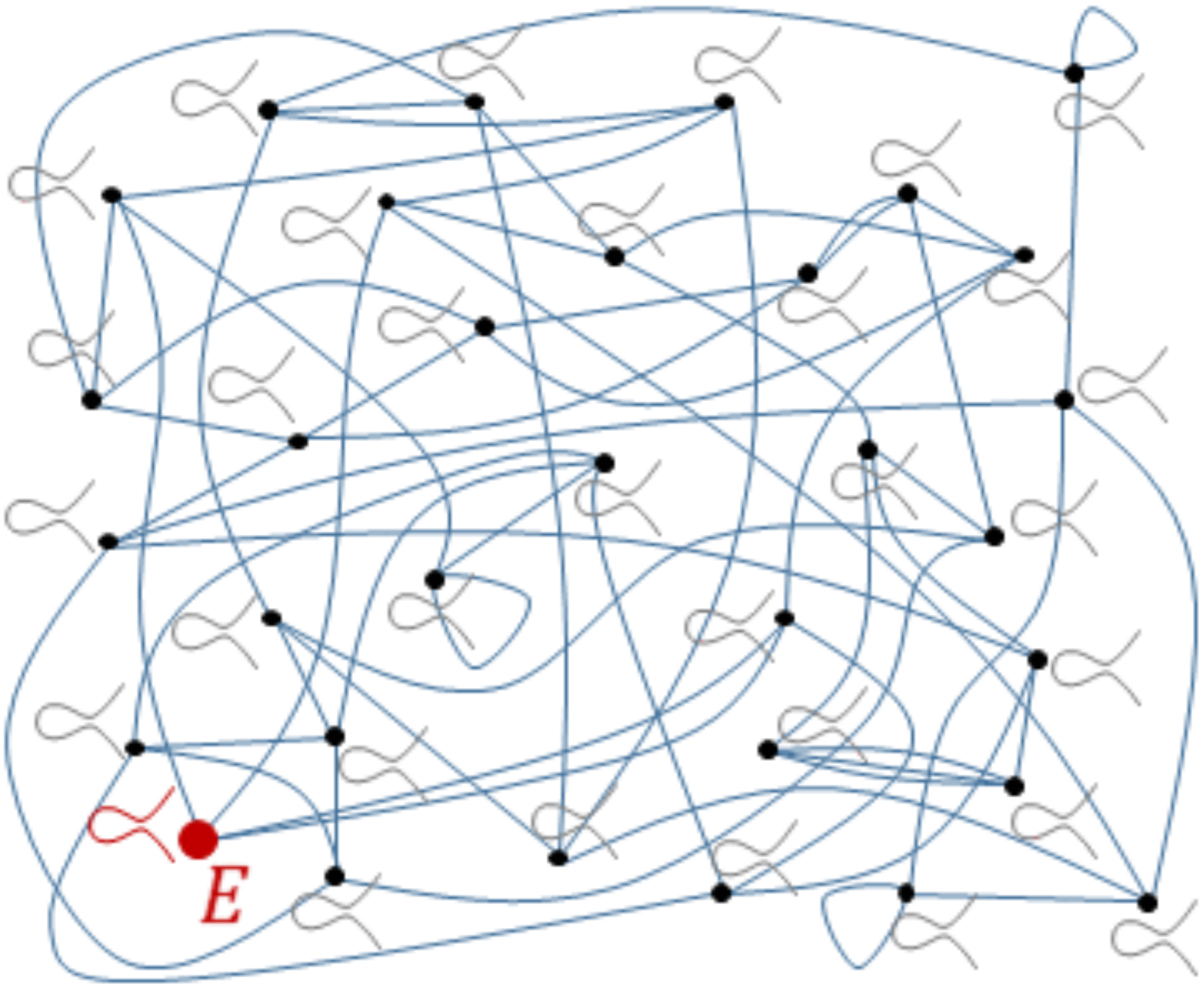
Microsoft Research



ASIACRYPT
December 6, 2018
Brisbane, Australia

ECC vs. post-quantum ECC



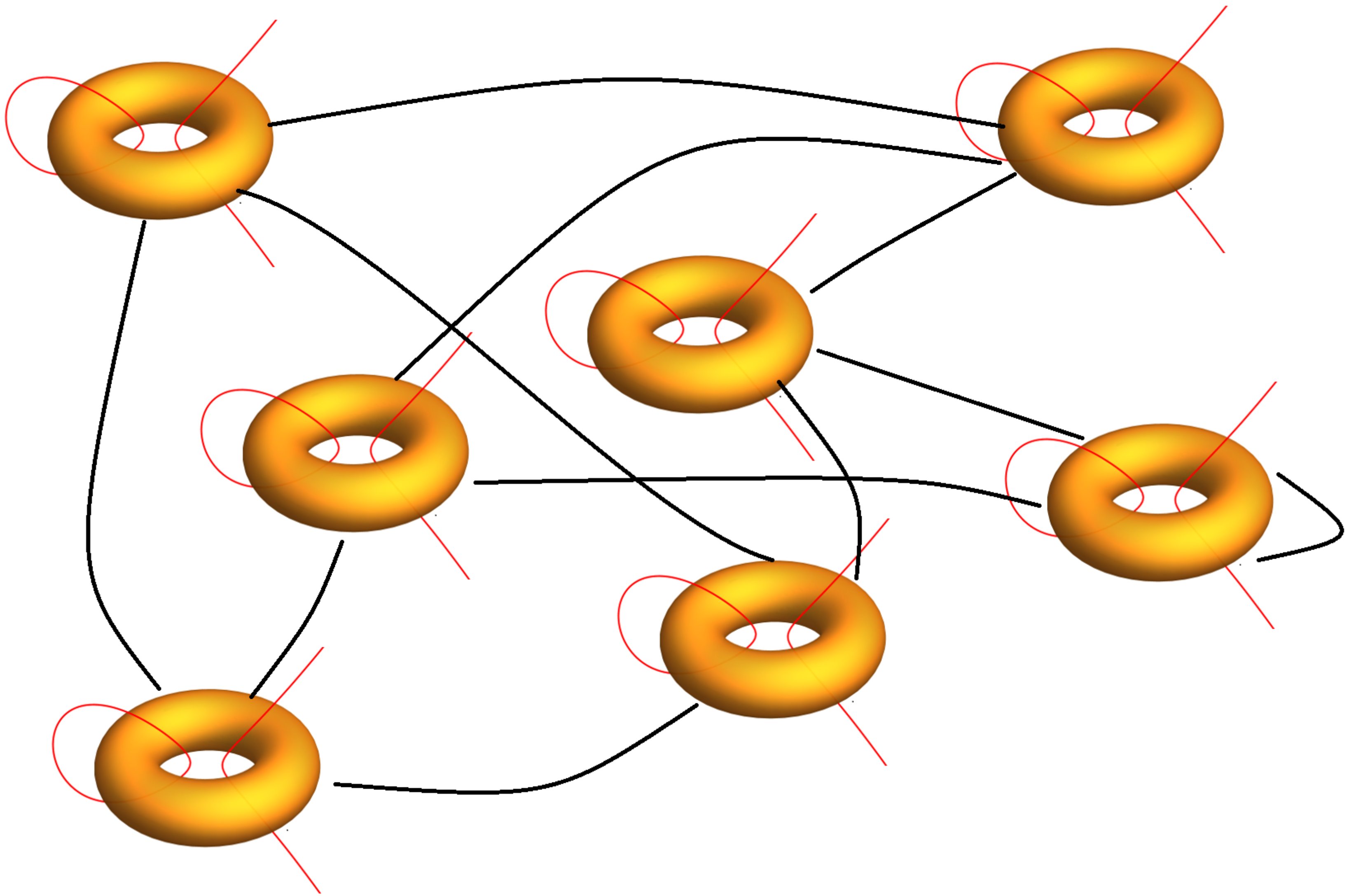


W. Castryck (GIF): https://www.esat.kuleuven.be/cosic/?p=7404

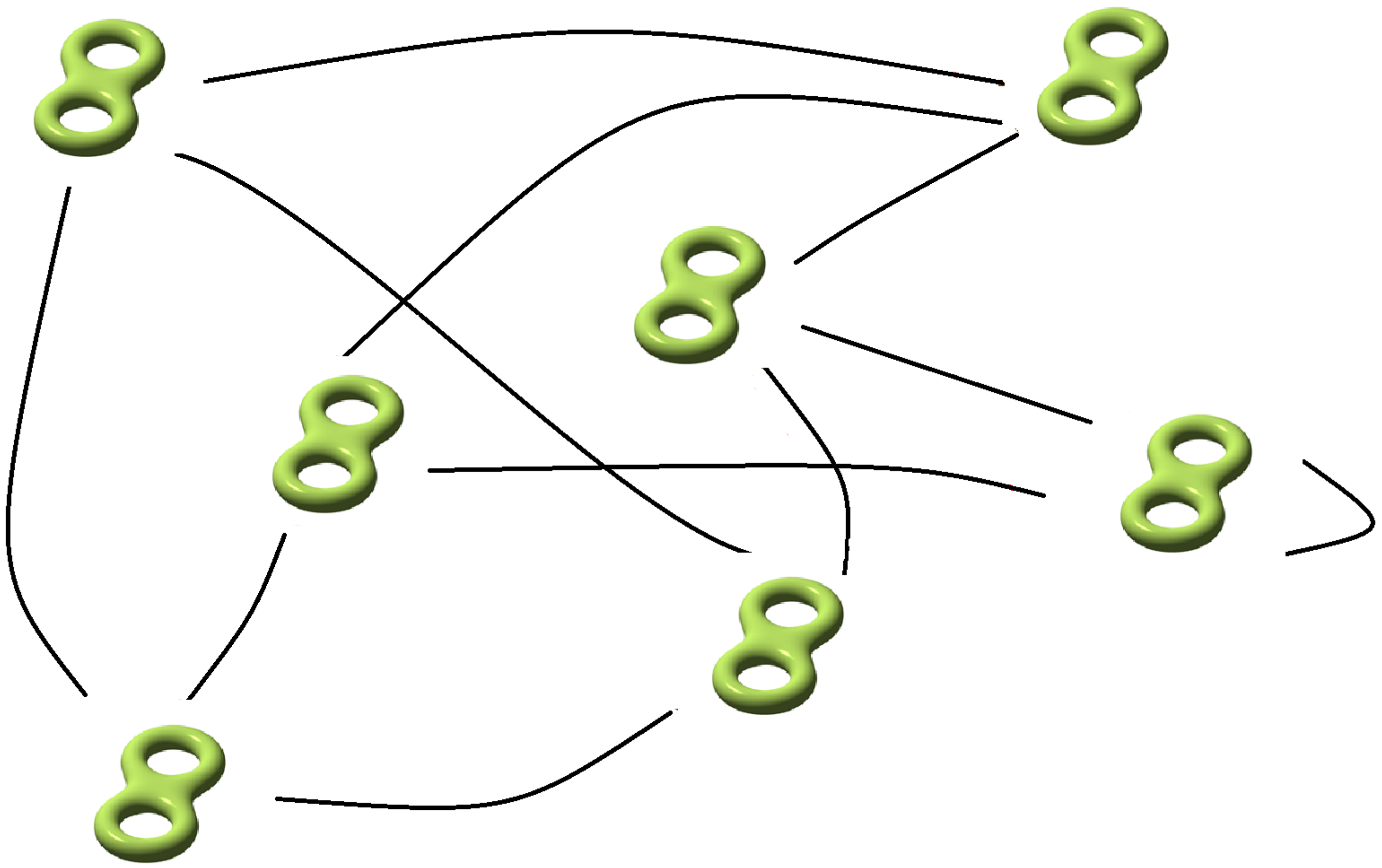
Alice 2^e-isogenies, Bob 3^f-isogenies

W. Castryck (GIF): https://www.esat.kuleuven.be/cosic/?p=7404

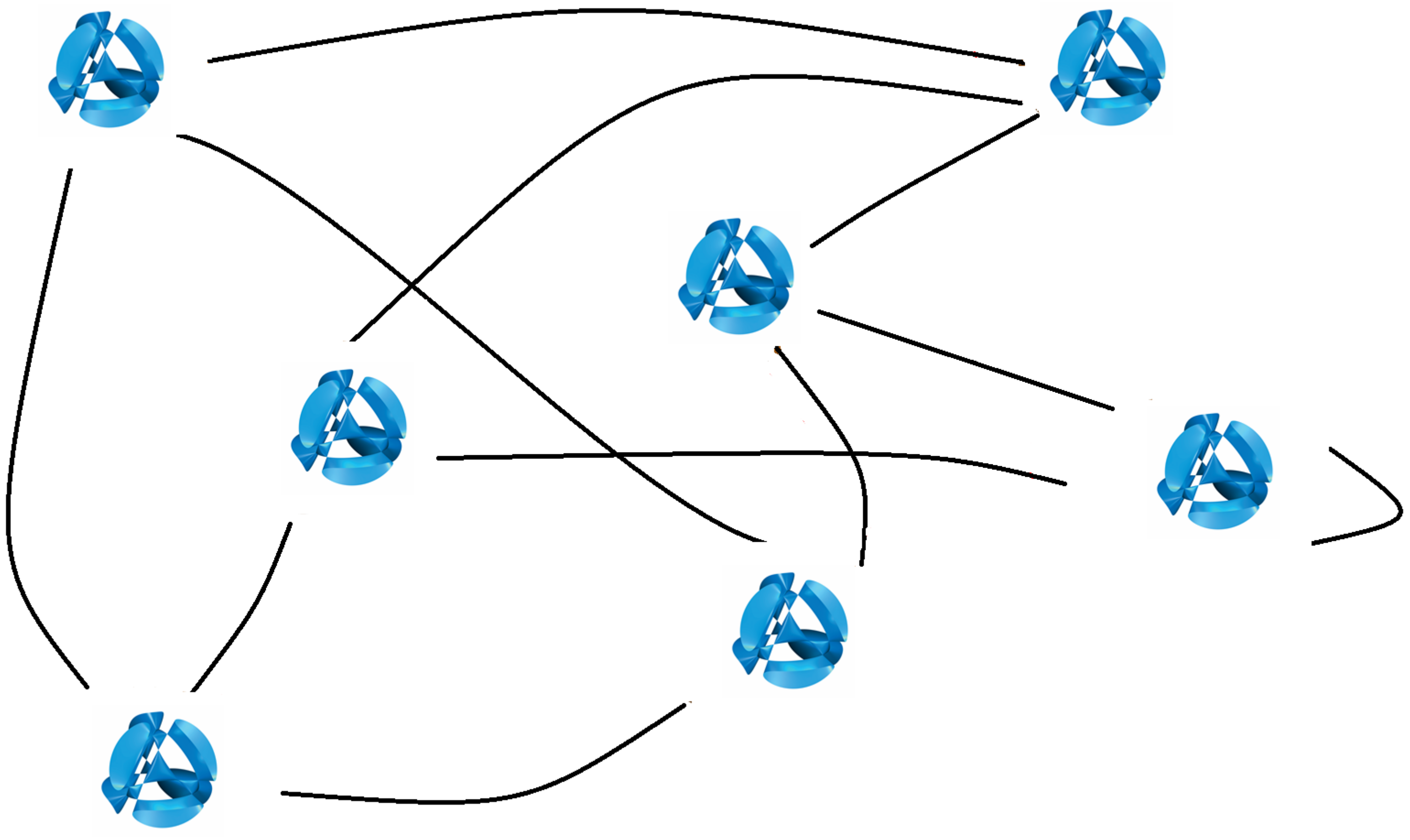
In a nutshell: $E(\mathbb{F}_{p^2})$



In a nutshell: $J_C(\mathbb{F}_p)$

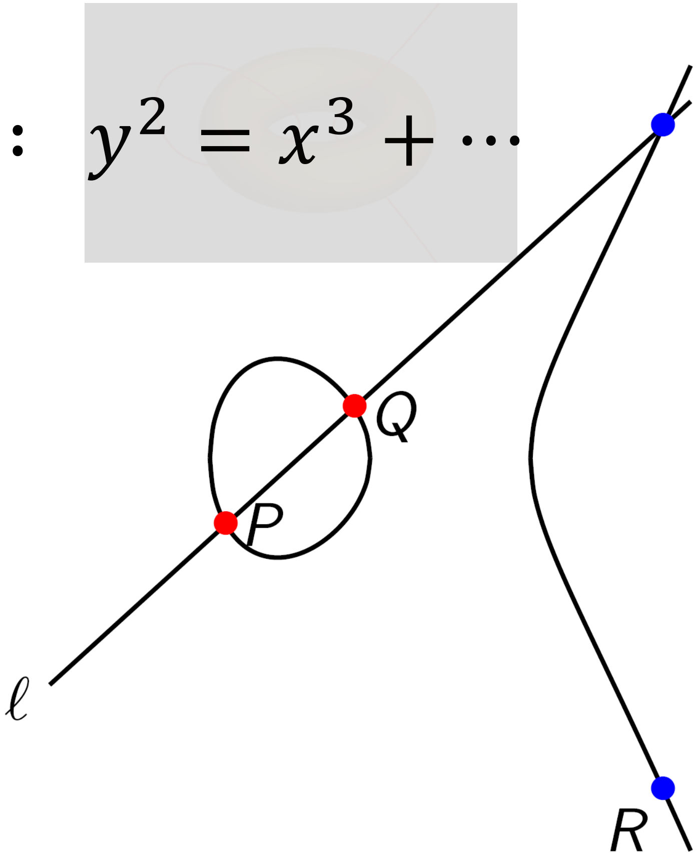


In a nutshell: $K(\mathbb{F}_p)$



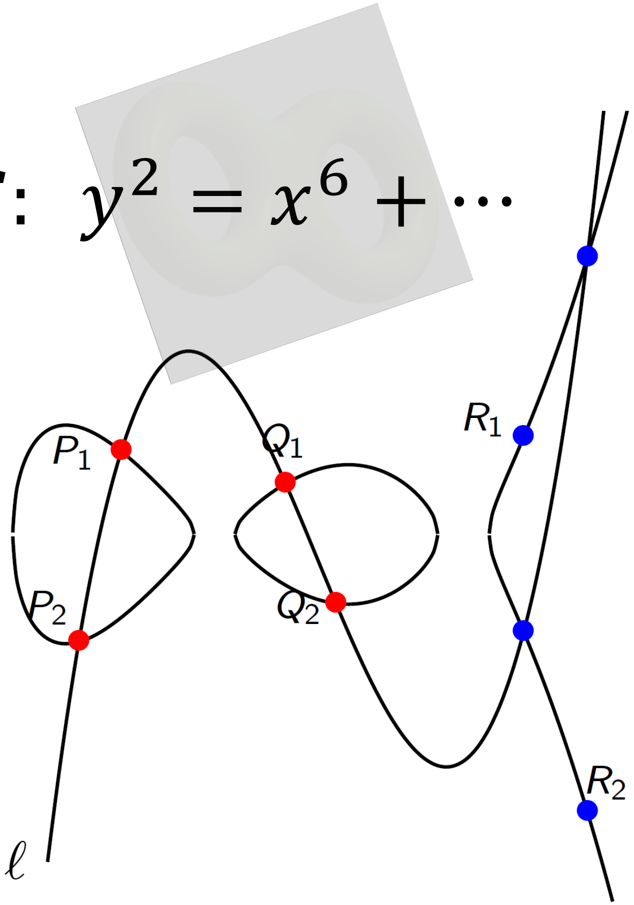
Why go hyperelliptic?

$E: \; y^2 = x^3 + \cdots$



$\#E(\mathbb{F}_q) \approx \#C(\mathbb{F}_q)$

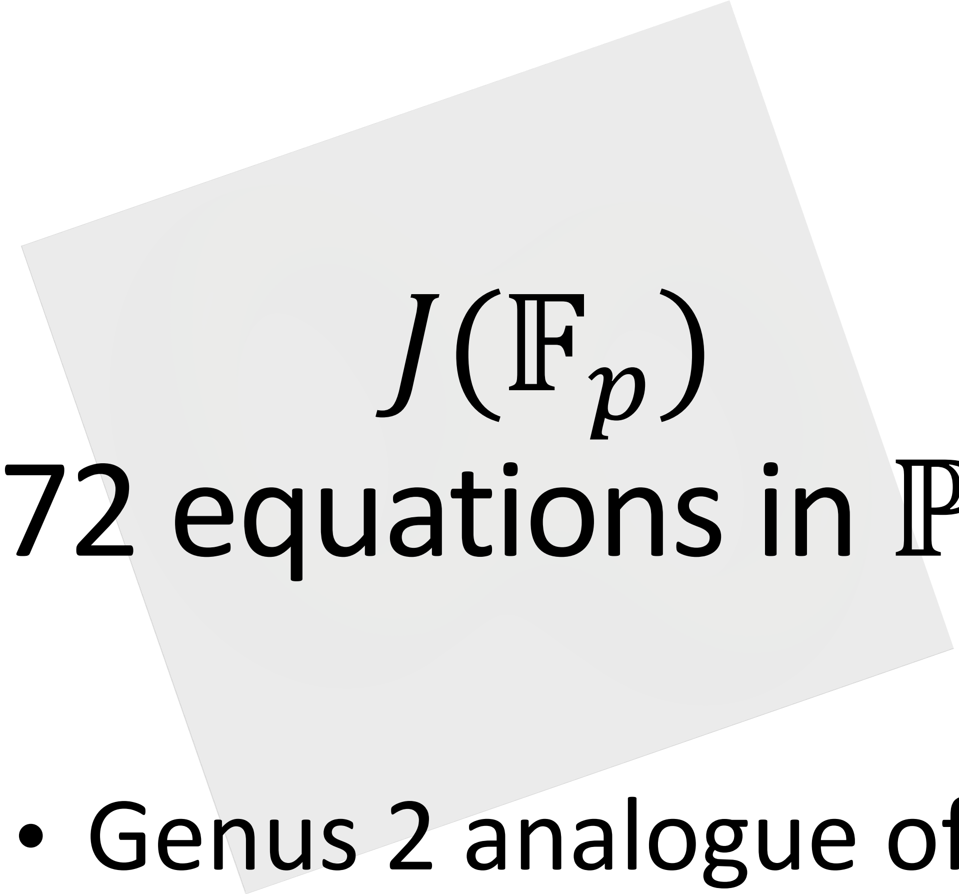
$C\colon \; y^2 = x^6 + \cdots$



$$G = E$$
$$|G| = \#E$$

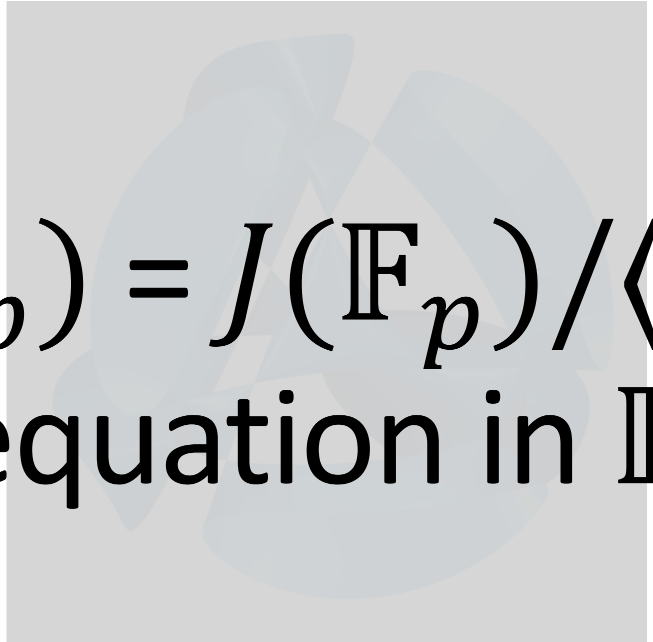
$$G \approx C \times C$$
$$|G| = (\#C)^2$$

Why go Kummer?



$J(\mathbb{F}_p)$

72 equations in $\mathbb{P}^{15}$



$K(\mathbb{F}_p) = J(\mathbb{F}_p)/\langle \pm 1 \rangle$

1 equation in $\mathbb{P}^3$

- Genus 2 analogue of elliptic curve x-line
- Extremely efficient arithmetic

… a few of my favourite things…

WEIL RESTRICTION OF AN ELLIPTIC CURVE OVER A QUADRATIC EXTENSION

JASPER SCHOLTEN

ABSTRACT. Let K be a finite field of characteristic not equal to 2, and L a quadratic extension of K. For a large class of elliptic curves E defined over L we construct hyperelliptic curves over K of genus 2 whose jacobian is isogenous to the Weil restriction $\mathrm{Res}_K^L(E)$.

Hyper-and-elliptic-curve cryptography

Daniel J. Bernstein and Tanja Lange

At this point one can and should object that [48, Lemma 2.1] merely guarantees the existence of an isogeny from W to J; it does not guarantee the existence of an *efficient* isogeny from W to J.

The main challenge addressed in this section is to show that W and J are *efficiently* isogenous.

Fast genus 2 arithmetic based on Theta functions

P. Gaudry

Remark 3.5. The pseudo-group law that we just described is somewhat surprising, because it heavily relies on a (2,2)-isogenous abelian variety for the computation: for the doubling, the point is pushed through isogenies back and forth, thus obtaining a multiplication by 2 map.

qDSA: Small and Secure Digital Signatures with Curve-based Diffie–Hellman Key Pairs

Joost Renes[1⋆] and Benjamin Smith[2]

$$\begin{tikzcd}
& \mathcal{K}^{\mathrm{Can}} \arrow[r, "\mathcal{S}", "(2,2)"'] & \mathcal{K}^{\mathrm{Sqr}} \arrow[dr, "\mathcal{H}", "\cong"'] & \\
\widehat{\mathcal{K}}^{\mathrm{Int}} \arrow[ur, "\mathcal{C}", "\cong"'] & & & \mathcal{K}^{\mathrm{Int}} \arrow[dl, "\widehat{\mathcal{C}}", "\cong"'] \\
& \widehat{\mathcal{K}}^{\mathrm{Sqr}} \arrow[ul, "\widehat{\mathcal{H}}", "\cong"'] & \widehat{\mathcal{K}}^{\mathrm{Can}} \arrow[l, "\widehat{\mathcal{S}}", "(2,2)"'] &
\end{tikzcd}$$

TOWARDS QUANTUM-RESISTANT CRYPTOSYSTEMS FROM SUPERSINGULAR ELLIPTIC CURVE ISOGENIES

LUCA DE FEO, DAVID JAO, AND JÉRÔME PLÛT

Also observe that since P and $-P$ generate the same subgroup, isogenies can be defined and evaluated correctly on the Kummer line.

It is not immediately evident how to put F in Montgomery form without computing square roots. If P_8 is a point satisfying $[2]P_8 = P_4$, then $\phi(P_8) = (2\sqrt{2+A}, \ldots)$, and F can be put in the form

From elliptic to hyperelliptic

Consider

$$E/K: \quad y^2 = x^3 + 1 \qquad\qquad C/K: \quad y^2 = x^6 + 1$$

Obvious map

$$\omega : \; C(K) \to E(K)$$
$$(x, y) \mapsto (x^2, y)$$

1: But what about $\omega^{-1} : E(K) \to C(?)$…

2: Points on E are group elements, points on C are not…

3: Actually want map $E \to J_C$, but $\dim(E) = 1$ while $\dim(J_C) = 2$…

4: Want *general* ω, ω^{-1} between $y^2 = x^3 + Ax^2 + x$ to $y^2 = x^6 + Ax^4 + x^2$???

Proposition 1

$\mathbb{F}_{p^2} = \mathbb{F}_p(i)$ with $i^2 + 1 = 0$

$$E/\mathbb{F}_{p^2}: \quad y^2 = x(x - \alpha)(x - 1/\alpha)$$

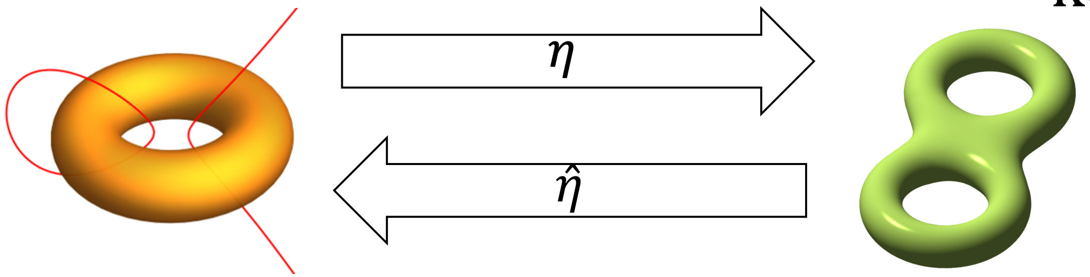
$\alpha = \alpha_0 + \alpha_1 i$ with $\alpha_0, \alpha_1 \in \mathbb{F}_p$

$$C/\mathbb{F}_p: \quad y^2 = (x^2 + mx - 1)(x^2 - mx - 1)(x^2 - mnx - 1)$$

$m = \frac{2\alpha_0}{\alpha_1}$, $n = \frac{(\alpha_0^2 + \alpha_1^2 - 1)}{(\alpha_0 + \alpha_1^2 + 1)}$ both in $\mathbb{F}_p$

Then $\mathrm{Res}_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)$ is (2,2)-isogenous to $J_C(\mathbb{F}_p)$

Or, pictorially,



$\ker(\eta) \cong \ker(\hat{\eta}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$

$\eta \circ \hat{\eta} = [2]$

Unpacking Proposition 1

- Weil restriction turns 1 equation over $\mathbb{F}_{p^2}$ into two equations over $\mathbb{F}_p$
- Simple linear transform of $E/\mathbb{F}_{p^2}: y^2 = f(x) = x^3 + Ax^2 + x$ to $\tilde{E}/\mathbb{F}_{p^2}:\ y^2 = g(x)$ such that $C/\mathbb{F}_{p^2}: y^2 = g(x^2)$ is non-singular $\quad\Longleftarrow\quad \boxed{\psi}$
- Pullback ω^* of $\omega : (x, y) \mapsto (x^2, y)$ gives 2 points in $C\left(\mathbb{F}_{p^4}\right)$, but composition with Abel-Jacobi map bring these to $J_C(\mathbb{F}_{p^2})$ $\quad\Longleftarrow\quad \boxed{\rho}$
- Need to go from $J_C(\mathbb{F}_{p^2})$ to $J_C(\mathbb{F}_p)$; cue good old Trace map, $\quad\Longleftarrow\quad \boxed{\tau}$

$$\tau:\ P \mapsto \sum_{\sigma\in\mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)}^{n} \sigma(P)$$

$$\eta :\quad \mathrm{Res}_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E) \to J_C(\mathbb{F}_p), \qquad P \mapsto (\tau \circ \rho \circ \psi)(P)$$

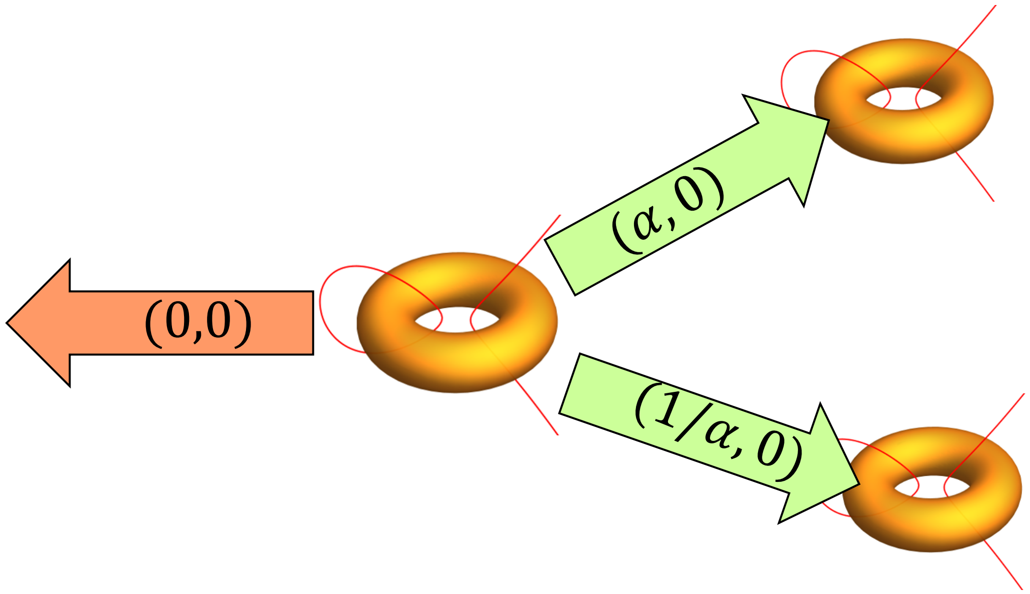
Matching 2-kernels in $\mathbb{F}_{p^2}$ with (2,2)-kernels in $\mathbb{F}_p$

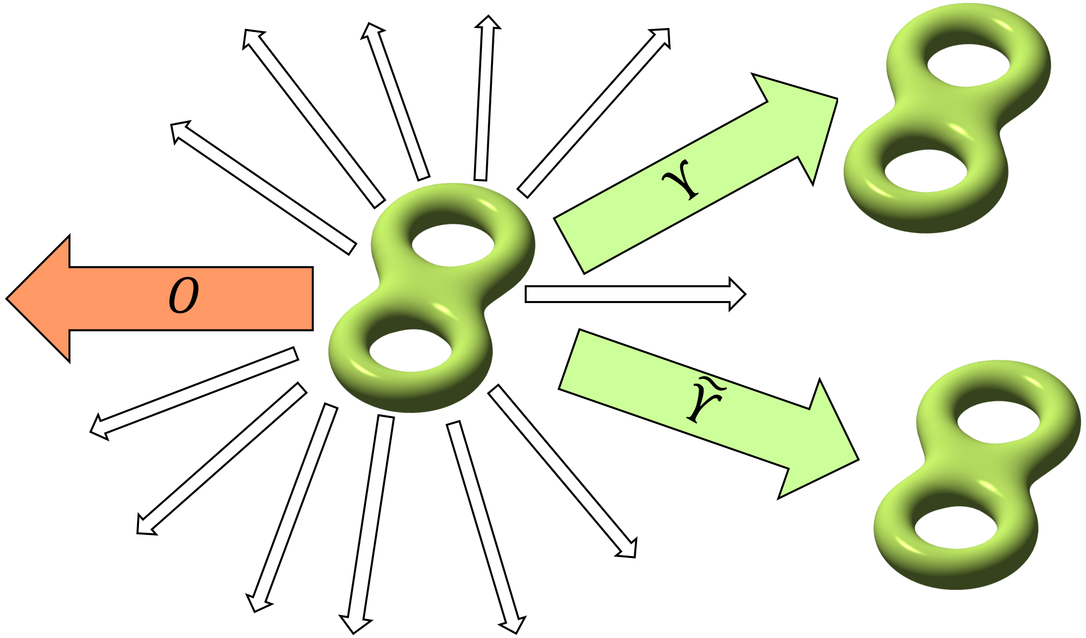
$E \cong \mathbb{Z}_{(p+1)} \times \mathbb{Z}_{(p+1)}$

$E[2] \cong \mathbb{Z}_2 \times \mathbb{Z}_2$

$J_C \cong \mathbb{Z}_{(p+1)/2} \times \mathbb{Z}_{(p+1)/2} \times \mathbb{Z}_2 \times \mathbb{Z}_2$

$J_C[2] \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$





- Fifteen (2,2)-kernels in $J_C(\mathbb{F}_p)$. Number of ways to split C's sextic into three quadratic factors.
- **Lemma 2**: identifies $O \leftrightarrow (0,0)$ and $\{\Upsilon, \widetilde{\Upsilon}\} \leftrightarrow \{(\alpha, 0), (1/\alpha, 0)\}$

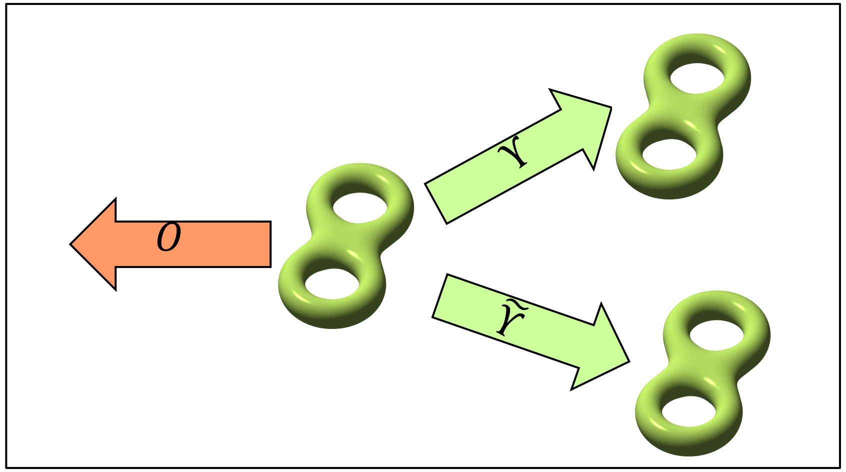
Richelot isogenies in genus 2

- Elliptic curve isogenies are easy/explicit/fast, thanks to Vélu. But beyond elliptic curves, far from true!

- $(2,2)$-isogenies in genus 2 are exception, thanks to work beginning with Richelot in 1836

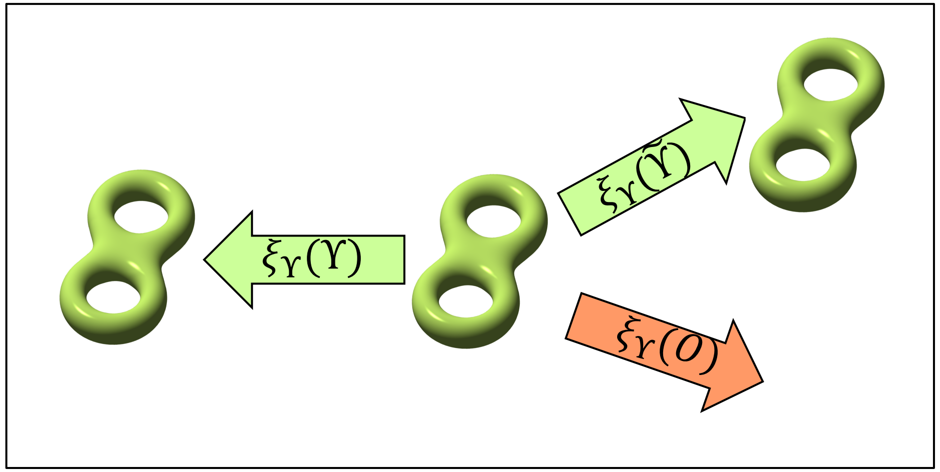
- Lessons learned from elliptic case:

(1) easiest to derive explicitly when the kernel is O, i.e. the kernel we don't want!
(2) when kernel is Υ, precompose with isomorphism $\xi_\Upsilon : J_C \to J_{C'}$, $\Upsilon \mapsto O'$
(3) ξ_Υ either requires a square root, or torsion "from above"
(4) who cares about the full Jacobian group, let's move the Kummer variety



ξ_Υ

$\cong$



Supersingular Kummer surfaces

$$K^{\mathrm{Sqr}}_{F,G,H}\colon \quad F\cdot X_1X_2X_3X_4 = \left(X_1^2+X_2^2+X_3^2+X_4^2 - G(X_1+X_2)(X_3+X_4) - H(X_1X_2+X_3X_4)\right)^2$$

Surface constants $F, G, H \in \mathbb{F}_p$

Points $(X_1\colon X_2\colon X_3\colon X_4) \in \mathbb{P}^3(\mathbb{F}_p)$

Theta constants $(\mu_1\colon \mu_2\colon 1\colon 1) \sim (\lambda\mu_1\colon \lambda\mu_2\colon \lambda\colon \lambda)$

Arithmetic constants $(\pi_1\colon \pi_2\colon \pi_3\colon \pi_4)$; functions of μ_1, μ_2

$$\begin{tikzcd}
 & \mathcal{K}^{\mathrm{Can}} \arrow[r, "\mathcal{S}", "(2,2)"'] & \mathcal{K}^{\mathrm{Sqr}} \arrow[dr, "\mathcal{H}", "\cong"'] & \\
\widehat{\mathcal{K}}^{\mathrm{Int}} \arrow[ur, "\mathcal{C}", "\cong"'] & & & \mathcal{K}^{\mathrm{Int}} \arrow[dl, "\widehat{\mathcal{C}}", "\cong"'] \\
 & \widehat{\mathcal{K}}^{\mathrm{Sqr}} \arrow[ul, "\widehat{\mathcal{H}}", "\cong"'] & \widehat{\mathcal{K}}^{\mathrm{Can}} \arrow[l, "(2,2)"', "\widehat{\mathcal{S}}"] &
\end{tikzcd}$$

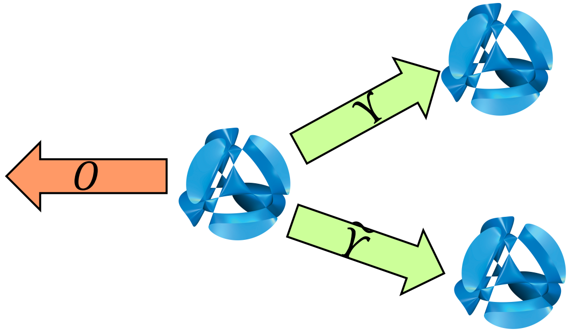
S: $(\ell_1\colon \ell_2\colon \ell_3\colon \ell_4) \mapsto (\ell_1^2\colon \ell_2^2\colon \ell_3^2\colon \ell_4^2)$

C: $(\ell_1\colon \ell_2\colon \ell_3\colon \ell_4) \mapsto (\pi_1\ell_1\colon \pi_2\ell_2\colon \pi_3\ell_3\colon \pi_4\ell_4)$

H: $(\ell_1\colon \ell_2\colon \ell_3\colon \ell_4) \mapsto (\ell_1+\ell_2+\ell_3+\ell_4\colon \ \ \ell_1+\ell_2-\ell_3-\ell_4\colon \ \ \ell_1-\ell_2+\ell_3-\ell_4\colon \ \ \ell_1-\ell_2-\ell_3+\ell_4)$

Doubling $[2]_{K^{Sqr}}\colon P \mapsto (S\circ \hat{C}\circ H\circ S\circ C\circ H)(P)$

2-isogeny (splitting [2]) $\varphi_O\colon P \mapsto (S\circ C\circ H)(P)$



Kummer isogenies for non-trivial kernels

- P point of order 2 on K corresponding to $G \in \{\Upsilon, \widetilde{\Upsilon}\}$. Write $H(P) = (P_1' : P_2' : P_3' : P_4')$
- Q point of order 4 on K such that $[2]Q = P$. Write $H(Q) = (Q_1' : Q_2' : Q_3' : Q_4')$
- Define $C_{Q,P} : (X_1 : X_2 : X_3 : X_4) \mapsto (\pi_1' X_1 : \pi_2' X_2 : \pi_3' X_3 : \pi_4' X_4)$
  where $(\pi_1 : \pi_2 : \pi_3 : \pi_4) = (P_2' Q_4' : P_1' Q_4' : P_2' Q_1' : P_2' Q_1')$
- Then φ_P: $K^{Sqr} \to K^{Sqr}/G$, $P \mapsto (S \circ H \circ C_{Q,P} \circ H)(P)$ 4M+4S+16A

$$\begin{tikzcd}
 & & \mathcal{K}_{\Upsilon}^{\mathrm{Int}'} \arrow[r, "\mathcal{H}", "\cong"'] & \hat{\mathcal{K}}_{\Upsilon}^{\mathrm{Can}} \arrow[r, "\mathcal{S}", "(2,2)"'] & \hat{\mathcal{K}}_{\Upsilon}^{\mathrm{Sqr}} = \mathcal{K}^{\mathrm{Sqr}}/\Upsilon \\
\mathcal{K}^{\mathrm{Sqr}} \arrow[r, "\mathcal{H}", "\cong"'] & \mathcal{K}^{\mathrm{Int}} \arrow[ur, "\mathcal{C}_{\Upsilon}", "\cong"'] \arrow[rr, "\mathcal{C}_{O}", "\cong"'] \arrow[dr, "\mathcal{C}_{\tilde{\Upsilon}}"', "\cong"] & & \hat{\mathcal{K}}_{O}^{\mathrm{Can}} \arrow[r, "\mathcal{S}", "(2,2)"'] & \hat{\mathcal{K}}_{O}^{\mathrm{Sqr}} = \mathcal{K}^{\mathrm{Sqr}}/O \\
 & & \mathcal{K}_{\tilde{\Upsilon}}^{\mathrm{Int}'} \arrow[r, "\cong", "\mathcal{H}"'] & \hat{\mathcal{K}}_{\tilde{\Upsilon}}^{\mathrm{Can}} \arrow[r, "\mathcal{S}", "(2,2)"'] & \hat{\mathcal{K}}_{\tilde{\Upsilon}}^{\mathrm{Sqr}} = \mathcal{K}^{\mathrm{Sqr}}/\tilde{\Upsilon}
\end{tikzcd}$$

Implications

Operation	chained 2-isogenies on Montgomery curves over $\mathbb{F}_{p^2}$ (**previous work**)				chained $(2,2)$-isogenies on Kummer surfaces over $\mathbb{F}_p$ (**this work**)				
	M	**S**	**A**	$\approx$ cycles	**m**	**s**	**a**	$\approx$ cycles	
								$\mathbf{s}=\mathbf{m}$	$\mathbf{s}=0.8\mathbf{m}$
doubling	4	2	4	5862	8	8	16	6272	5714
2-isog. curve	-	2	1	2088	19	4	28	9231	8952
2-isog. point	4	0	4	4336	4	4	16	3480	3200

- Theta constants map to theta constants: no special map needed to find image surface
- Comparison in Table/paper very conservative. Kummer will win in aggressive impl.:

  - Recall Kummer over $\mathbb{F}_{2^{127}-1}$ almost as fast as FourQ over $\mathbb{F}_{(2^{127}-1)^2}$ (scalars 4 x larger)
  - Recall that "doubling" and "2-isog. point" are bottlenecks in optimal tree strategy
  - Pushing points through 2^{ℓ} for small ℓ likely to be better on Kummer, don't need to compute all intermediate surface constants

Related future work

- To use this right now, Alice need to map back-and-forth using η and $\hat{\eta}$. Certainly not a deal-breaker! **Thus, this is a call for skilled implementers!**
- But ideally we want Bob to be able to use the Kummer, too! Then uncompressed SIDH/SIKE can be defined as Kummer everywhere!
Thus, this is a call for fast $(3, 3)$-isogenies on fast Kummers!
- Going further, general isogenies in Montgomery elliptic case have a nice explicit form (see [C-Hisil, AsiaCrypt’17] and [Renes,PQCrypto’18]). **Thus, this is a call for fast (ℓ, ℓ)-isogenies on fast Kummers!**
- Gut feeling is that there’s a better way to write down supersingular Kummers, and their arithmetic. **Thus, this is a call for smart geometers!**

Cheers!

https://eprint.iacr.org/2018/850.pdf

https://www.microsoft.com/en-us/download/details.aspx?id=57309