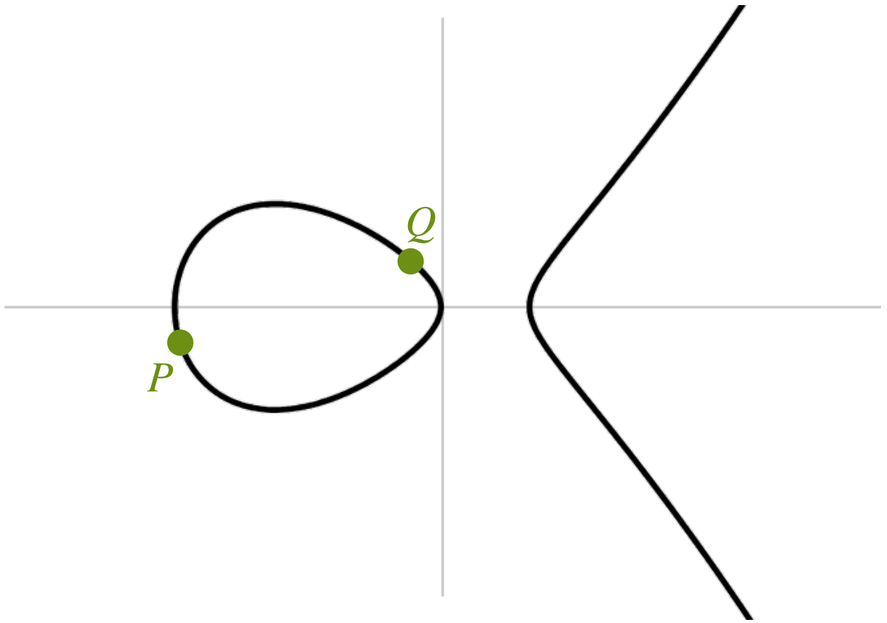
Return of the Kummer

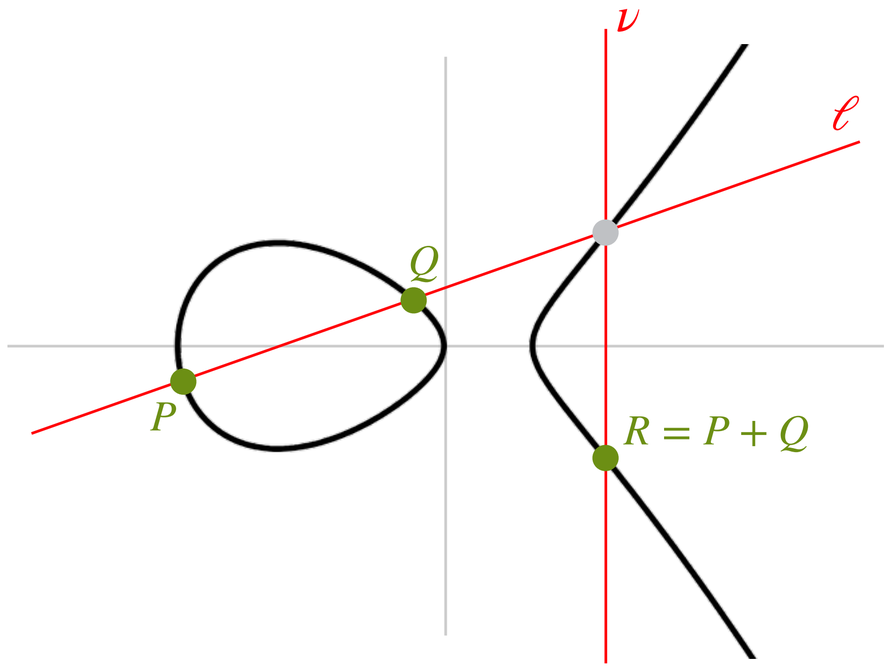
from curves to Kummers and back

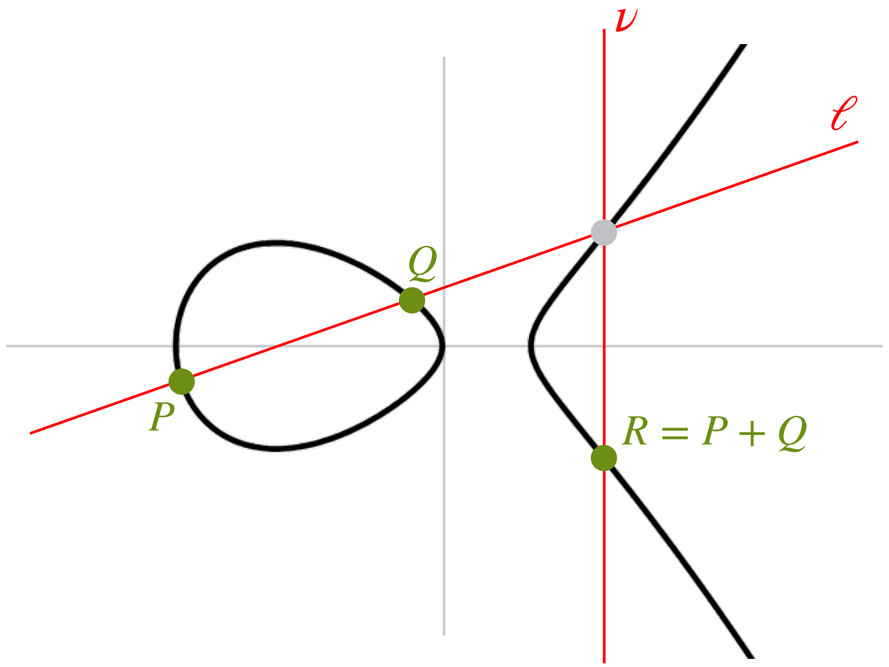
joint work with Maria Corte-Real Santos

Krijn Reijnders
KULB - March 15, 2024

Radboud University

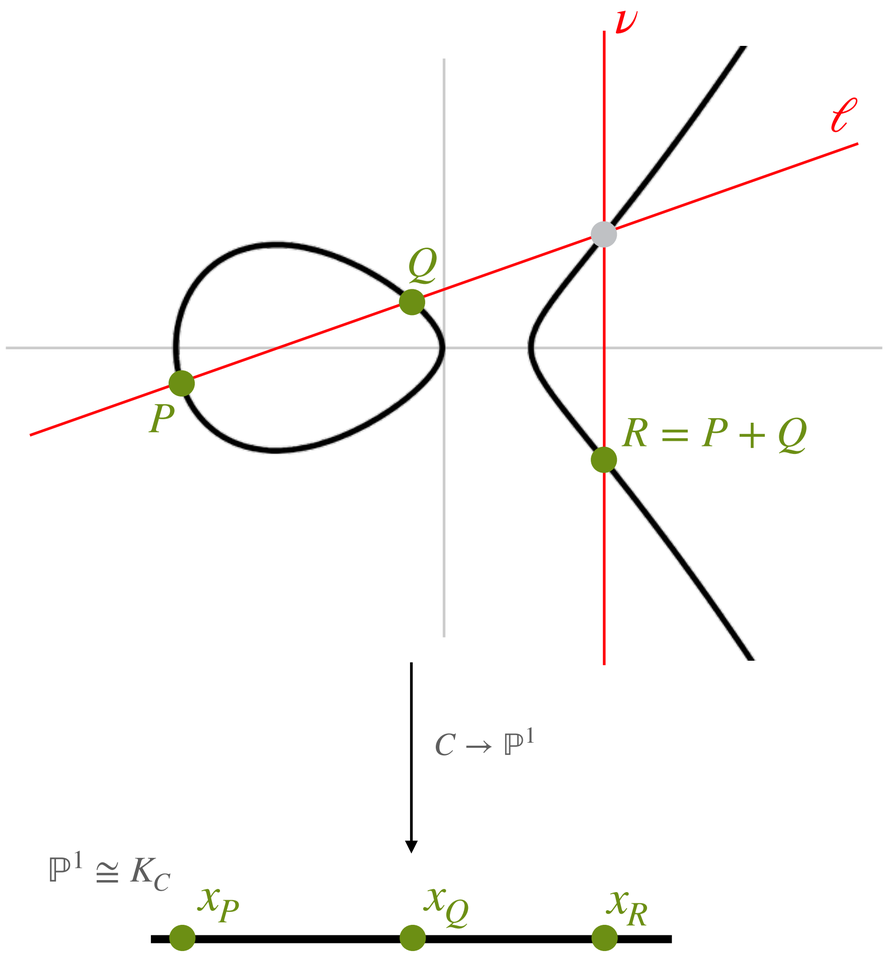

Q
P


v
ℓ
Q
P
R = P + Q



1. Points on the curve $P, Q, R \in C(k)$, i.e. satisfying some (geometric) curve equation $C : y^2 = f(x)$

2. Addition of divisors using lines from the function field $\ell, \nu \in k(C)$ for reduction, i.e. arithmetic on the Jacobian $J_C = \mathrm{Pic}^0(C)$

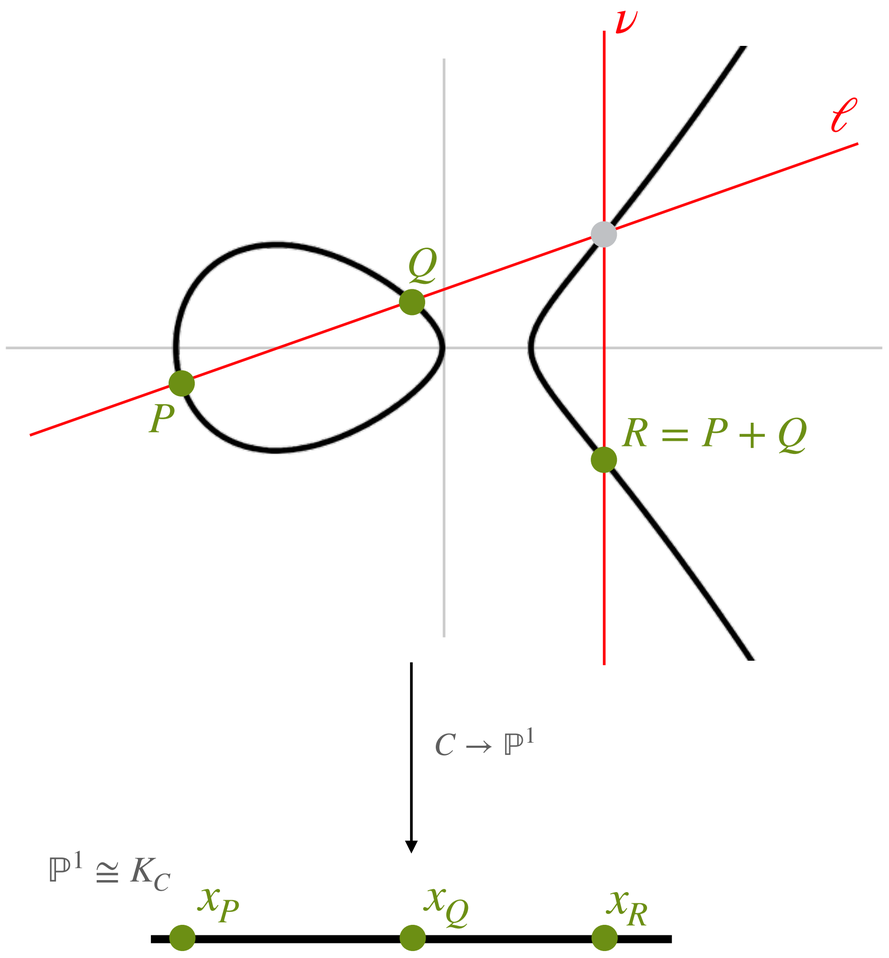


1. Points on the curve $P, Q, R \in C(k)$, i.e. satisfying some (geometric) curve equation $C : y^2 = f(x)$

2. Addition of divisors using lines from the function field $\ell, \nu \in k(C)$ for reduction, i.e. arithmetic on the Jacobian $J_C = \mathrm{Pic}^0(C)$

(in cryptography)

3. x-only arithmetic, i.e. working on the *Kummer line* K_C



1. Points on the curve $P, Q, R \in C(k)$, i.e. satisfying some (geometric) curve equation $C : y^2 = f(x)$

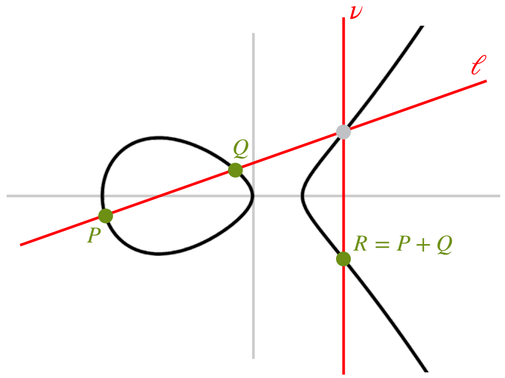
in genus 1, C is isomorphic to J_C

2. Addition of divisors using lines from the function field $\ell, \nu \in k(C)$ for reduction, i.e. arithmetic on the Jacobian $J_C = \mathrm{Pic}^0(C)$

(in cryptography)

3. x-only arithmetic, i.e. working on the *Kummer line* K_C

1. The set of points $C(k)$ of a **curve** $C : y^2 = f(x)$



2. The **Jacobian** $J_C = \mathrm{Pic}^0_k(C)$

$$J_C = \{\ (P) - (\mathcal{O})\ :\ P \in C(k)\ \}$$

3. The **Kummer line** $K_C = J_C/\pm$

$\mathbb{P}^1 \cong K_C$

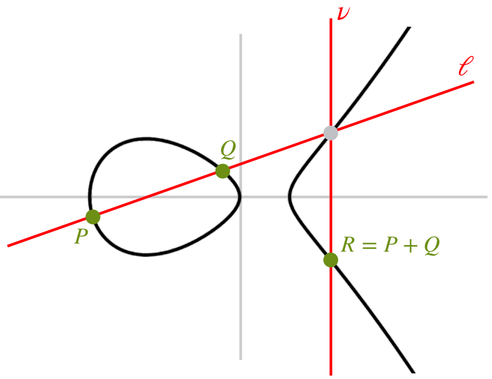
1. The set of points $C(k)$ of a **curve** $C : y^2 = f(x)$

2. The **Jacobian** $J_C = \mathrm{Pic}^0_k(C)$

3. The **Kummer line** $K_C = J_C/\pm$

surface

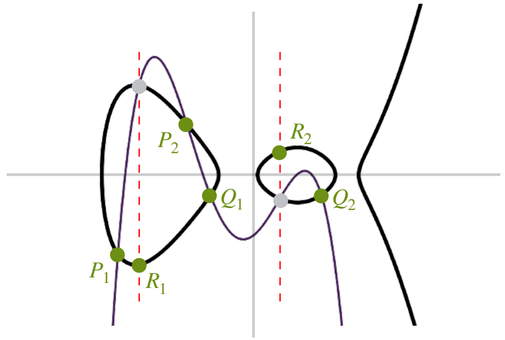
Genus 1



$$J_C = \{\ (P) - (\mathcal{O})\ :\ P \in C(k)\ \}$$

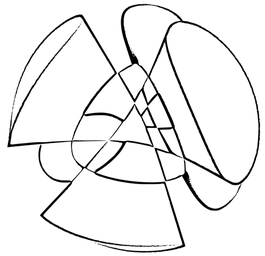
$\mathbb{P}^1 \cong K_C$

Genus 2



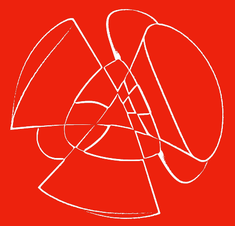
$$J_C = \{\ (P) + (Q) - D_\infty\ :\ P, Q \in C\ \}$$

$K_C \hookrightarrow \mathbb{P}^3$



Return of the Kummer

1



Kummer Surfaces

2

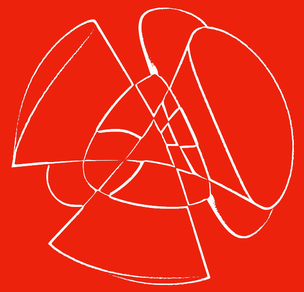
$$\begin{array}{ccc} \mathcal{J}_\alpha & \xrightarrow{\kappa} & \mathcal{J}_{\lambda,\mu,\nu} \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ \mathcal{K}_\alpha & \xrightarrow{\kappa^*} & \mathcal{K}_{\lambda,\mu,\nu} \end{array}$$

Kummers In Cryptography

3

$$\begin{array}{ccccc} 0 & \longrightarrow & E[n] & \longrightarrow & E \\ & & & & \downarrow{\scriptstyle [n]} \\ E & \longrightarrow & E/[n]E & \longrightarrow & 0 \end{array}$$

Pairings on Kummers



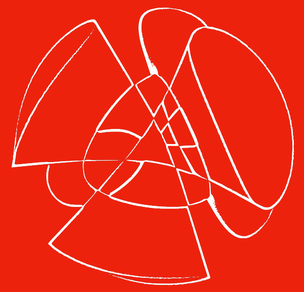
Kummer Surfaces

1

Starting point
genus 2 *hyperelliptic curve*

$$C : y^2 = f(x)$$

(general form)



Kummer Surfaces

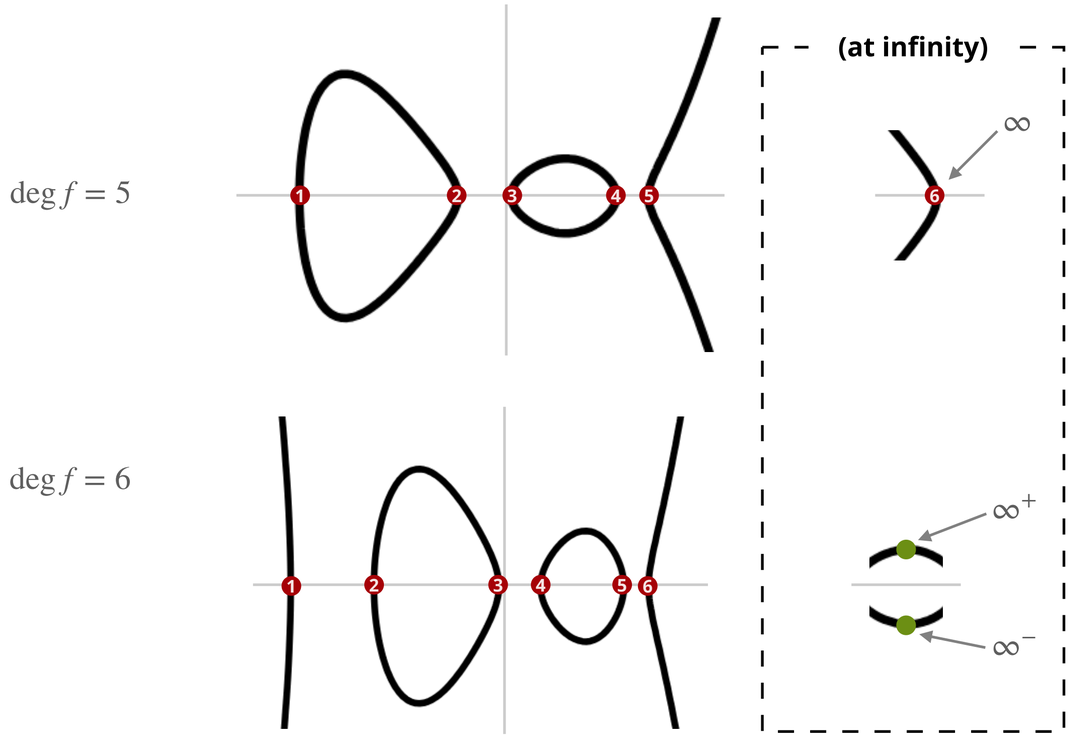
1

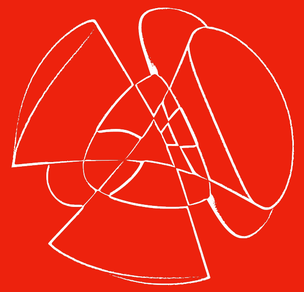
Starting point
genus 2 *hyperelliptic curve*

$$C : y^2 = f(x)$$

(general form)

Interpretation of curves





Kummer Surfaces

1

Starting point
genus 2 *hyperelliptic curve*

$$C : y^2 = f(x)$$

(general form)

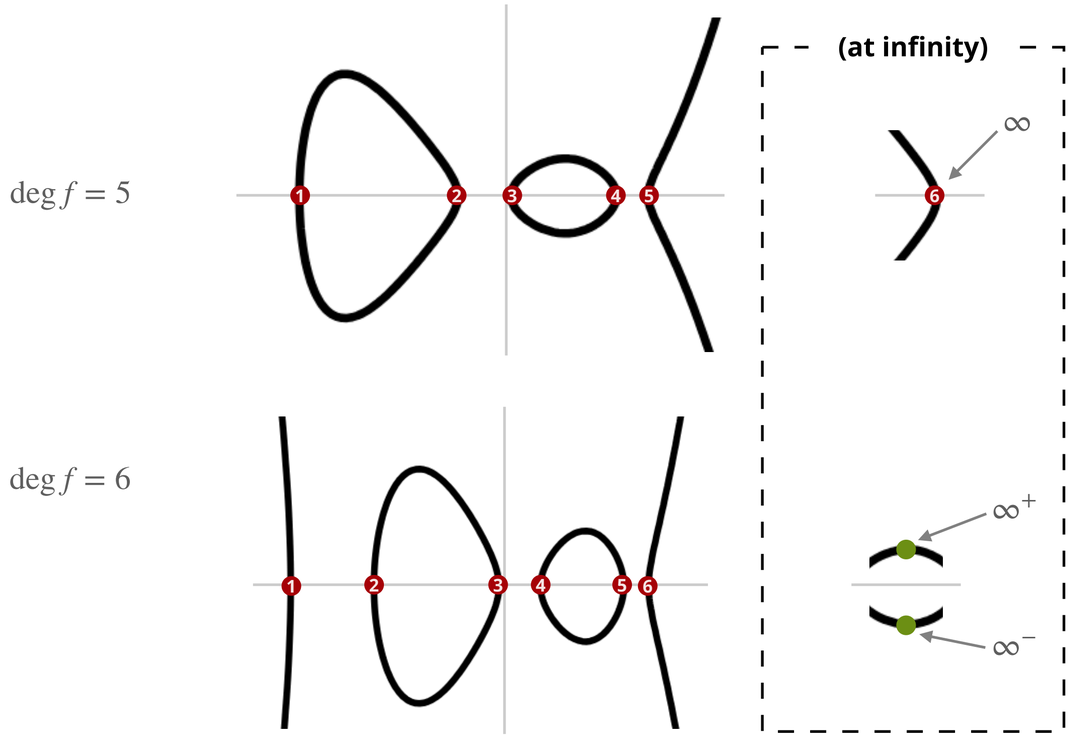
2

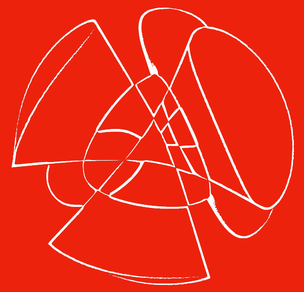
Rosenhain form

$$C_{\lambda,\mu,\nu} : y^2 = x(x-1)(x-\lambda)(x-\mu)(x-\nu)$$

$\lambda, \mu, \nu \in k$ are Rosenhain invariants

Interpretation of curves





Kummer Surfaces

1

Starting point
genus 2 *hyperelliptic curve*

$$C : y^2 = f(x)$$

(general form)

$$\kappa \downarrow \quad (x, y) \in C \quad \mapsto \quad \left(\frac{ax+b}{cx+d}, \frac{ey}{(cx+d)^3}\right) \in C_{\lambda,\mu,\nu}$$

! when 2-torsion is rational

2

Rosenhain form

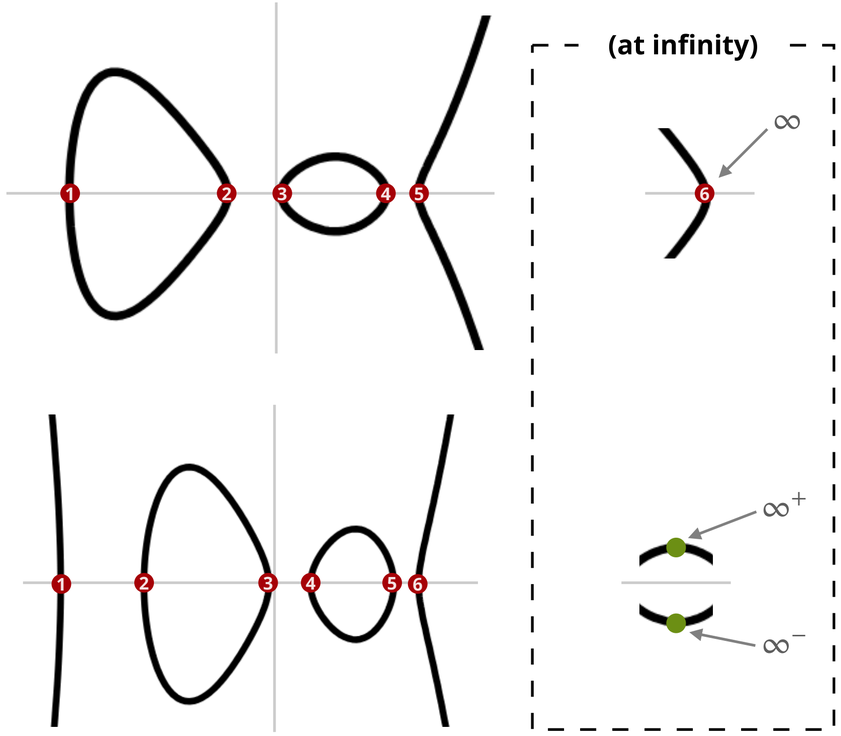
$$C_{\lambda,\mu,\nu} : y^2 = x(x-1)(x-\lambda)(x-\mu)(x-\nu)$$

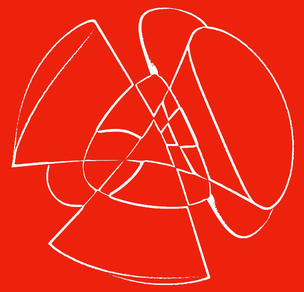
$\lambda, \mu, \nu \in k$ are Rosenhain invariants

Interpretation of curves

$\deg f = 5$

$\deg f = 6$





Kummer Surfaces

1

Starting point
genus 2 *hyperelliptic curve*

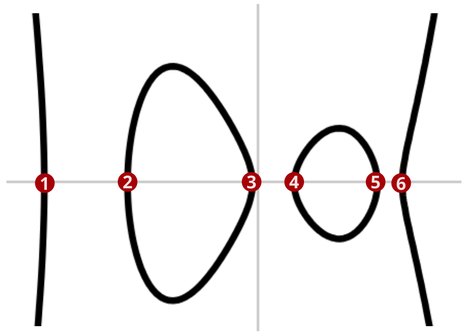
$$C : y^2 = f(x)$$

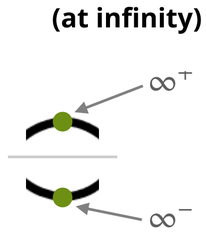
(general form)

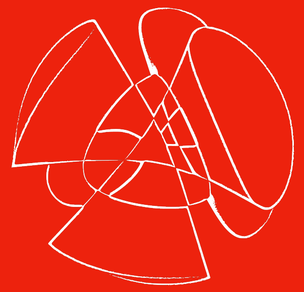
2

Jacobian
start with *two* points on C,
map to divisors

$$(P_1, P_2) \mapsto (P_1) + (P_2) - D_\infty$$







Kummer Surfaces

1

Starting point
genus 2 *hyperelliptic curve*

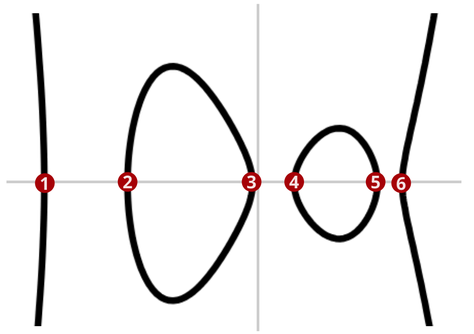
$$C : y^2 = f(x)$$

(general form)

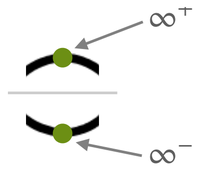
2

Jacobian
start with *two* points on C,
map to divisors

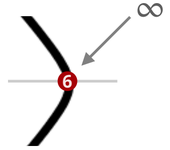
$$(P_1, P_2) \mapsto (P_1) + (P_2) - D_\infty$$



(at infinity)

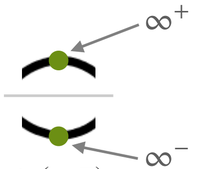


$\deg f = 5$

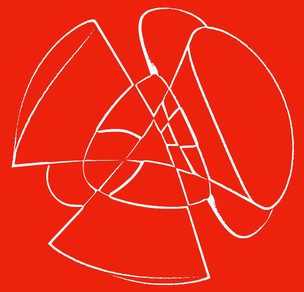


$D_\infty = 2(\infty)$

$\deg f = 6$



$D_\infty = (\infty^+) + (\infty^-)$



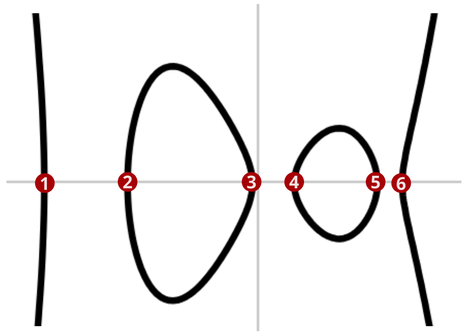
Kummer Surfaces

1

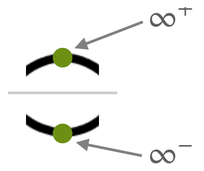
Starting point
genus 2 *hyperelliptic curve*

$$C : y^2 = f(x)$$

(general form)



(at infinity)

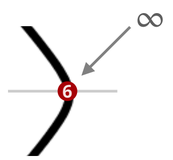


2

Jacobian
start with *two* points on C,
map to divisors

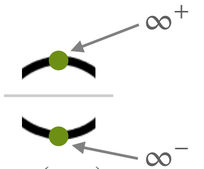
$$(P_1, P_2) \mapsto (P_1) + (P_2) - D_\infty$$

$\deg f = 5$



$D_\infty = 2(\infty)$

$\deg f = 6$



$D_\infty = (\infty^+) + (\infty^-)$

Mumford representation

We will represent an element of the Jacobian

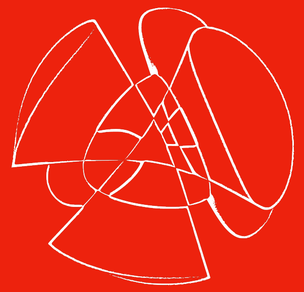
$$D_P = (P_1) + (P_2) \in J_C \qquad P_1 = (x_1, y_1), \quad P_2 = (x_2, y_2)$$

using the *Mumford representation* $\langle a(x), b(x) \rangle$

$$a(x) = (x - x_1)(x - x_2)\ , \qquad b(x_i) = y_i\ .$$

With D_∞ as $\langle 1,0 \rangle$

1



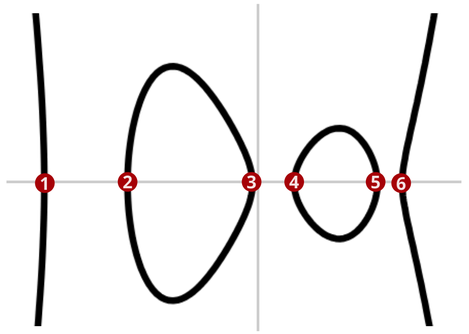
Kummer Surfaces

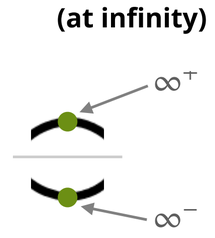
1

Starting point
genus 2 *hyperelliptic curve*

$$C : y^2 = f(x)$$

(general form)

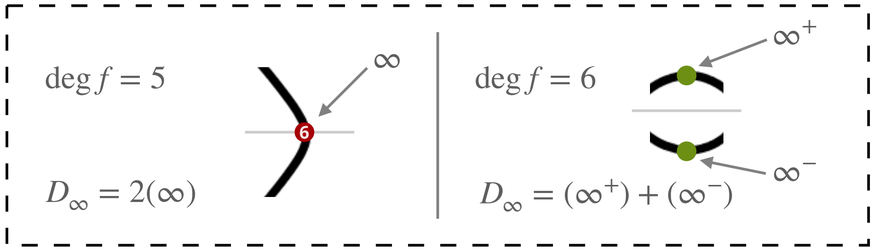




2

Jacobian
start with *two* points on C,
map to divisors

$$(P_1, P_2) \mapsto (P_1) + (P_2) - D_\infty$$



Mumford representation

We will represent an element of the Jacobian

$$D_P = (P_1) + (P_2) \in J_C \qquad P_1 = (x_1, y_1), \quad P_2 = (x_2, y_2)$$

using the *Mumford representation* $\langle a(x), b(x) \rangle$

$$a(x) = (x - x_1)(x - x_2)\ , \qquad b(x_i) = y_i\ .$$

With D_∞ as $\langle 1,0 \rangle$

Galois invariance

Elements of J_C are not just pairs of points from $C(k)$, but can come from larger fields $C(K)$, as long as they are Galois invariant under $\mathrm{Gal}(K/k)$!

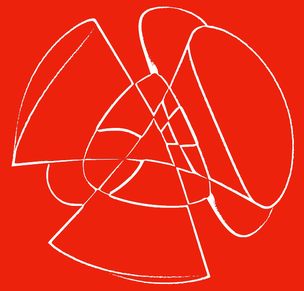
For us, in practice with $k = \mathbb{F}_p$, this means also elements

$$D_P = \big((i, 3 - i)\big) + \big((-i, 3 + i)\big)$$

Convenient: Mumford rep. is then defined over k:

$$D_P = \big(x^2 + 1, -x + 3\big)$$

1



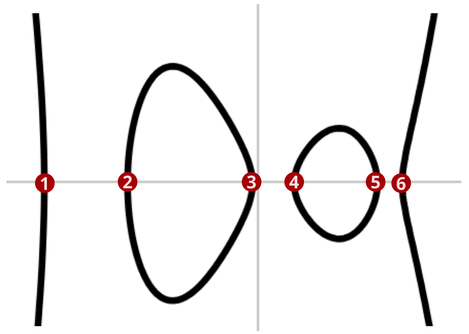
Kummer Surfaces

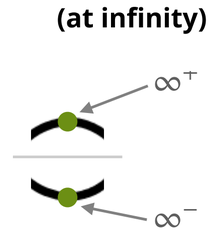
1

Starting point
genus 2 *hyperelliptic curve*

$$C : y^2 = f(x)$$

(general form)

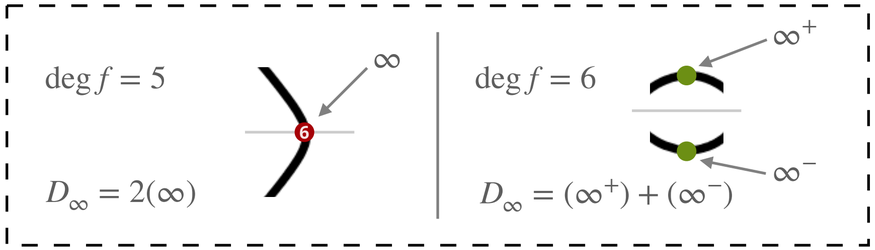




2

Jacobian
start with *two* points on C,
map to divisors

$$(P_1, P_2) \mapsto (P_1) + (P_2) - D_\infty$$



Mumford representation

We will represent an element of the Jacobian

$$D_P = (P_1) + (P_2) \in J_C \qquad P_1 = (x_1, y_1), \quad P_2 = (x_2, y_2)$$

using the *Mumford representation* $\langle a(x), b(x) \rangle$

$$a(x) = (x - x_1)(x - x_2)\ , \qquad b(x_i) = y_i\ .$$

With D_∞ as $\langle 1,0 \rangle$

Galois invariance

Elements of J_C are not just pairs of points from $C(k)$, but can come from larger fields $C(K)$, as long as they are Galois invariant under $\mathrm{Gal}(K/k)$!

For us, in practice with $k = \mathbb{F}_p$, this means also elements

$$D_P = \big((i, 3 - i)\big) + \big((-i, 3 + i)\big)$$

Convenient: Mumford rep. is then defined over k:

$$D_P = \big(x^2 + 1, -x + 3\big)$$

!

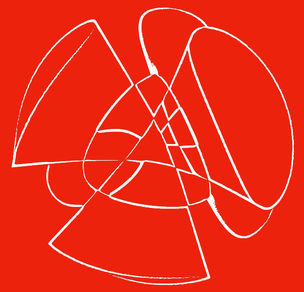
genus 1

This should remind you of how $\langle K \rangle$ can be the kernel of an isogeny over $\mathbb{F}_p$, even if K is a point in $C(\mathbb{F}_{p^2})$:

$$f(x) = \prod (x - x_{[i]K})$$

is defined over $\mathbb{F}_p$!

Radboud University



Kummer Surfaces

1

Starting point
genus 2 *hyperelliptic curve*

$$C : y^2 = f(x)$$

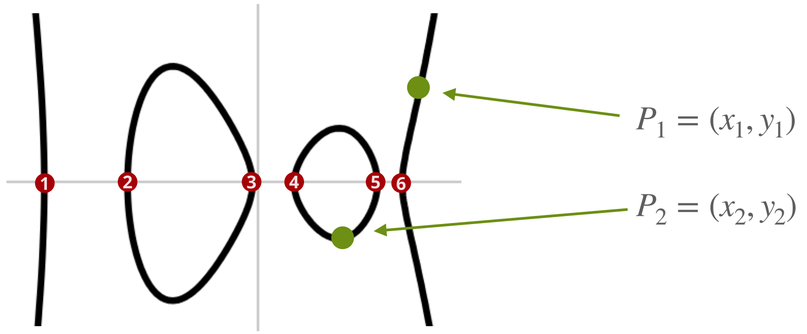
(general form)

2

Jacobian
start with *two* points on C,
map to divisors

$$(P_1, P_2) \mapsto (P_1) + (P_2) - D_\infty$$

then use Mumford representation $\langle\ a(x),\ b(x)\ \rangle$



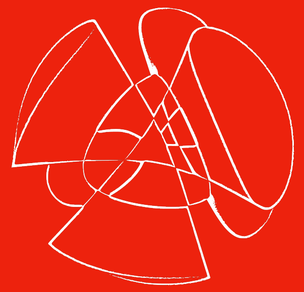
$$D_P = \langle\ a(x),\ b(x)\ \rangle \in \mathrm{Jac}(C)$$

Cantor's algorithm

Given two elements D_P, D_Q in Mumford rep.
computes the resulting $D_R = D_P + D_Q$.

Roughly all we need to do arithmetic on the Jacobian, e.g. scalar mults and so on!
However, very slow for practical things...

[1] D. Cantor, "Computing in the jacobian of a hyperelliptic curve", Mathematics of Computation, 48 (1987), 95-101.



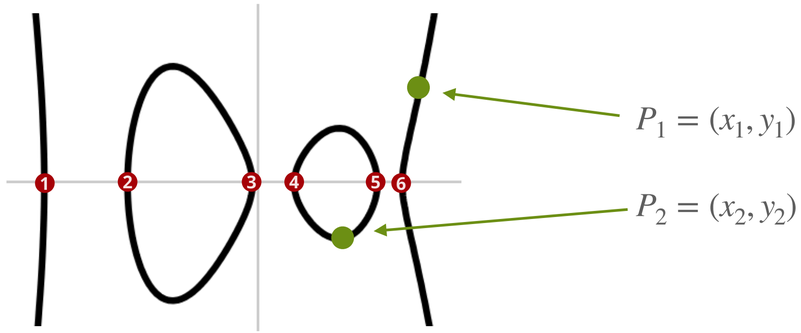
Kummer Surfaces

1

Starting point
genus 2 *hyperelliptic curve*

$$C : y^2 = f(x)$$

(general form)



2

Jacobian
start with *two* points on C,
map to divisors

$$(P_1, P_2) \mapsto (P_1) + (P_2) - D_\infty$$

then use Mumford representation $\langle\ a(x),\ b(x)\ \rangle$

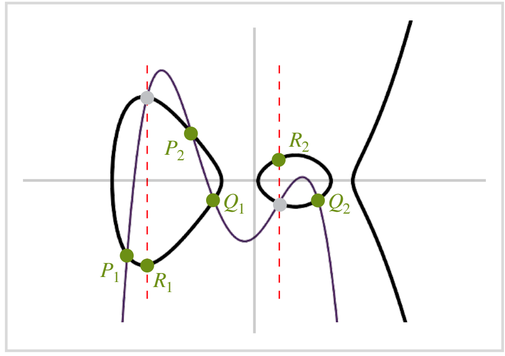
$$D_P = \langle\ a(x),\ b(x)\ \rangle \in \mathrm{Jac}(C)$$

Cantor's algorithm

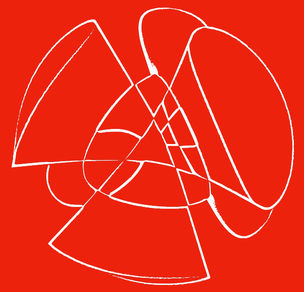
Given two elements D_P, D_Q in Mumford rep.
computes the resulting $D_R = D_P + D_Q$.

Roughly all we need to do arithmetic on the Jacobian, e.g. scalar mults and so on!
However, very slow for practical things...

curve interpretation



[1] D. Cantor, "Computing in the jacobian of a hyperelliptic curve", Mathematics of Computation, 48 (1987), 95-101.



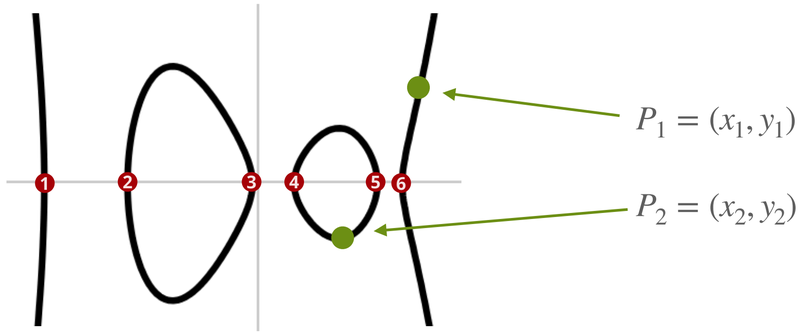
Kummer Surfaces

1

Starting point
genus 2 *hyperelliptic curve*

$$C : y^2 = f(x)$$

(general form)



2

Jacobian
start with *two* points on C,
map to divisors

$$(P_1, P_2) \mapsto (P_1) + (P_2) - D_\infty$$

then use Mumford representation $\langle\ a(x),\ b(x)\ \rangle$

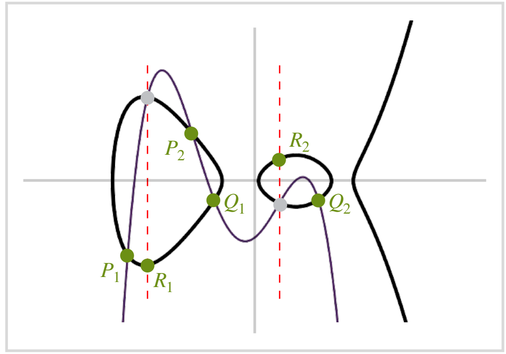
$$D_P = \langle\ a(x),\ b(x)\ \rangle \in \mathrm{Jac}(C)$$

Cantor's algorithm

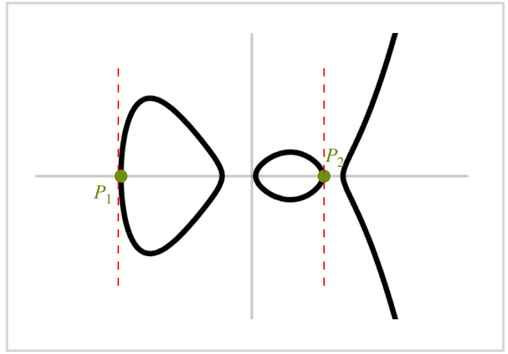
Given two elements D_P, D_Q in Mumford rep.
computes the resulting $D_R = D_P + D_Q$.

Roughly all we need to do arithmetic on the Jacobian, e.g. scalar mults and so on!
However, very slow for practical things...

curve interpretation →

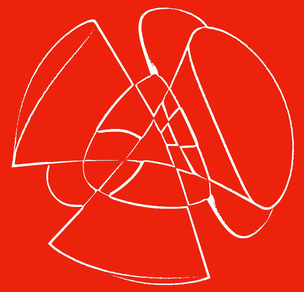


order 2? →



[1] D. Cantor, "Computing in the jacobian of a hyperelliptic curve", Mathematics of Computation, 48 (1987), 95-101.

1



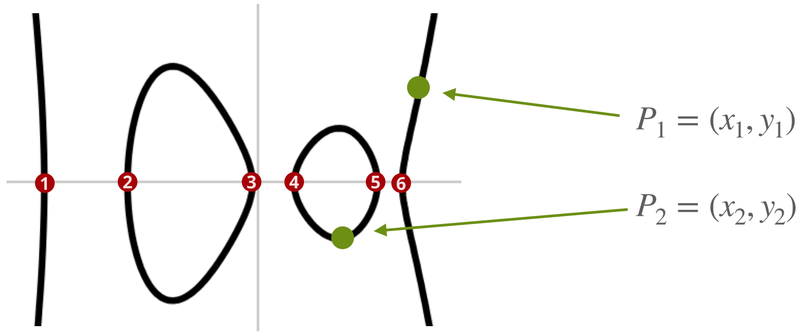
Kummer Surfaces

1

Starting point
genus 2 *hyperelliptic curve*

$$C : y^2 = f(x)$$

(general form)



2

Jacobian
start with *two* points on C,
map to divisors

$$(P_1, P_2) \mapsto (P_1) + (P_2) - D_\infty$$

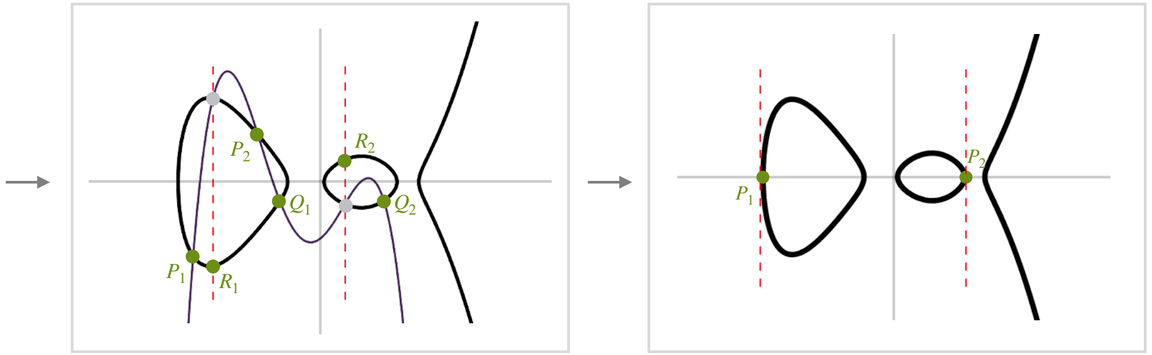
then use Mumford representation $\langle\ a(x),\ b(x)\ \rangle$

$$D_P = \langle\ a(x),\ b(x)\ \rangle \in \mathrm{Jac}(C)$$

Cantor's algorithm

Given two elements D_P, D_Q in Mumford rep.
computes the resulting $D_R = D_P + D_Q$.

Roughly all we need to do arithmetic on the Jacobian, e.g. scalar mults and so on!
However, very slow for practical things...



Points of order 2

Precisely the elements given by pairs of *Weierstrass points* $(w_i,0)$, for $1 \le i \le 6$.

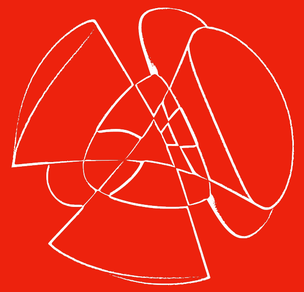
In Mumford representation

$$L_{i,j} = \langle (x - w_i)(x - w_j),\ 0 \rangle\ ,$$

and we easily count $\binom{6}{2} = 15$ of them:

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

[1] D. Cantor, "Computing in the jacobian of a hyperelliptic curve", Mathematics of Computation, 48 (1987), 95-101.



Kummer Surfaces

1

Starting point
genus 2 *hyperelliptic curve*

$$C : y^2 = f(x)$$

(general form)

2

Jacobian
start with *two* points on C,
map to divisors

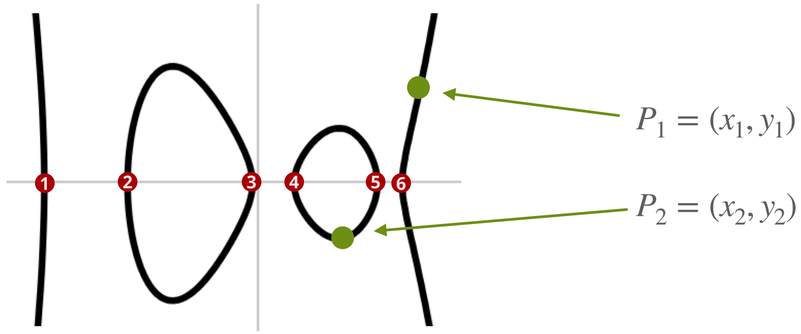
$$(P_1, P_2) \mapsto (P_1) + (P_2) - D_\infty$$

then use Mumford representation $\langle\ a(x),\ b(x)\ \rangle$

3

Kummer
essentially, elements $D_P \in \mathrm{Jac}(C)$
up to ± 1, so $D_p = -D_p$ on Kummer

by *magic* becomes a surface K_C in $\mathbb{P}^3$

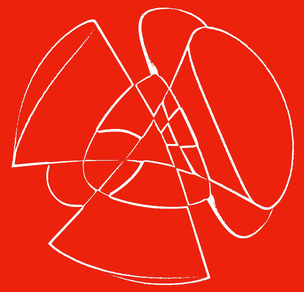


$$D_P = \langle\ a(x),\ b(x)\ \rangle \in \mathrm{Jac}(C)$$

$$K_C : K_2 \cdot X_4^2 + K_1 \cdot X_4 + K_0 = 0\ .$$

for polynomials K_0, K_1, K_2
in variables X_1, X_2, X_3

Elements are $\pm D_P = (X_1 : X_2 : X_3 : X_4) \in K_C$



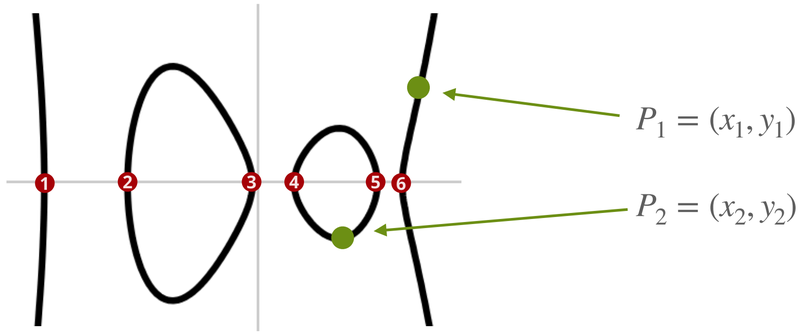
Kummer Surfaces

1

Starting point
genus 2 *hyperelliptic curve*

$$C : y^2 = f(x)$$

(general form)



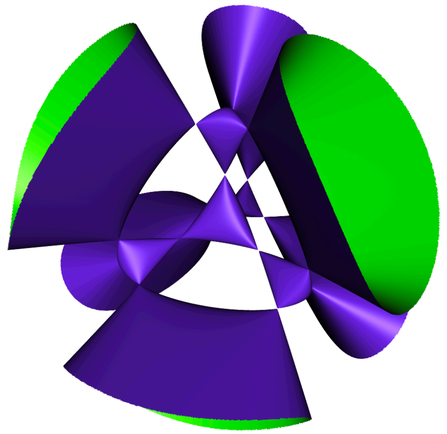
2

Jacobian
start with *two* points on C,
map to divisors

$$(P_1, P_2) \mapsto (P_1) + (P_2) - D_\infty$$

then use Mumford representation $\langle\ a(x),\ b(x)\ \rangle$

$$D_P = \langle\ a(x),\ b(x)\ \rangle \in \mathrm{Jac}(C)$$



3

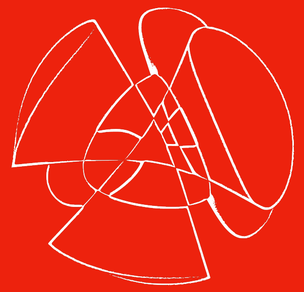
Kummer
essentially, elements $D_P \in \mathrm{Jac}(C)$
up to ± 1, so $D_p = -D_p$ on Kummer

by *magic* becomes a surface K_C in $\mathbb{P}^3$

$$K_C : K_2 \cdot X_4^2 + K_1 \cdot X_4 + K_0 = 0\ .$$

for polynomials K_0, K_1, K_2
in variables X_1, X_2, X_3

Elements are $\pm D_P = (X_1 : X_2 : X_3 : X_4) \in K_C$



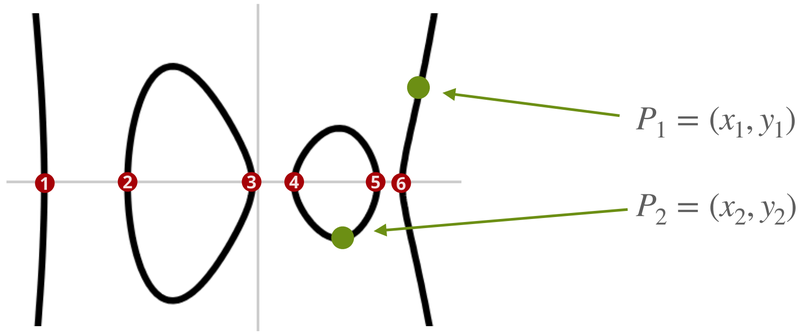
Kummer Surfaces

1

Starting point
genus 2 *hyperelliptic curve*

$$C : y^2 = f(x)$$

(general form)



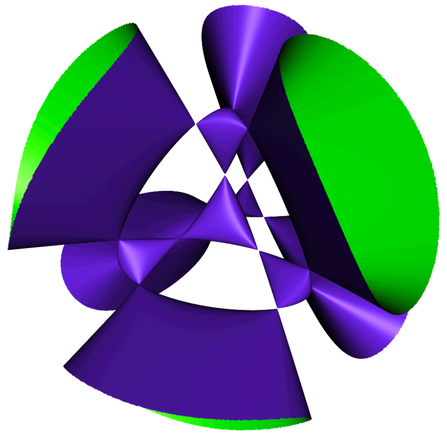
2

Jacobian
start with *two* points on C,
map to divisors

$$(P_1, P_2) \mapsto (P_1) + (P_2) - D_\infty$$

then use Mumford representation $\langle\ a(x),\ b(x)\ \rangle$

$$D_P = \langle\ a(x),\ b(x)\ \rangle \in \mathrm{Jac}(C)$$



3

Kummer
essentially, elements $D_P \in \mathrm{Jac}(C)$
up to ± 1, so $D_p = -D_p$ on Kummer

by *magic* becomes a surface K_C in $\mathbb{P}^3$

$$K_C : K_2 \cdot X_4^2 + K_1 \cdot X_4 + K_0 = 0\ .$$

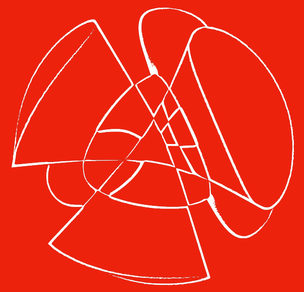
for polynomials K_0, K_1, K_2
in variables X_1, X_2, X_3

Elements are $\pm D_P = (X_1 : X_2 : X_3 : X_4) \in K_C$

Examples

$$D_\infty \in \mathrm{Jac}(C) \quad \longrightarrow \quad \mathbf{o} = (\ 0 : 0 : 0 : 1\ ) \in K_C$$

$$L_{i,j} = \langle\ (x - w_i)(x - w_j),\ 0\ \rangle \quad \longrightarrow \quad D_{i,j} = (\ 1 : w_i + w_j : w_i \cdot w_j : \gamma\ )$$



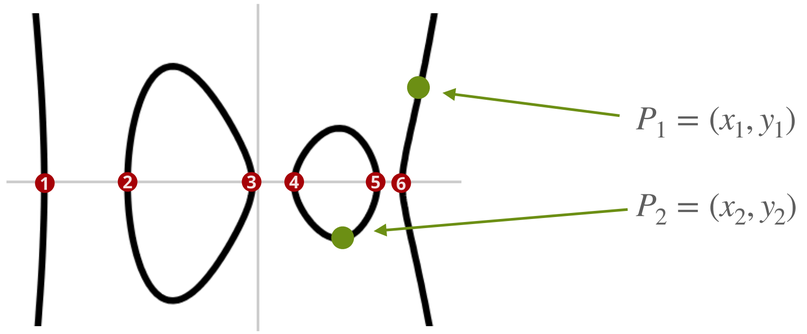
Kummer Surfaces

1

Starting point
genus 2 *hyperelliptic curve*

$$C : y^2 = f(x)$$

(general form)



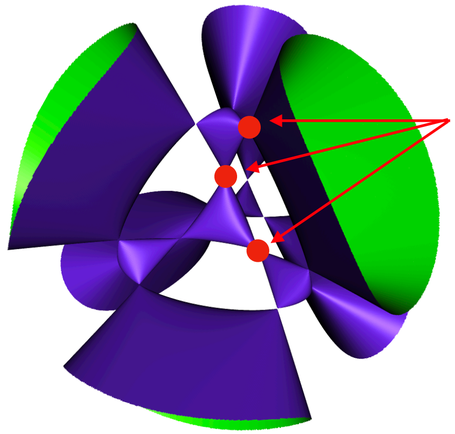
2

Jacobian
start with *two* points on C,
map to divisors

$$(P_1, P_2) \mapsto (P_1) + (P_2) - D_\infty$$

then use Mumford representation $\langle\ a(x),\ b(x)\ \rangle$

$$D_P = \langle\ a(x),\ b(x)\ \rangle \in \mathrm{Jac}(C)$$



3

Kummer
essentially, elements $D_P \in \mathrm{Jac}(C)$
up to ± 1, so $D_p = -D_p$ on Kummer

by *magic* becomes a surface K_C in $\mathbb{P}^3$

$$K_C : K_2 \cdot X_4^2 + K_1 \cdot X_4 + K_0 = 0\ .$$

for polynomials K_0, K_1, K_2
in variables X_1, X_2, X_3

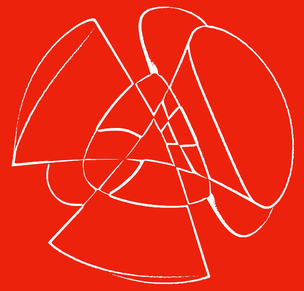
Elements are $\pm D_P = (X_1 : X_2 : X_3 : X_4) \in K_C$

Examples

$$D_\infty \in \mathrm{Jac}(C) \quad \longrightarrow \quad \mathbf{o} = (\ 0 : 0 : 0 : 1\ ) \in K_C$$

$$L_{i,j} = \langle\ (x - w_i)(x - w_j),\ 0\ \rangle \quad \longrightarrow \quad D_{i,j} = (\ 1 : w_i + w_j : w_i \cdot w_j : \gamma\ )$$

1



Kummer Surfaces

1

Curve

$$C : y^2 = x^6 + c_5x^5 + c_4x^4 + c_3x^3 + c_2x^2 + c_1x + c_0$$

2

Jacobian

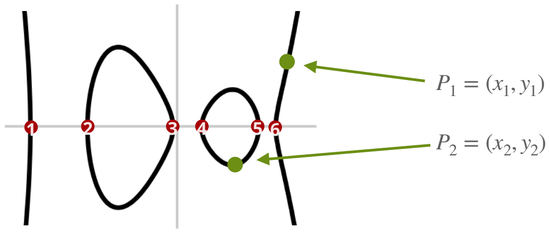
Mumford Reps. $D_P = \langle a(x), b(x) \rangle$ of pairs of points of C

3

Kummer surface

Elem. of J_C up to involution $\pm$, embedded into $\mathbb{P}^3$

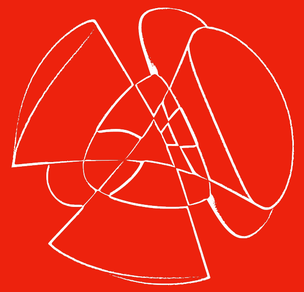
$$\pm D_P = (X_1 : X_2 : X_3 : X_4)\ , \qquad K_C : K_2 \cdot X_4^2 + K_1 \cdot X_4 + K_0 = 0\ .$$



$$D_P = \langle\ a(x),\ b(x)\ \rangle \in \mathrm{Jac}(C)$$

$$\pm D_P = (X_1 : X_2 : X_3 : X_4) \in K_C$$

1



Kummer Surfaces

1 Curve

$$C : y^2 = x^6 + c_5x^5 + c_4x^4 + c_3x^3 + c_2x^2 + c_1x + c_0$$

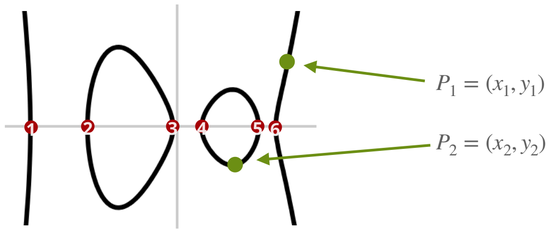
2 Jacobian

Mumford Reps. $D_P = \langle a(x), b(x) \rangle$ of pairs of points of C

3 Kummer surface

Elem. of J_C up to involution $\pm$, embedded into $\mathbb{P}^3$

$$\pm D_P = (X_1 : X_2 : X_3 : X_4) \ , \qquad K_C : K_2 \cdot X_4^2 + K_1 \cdot X_4 + K_0 = 0 \ .$$



$$D_P = \langle \ a(x), \ b(x) \ \rangle \in \mathrm{Jac}(C)$$

$$\pm D_P = (X_1 : X_2 : X_3 : X_4) \in K_C$$

warning!

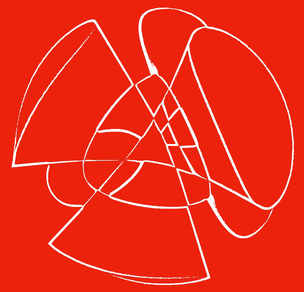
The construction *so far* assumes a **general** curve C and constructs the **general** Kummer surface K_C

Advantage:
- mathematically elegant
- always exists
- well-described by Cassels & Flynn

Disadvantage:
- not fast enough

[1] J.W.S. Cassels and E.V. Flynn, *Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2,* Cambridge University Press, 1996.
[2] D.V Chudnovsky, G.V Chudnovsky, *Sequences of numbers generated by addition in formal groups and new primality and factorization tests,* Advances in Applied Mathematics, Volume 7, Issue 4, 1986.
[3] P. Gaudry. *Fast genus 2 arithmetic based on Theta functions.* J. Mathematical Cryptology, 1(3):243– 265, 2007.
[4] D. J. Bernstein. *Elliptic vs. Hyperelliptic, part I.* Talk at ECC (slides at http://cr.yp.to/talks/ 2006.09.20/slides.pdf), September 2006.

1



Kummer Surfaces

1

Curve

$$C : y^2 = x^6 + c_5x^5 + c_4x^4 + c_3x^3 + c_2x^2 + c_1x + c_0$$

2

Jacobian

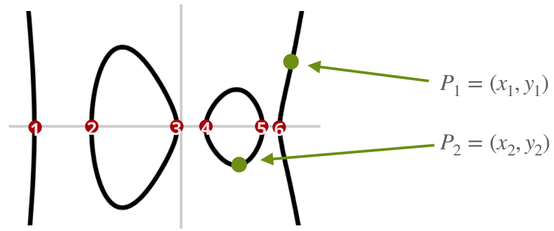
Mumford Reps. $D_P = \langle a(x), b(x) \rangle$ of pairs of points of C

3

Kummer surface

Elem. of J_C up to involution $\pm$, embedded into $\mathbb{P}^3$

$$\pm D_P = (X_1 : X_2 : X_3 : X_4) \ , \qquad K_C : K_2 \cdot X_4^2 + K_1 \cdot X_4 + K_0 = 0 \ .$$



$$D_P = \langle \ a(x), \ b(x) \ \rangle \in \mathrm{Jac}(C)$$

$$\pm D_P = (X_1 : X_2 : X_3 : X_4) \in K_C$$

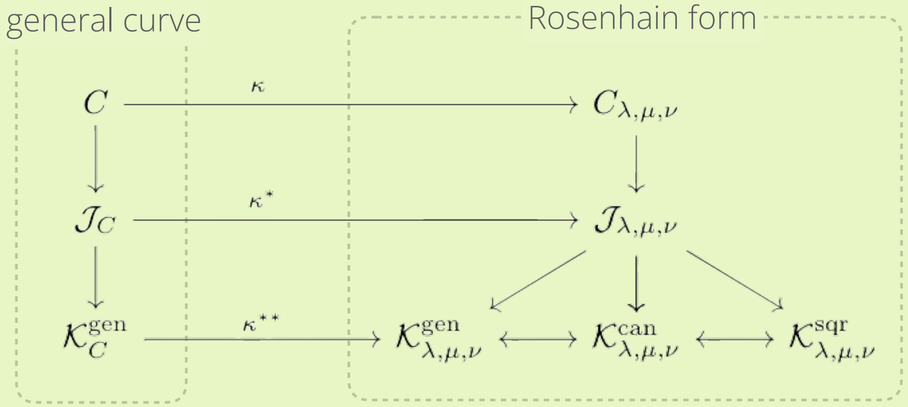
warning!

The construction *so far* assumes a **general** curve C and constructs the **general** Kummer surface K_C

Advantage:
- mathematically elegant
- always exists
- well-described by Cassels & Flynn

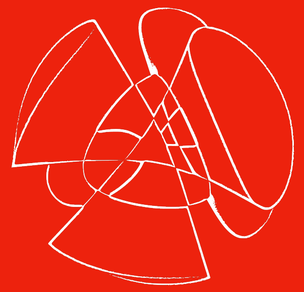
Disadvantage:
- not fast enough

Kummer zoo



[1] J.W.S. Cassels and E.V. Flynn, *Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2,* Cambridge University Press, 1996.
[2] D.V Chudnovsky, G.V Chudnovsky, *Sequences of numbers generated by addition in formal groups and new primality and factorization tests,* Advances in Applied Mathematics, Volume 7, Issue 4, 1986.
[3] P. Gaudry. *Fast genus 2 arithmetic based on Theta functions.* J. Mathematical Cryptology, 1(3):243– 265, 2007.
[4] D. J. Bernstein. *Elliptic vs. Hyperelliptic, part I.* Talk at ECC (slides at http://cr.yp.to/talks/ 2006.09.20/slides.pdf), September 2006.

1



Kummer Surfaces

1

Curve

$$C : y^2 = x^6 + c_5x^5 + c_4x^4 + c_3x^3 + c_2x^2 + c_1x + c_0$$

2

Jacobian

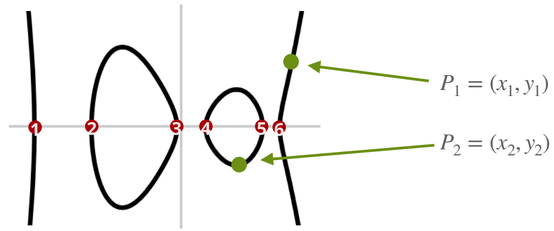
Mumford Reps. $D_P = \langle a(x), b(x) \rangle$ of pairs of points of C

3

Kummer surface

Elem. of J_C up to involution $\pm$, embedded into $\mathbb{P}^3$

$$\pm D_P = (X_1 : X_2 : X_3 : X_4) \ , \qquad K_C : K_2 \cdot X_4^2 + K_1 \cdot X_4 + K_0 = 0 \ .$$



$$D_P = \langle \ a(x), \ b(x) \ \rangle \in \mathrm{Jac}(C)$$

$$\pm D_P = (X_1 : X_2 : X_3 : X_4) \in K_C$$

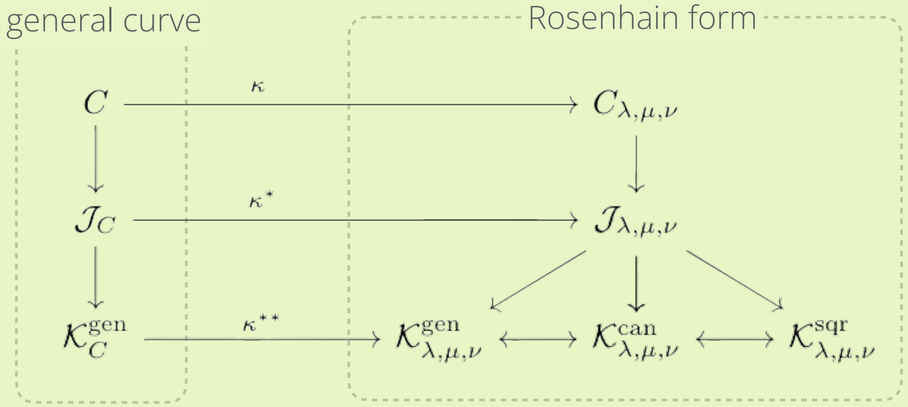
warning!

The construction *so far* assumes a **general** curve C and constructs the **general** Kummer surface K_C

Advantage:
- mathematically elegant
- always exists
- well-described by Cassels & Flynn

Disadvantage:
- not fast enough

Kummer zoo



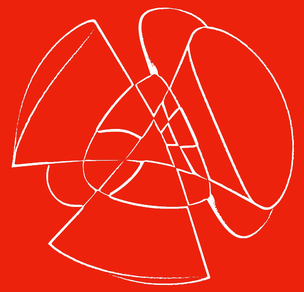
1

General Kummer with great intro by Cassels & Flynn, as described before, with

$$\mathcal{K}_{\lambda,\mu,\nu}^{\mathrm{gen}} \ : \ K_2 \cdot X_4^2 + K_1 \cdot X_4 + K_0 = 0 \ .$$

[1] J.W.S. Cassels and E.V. Flynn, *Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2,* Cambridge University Press, 1996.
[2] D.V Chudnovsky, G.V Chudnovsky, *Sequences of numbers generated by addition in formal groups and new primality and factorization tests,* Advances in Applied Mathematics, Volume 7, Issue 4, 1986.
[3] P. Gaudry. *Fast genus 2 arithmetic based on Theta functions.* J. Mathematical Cryptology, 1(3):243– 265, 2007.
[4] D. J. Bernstein. *Elliptic vs. Hyperelliptic, part I.* Talk at ECC (slides at http://cr.yp.to/talks/ 2006.09.20/slides.pdf), September 2006.

1



Kummer Surfaces

1

Curve

$$C : y^2 = x^6 + c_5x^5 + c_4x^4 + c_3x^3 + c_2x^2 + c_1x + c_0$$

2

Jacobian

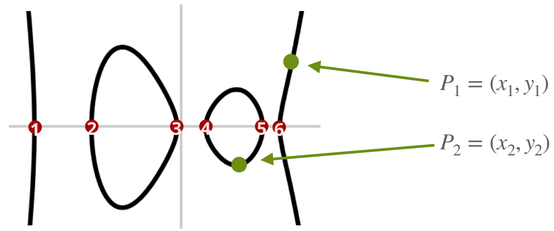
Mumford Reps. $D_P = \langle a(x), b(x) \rangle$ of pairs of points of C

3

Kummer surface

Elem. of J_C up to involution $\pm$, embedded into $\mathbb{P}^3$

$$\pm D_P = (X_1 : X_2 : X_3 : X_4) \ , \qquad K_C : K_2 \cdot X_4^2 + K_1 \cdot X_4 + K_0 = 0 \ .$$



$$D_P = \langle \ a(x), \ b(x) \ \rangle \in \mathrm{Jac}(C)$$

$$\pm D_P = (X_1 : X_2 : X_3 : X_4) \in K_C$$

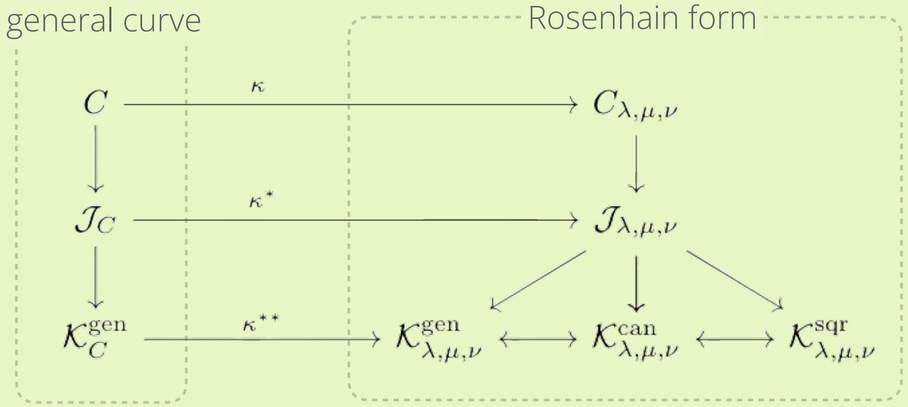
warning!

The construction *so far* assumes a **general** curve C and constructs the **general** Kummer surface K_C

Advantage:
- mathematically elegant
- always exists
- well-described by Cassels & Flynn

Disadvantage:
- not fast enough

Kummer zoo



1

General Kummer with great intro by Cassels & Flynn, as described before, with

$$\mathcal{K}_{\lambda,\mu,\nu}^{\mathrm{gen}} \ : \ K_2 \cdot X_4^2 + K_1 \cdot X_4 + K_0 = 0 \ .$$

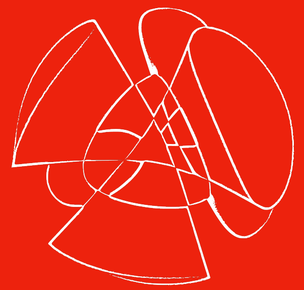
2

Canonical (?) Kummer introduced by Chud. bros, used by Gaudry, with

$$\mathcal{K}_{\lambda,\mu,\nu}^{\mathrm{can}} \ : \ X_1^4 + X_2^4 + X_3^4 + X_4^4 + 2E \cdot X_1X_2X_3X_4 = \begin{matrix} F \cdot (X_1^2X_4^2 + X_2^2X_3^2) \\ G \cdot (X_1^2X_3^2 + X_2^2X_4^2) \\ H \cdot (X_1^2X_2^2 + X_3^2X_4^2) \end{matrix} \begin{matrix} + \\ + \\ \end{matrix}$$

[1] J.W.S. Cassels and E.V. Flynn, *Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2,* Cambridge University Press, 1996.
[2] D.V Chudnovsky, G.V Chudnovsky, *Sequences of numbers generated by addition in formal groups and new primality and factorization tests,* Advances in Applied Mathematics, Volume 7, Issue 4, 1986.
[3] P. Gaudry. *Fast genus 2 arithmetic based on Theta functions.* J. Mathematical Cryptology, 1(3):243– 265, 2007.
[4] D. J. Bernstein. *Elliptic vs. Hyperelliptic, part I.* Talk at ECC (slides at http://cr.yp.to/talks/ 2006.09.20/slides.pdf), September 2006.

1



Kummer Surfaces

1

Curve

$$C : y^2 = x^6 + c_5x^5 + c_4x^4 + c_3x^3 + c_2x^2 + c_1x + c_0$$

2

Jacobian

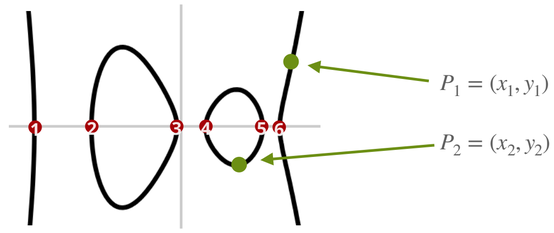
Mumford Reps. $D_P = \langle a(x), b(x) \rangle$ of pairs of points of C

3

Kummer surface

Elem. of J_C up to involution $\pm$, embedded into $\mathbb{P}^3$

$$\pm D_P = (X_1 : X_2 : X_3 : X_4) \ , \qquad K_C : K_2 \cdot X_4^2 + K_1 \cdot X_4 + K_0 = 0 \ .$$



$$D_P = \langle \ a(x), \ b(x) \ \rangle \in \mathrm{Jac}(C)$$

$$\pm D_P = (X_1 : X_2 : X_3 : X_4) \in K_C$$

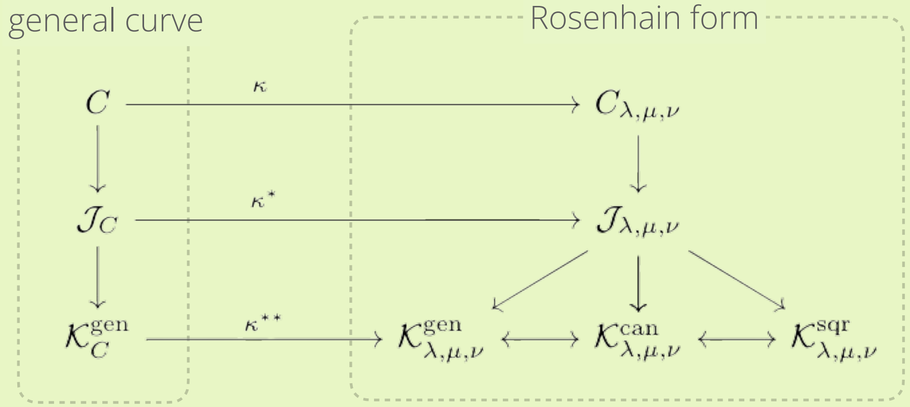
warning!

The construction *so far* assumes a **general** curve C and constructs the **general** Kummer surface K_C

Advantage:
- mathematically elegant
- always exists
- well-described by Cassels & Flynn

Disadvantage:
- not fast enough

Kummer zoo



1

General Kummer with great intro by Cassels & Flynn, as described before, with

$$\mathcal{K}_{\lambda,\mu,\nu}^{\mathrm{gen}} \ : \ K_2 \cdot X_4^2 + K_1 \cdot X_4 + K_0 = 0 \ .$$

2

Canonical (?) Kummer introduced by Chud. bros, used by Gaudry, with

$$\mathcal{K}_{\lambda,\mu,\nu}^{\mathrm{can}} \ : \ X_1^4 + X_2^4 + X_3^4 + X_4^4 + 2E \cdot X_1X_2X_3X_4 = \begin{matrix} F \cdot (X_1^2X_4^2 + X_2^2X_3^2) \\ G \cdot (X_1^2X_3^2 + X_2^2X_4^2) \\ H \cdot (X_1^2X_2^2 + X_3^2X_4^2) \end{matrix} \begin{matrix} + \\ + \\ \end{matrix}$$

3

Squared Kummer, adapted Canonical, by Bernstein for high-speed crypto, with

$$\mathcal{K}_{\lambda,\mu,\nu}^{\mathrm{sqr}} \ : \ F \cdot X_1X_2X_3X_4 = \\ (X_1^2 + X_2^2 + X_3^2 + X_4^2 - G \cdot (X_1 + X_2)(X_3 + X_4) - H \cdot (X_1X_2 + X_3X_4))^2$$

[1] J.W.S. Cassels and E.V. Flynn, *Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2,* Cambridge University Press, 1996.
[2] D.V Chudnovsky, G.V Chudnovsky, *Sequences of numbers generated by addition in formal groups and new primality and factorization tests,* Advances in Applied Mathematics, Volume 7, Issue 4, 1986.
[3] P. Gaudry. *Fast genus 2 arithmetic based on Theta functions.* J. Mathematical Cryptology, 1(3):243– 265, 2007.
[4] D. J. Bernstein. *Elliptic vs. Hyperelliptic, part I.* Talk at ECC (slides at http://cr.yp.to/talks/ 2006.09.20/slides.pdf), September 2006.

Radboud University

1

Hyperelliptic curve Diffie-Hellman

Sketched by Chudnovskys in 1986, picked up and worked out the details by Gaudry in 2004, then later improved by Bernstein in 2006 and others.

Hyperoptimized version in 2014:

Kummer strikes back
(Bernstein, Chuengsatiansup, Lange, Schwabe)

Faster than *elliptic* curve Diffie-Hellman, by using parallelisation only available in Kummer arithmetic.

These works give us the tools to do *fast* doubling and diff. addition on Kummer.

[1] J.W.S. Cassels and E.V. Flynn, *Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2,* Cambridge University Press, 1996.
[2] D.V Chudnovsky, G.V Chudnovsky, *Sequences of numbers generated by addition in formal groups and new primality and factorization tests,* Advances in Applied Mathematics, Volume 7, Issue 4, 1986.
[3] P. Gaudry. *Fast genus 2 arithmetic based on Theta functions*. J. Mathematical Cryptology, 1(3):243– 265, 2007.
[4] D. J. Bernstein. *Elliptic vs. Hyperelliptic, part I.* Talk at ECC (slides at http://cr.yp.to/talks/ 2006.09.20/slides.pdf), September 2006.
[5] D. J. Bernstein, C. Chuengsatiansup, T. Lange, and P. Schwabe. *Kummer strikes back: New DH speed records.* ASIACRYPT 2014.

1

Hyperelliptic curve Diffie-Hellman

Sketched by Chudnovskys in 1986, picked up and worked out the details by Gaudry in 2004, then later improved by Bernstein in 2006 and others.

Hyperoptimized version in 2014:

Kummer strikes back
(Bernstein, Chuengsatiansup, Lange, Schwabe)

Faster than *elliptic* curve Diffie-Hellman, by using parallelisation only available in Kummer arithmetic.

These works give us the tools to do *fast* doubling and diff. addition on Kummer.

2

Isogeny-based with Kummers

Works by Cosset, Lubicz, Robert since 2010, expanded by Costello in 2018. Recently, interest from HD-perspective, see e.g. Dartois, Maino, Pope, and Robert.

Goal: do cryptography on higher-dimensional abelian varieties, for example computing $(2^n,2^n)$-isogeny, either for products of curves (DMPR)

$$E \times E' \to E'' \times E'''$$

or simulate SIDH on Kummers (Costello)

$$E_\alpha \to K_\alpha \xrightarrow{\varphi} K_\beta \to E_\beta$$

These works give us the tools to do *fast* $(2,2)$-isogenies on Kummer, either using theta functions (DMPR) or curve (Costello)

[1] J.W.S. Cassels and E.V. Flynn, *Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2,* Cambridge University Press, 1996.
[2] D.V Chudnovsky, G.V Chudnovsky, *Sequences of numbers generated by addition in formal groups and new primality and factorization tests,* Advances in Applied Mathematics, Volume 7, Issue 4, 1986.
[3] P. Gaudry. *Fast genus 2 arithmetic based on Theta functions*. J. Mathematical Cryptology, 1(3):243– 265, 2007.
[4] D. J. Bernstein. *Elliptic vs. Hyperelliptic, part I.* Talk at ECC (slides at http://cr.yp.to/talks/ 2006.09.20/slides.pdf), September 2006.
[5] D. J. Bernstein, C. Chuengsatiansup, T. Lange, and P. Schwabe. *Kummer strikes back: New DH speed records.* ASIACRYPT 2014.

Radboud University

[6] For works by Cosset, Lubicz, Robert: too many to name specific one...
Good start is Robert's page: www.normalesup.org/~robert/
[7] C. Costello, *Computing supersingular isogenies on Kummer surfaces,* ASIACRYPT 2018
[8] P. Dartois, L. Maino, G. Pope, D. Robert, *An Algorithmic Approach to (2,2)-isogenies in the Theta Model and Applications to Isogeny-based Cryptography,* https://ia.cr/2023/1747

1

Hyperelliptic curve Diffie-Hellman

Sketched by Chudnovskys in 1986, picked up and worked out the details by Gaudry in 2004, then later improved by Bernstein in 2006 and others.

Hyperoptimized version in 2014:

Kummer strikes back
(Bernstein, Chuengsatiansup, Lange, Schwabe)

Faster than *elliptic* curve Diffie-Hellman, by using parallelisation only available in Kummer arithmetic.

These works give us the tools to do *fast* doubling and diff. addition on Kummer.

2

Isogeny-based with Kummers

Works by Cosset, Lubicz, Robert since 2010, expanded by Costello in 2018. Recently, interest from HD-perspective, see e.g. Dartois, Maino, Pope, and Robert.

Goal: do cryptography on higher-dimensional abelian varieties, for example computing $(2^n,2^n)$-isogeny, either for products of curves (DMPR)

$$E \times E' \to E'' \times E'''$$

or simulate SIDH on Kummers (Costello)

$$E_\alpha \to K_\alpha \xrightarrow{\varphi} K_\beta \to E_\beta$$

These works give us the tools to do *fast* $(2,2)$-isogenies on Kummer, either using theta functions (DMPR) or curve (Costello)

3

Advanced protocols on Kummers

The tools from Kummer arithmetic (1) and Kummer isogenies (2) allow us to do a single long $(2^n,2^n)$-isogeny. Can we build more tools, achieve SQIsign verification?

Goal: develop tools for point sampling, three point ladder, faster isogenies, to be able to do the full SQIsign verification only on Kummer surfaces.

$$K_0 \xrightarrow{\varphi_1} K_1 \xrightarrow{\varphi_2} \dots \xrightarrow{\varphi_{n-1}} K_n$$

Hope: use parallelisation from Kummer arithmetic to achieve fast(er?) verification.

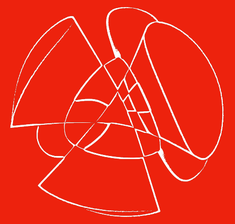
[1] J.W.S. Cassels and E.V. Flynn, *Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2,* Cambridge University Press, 1996.
[2] D.V Chudnovsky, G.V Chudnovsky, *Sequences of numbers generated by addition in formal groups and new primality and factorization tests,* Advances in Applied Mathematics, Volume 7, Issue 4, 1986.
[3] P. Gaudry. *Fast genus 2 arithmetic based on Theta functions*. J. Mathematical Cryptology, 1(3):243– 265, 2007.
[4] D. J. Bernstein. *Elliptic vs. Hyperelliptic, part I.* Talk at ECC (slides at http://cr.yp.to/talks/ 2006.09.20/slides.pdf), September 2006.
[5] D. J. Bernstein, C. Chuengsatiansup, T. Lange, and P. Schwabe. *Kummer strikes back: New DH speed records.* ASIACRYPT 2014.

Radboud University

[6] For works by Cosset, Lubicz, Robert: too many to name specific one... Good start is Robert's page: www.normalesup.org/~robert/
[7] C. Costello, *Computing supersingular isogenies on Kummer surfaces,* ASIACRYPT 2018
[8] P. Dartois, L. Maino, G. Pope, D. Robert, *An Algorithmic Approach to (2,2)-isogenies in the Theta Model and Applications to Isogeny-based Cryptography,* https://ia.cr/2023/1747

Return of the Kummer

✓



Kummer Surfaces

2

$$\begin{array}{ccc} \mathcal{J}_\alpha & \xrightarrow{\kappa} & \mathcal{J}_{\lambda,\mu,\nu} \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ \mathcal{K}_\alpha & \xrightarrow{\kappa^*} & \mathcal{K}_{\lambda,\mu,\nu} \end{array}$$

Kummers In Cryptography

3

$$\begin{array}{ccccc} 0 & \longrightarrow & E[n] & \longrightarrow & E \\ & & \downarrow{\scriptstyle [n]} & & \\ E & \longrightarrow & E/[n]E & \longrightarrow & 0 \end{array}$$

Pairings on Kummers

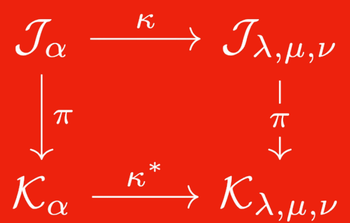
Running example: SQIsign verification using Kummers

$$\begin{array}{ccc} \mathcal{J}_\alpha & \xrightarrow{\kappa} & \mathcal{J}_{\lambda,\mu,\nu} \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ \mathcal{K}_\alpha & \xrightarrow{\kappa^*} & \mathcal{K}_{\lambda,\mu,\nu} \end{array}$$

Kummers in Cryptography

Scholten's construction

Any elliptic curve $E_\alpha/\mathbb{F}_{p^2}$ has a genus-2 friend $J_\alpha/\mathbb{F}_p$ which is $(2,2)$-isogenous, where $E_\alpha : y^2 = x(x-\alpha)(x-1/\alpha)$ with $\alpha = \alpha_0 + i \cdot \alpha_1 \in \mathbb{F}_{p^2}$



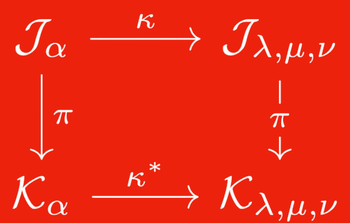
Kummers in Cryptography

Scholten's construction

Any elliptic curve $E_\alpha/\mathbb{F}_{p^2}$ has a genus-2 friend $J_\alpha/\mathbb{F}_p$ which is $(2,2)$-isogenous, where $E_\alpha : y^2 = x(x-\alpha)(x-1/\alpha)$ with $\alpha = \alpha_0 + i \cdot \alpha_1 \in \mathbb{F}_{p^2}$

ORIGINAL POINT-OF-VIEW

1. Take the *Weil restriction* $W_\alpha := W_{\mathbb{F}_p}^{\mathbb{F}_{p^2}}(E_\alpha)$
2. Construct a specific hyper ell. curve $C_\alpha : y^2 = f_0(x) \cdot f_1(x) \cdot f_2(x)$, with $f_i(x)$ derived from α_0, α_1
3. Then we can give a $(2,2)$-isogeny η between W_α and $J_\alpha := \mathrm{Jac}(C_\alpha)$ defined over $\mathbb{F}_p$



Kummers in Cryptography

Scholten's construction

Any elliptic curve $E_\alpha/\mathbb{F}_{p^2}$ has a genus-2 friend $J_\alpha/\mathbb{F}_p$ which is $(2,2)$-isogenous, where $E_\alpha : y^2 = x(x-\alpha)(x-1/\alpha)$ with $\alpha = \alpha_0 + i \cdot \alpha_1 \in \mathbb{F}_{p^2}$

ORIGINAL POINT-OF-VIEW

1. Take the *Weil restriction* $W_\alpha := W_{\mathbb{F}_p}^{\mathbb{F}_{p^2}}(E_\alpha)$
2. Construct a specific hyper ell. curve $C_\alpha : y^2 = f_0(x) \cdot f_1(x) \cdot f_2(x)$, with $f_i(x)$ derived from α_0, α_1
3. Then we can give a $(2,2)$-isogeny η between W_α and $J_\alpha := \mathrm{Jac}(C_\alpha)$ defined over $\mathbb{F}_p$

REPHRASED POINT-OF-VIEW

1. The Weil restriction is a specific *glueing*
2. Glue $E_\alpha \times E_\alpha^{(p)}$ along the right 2-torsion
3. This gives us $\eta' : E_\alpha \times E_\alpha^{(p)} \to J_\alpha$

$$\begin{array}{ccc} \mathcal{J}_\alpha & \xrightarrow{\kappa} & \mathcal{J}_{\lambda,\mu,\nu} \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ \mathcal{K}_\alpha & \xrightarrow{\kappa^*} & \mathcal{K}_{\lambda,\mu,\nu} \end{array}$$

Kummers in Cryptography

Scholten's construction

Any elliptic curve $E_\alpha/\mathbb{F}_{p^2}$ has a genus-2 friend $J_\alpha/\mathbb{F}_p$ which is $(2,2)$-isogenous, where $E_\alpha : y^2 = x(x-\alpha)(x-1/\alpha)$ with $\alpha = \alpha_0 + i \cdot \alpha_1 \in \mathbb{F}_{p^2}$

ORIGINAL POINT-OF-VIEW

1. Take the *Weil restriction* $W_\alpha := W_{\mathbb{F}_p}^{\mathbb{F}_{p^2}}(E_\alpha)$
2. Construct a specific hyper ell. curve $C_\alpha : y^2 = f_0(x) \cdot f_1(x) \cdot f_2(x)$, with $f_i(x)$ derived from α_0, α_1
3. Then we can give a $(2,2)$-isogeny η between W_α and $J_\alpha := \mathrm{Jac}(C_\alpha)$ defined over $\mathbb{F}_p$

REPHRASED POINT-OF-VIEW

1. The Weil restriction is a specific *glueing*
2. Glue $E_\alpha \times E_\alpha^{(p)}$ along the right 2-torsion
3. This gives us $\eta' : E_\alpha \times E_\alpha^{(p)} \to J_\alpha$

1 Take ell curve over $\mathbb{F}_{p^2}$ → E_α

$$\begin{array}{ccc} \mathcal{J}_\alpha & \xrightarrow{\kappa} & \mathcal{J}_{\lambda,\mu,\nu} \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ \mathcal{K}_\alpha & \xrightarrow{\kappa^*} & \mathcal{K}_{\lambda,\mu,\nu} \end{array}$$

Kummers in Cryptography

Scholten's construction

Any elliptic curve $E_\alpha/\mathbb{F}_{p^2}$ has a genus-2 friend $J_\alpha/\mathbb{F}_p$ which is $(2,2)$-isogenous, where $E_\alpha : y^2 = x(x-\alpha)(x-1/\alpha)$ with $\alpha = \alpha_0 + i \cdot \alpha_1 \in \mathbb{F}_{p^2}$

ORIGINAL POINT-OF-VIEW

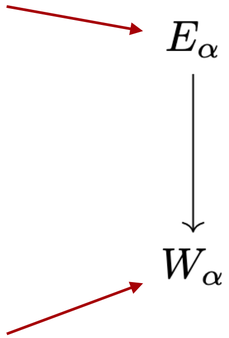
1. Take the *Weil restriction* $W_\alpha := W_{\mathbb{F}_p}^{\mathbb{F}_{p^2}}(E_\alpha)$
2. Construct a specific hyper ell. curve $C_\alpha : y^2 = f_0(x) \cdot f_1(x) \cdot f_2(x)$, with $f_i(x)$ derived from α_0, α_1
3. Then we can give a $(2,2)$-isogeny η between W_α and $J_\alpha := \mathrm{Jac}(C_\alpha)$ defined over $\mathbb{F}_p$

REPHRASED POINT-OF-VIEW

1. The Weil restriction is a specific *glueing*
2. Glue $E_\alpha \times E_\alpha^{(p)}$ along the right 2-torsion
3. This gives us $\eta' : E_\alpha \times E_\alpha^{(p)} \to J_\alpha$

1 Take ell curve over $\mathbb{F}_{p^2}$

2 Take Weil restriction over $\mathbb{F}_p$



2

$$\begin{array}{ccc} \mathcal{J}_\alpha & \xrightarrow{\kappa} & \mathcal{J}_{\lambda,\mu,\nu} \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ \mathcal{K}_\alpha & \xrightarrow{\kappa^*} & \mathcal{K}_{\lambda,\mu,\nu} \end{array}$$

Kummers in Cryptography

Scholten's construction

Any elliptic curve $E_\alpha/\mathbb{F}_{p^2}$ has a genus-2 friend $J_\alpha/\mathbb{F}_p$ which is $(2,2)$-isogenous, where $E_\alpha : y^2 = x(x-\alpha)(x-1/\alpha)$ with $\alpha = \alpha_0 + i \cdot \alpha_1 \in \mathbb{F}_{p^2}$

ORIGINAL POINT-OF-VIEW

1. Take the *Weil restriction* $W_\alpha := W_{\mathbb{F}_p}^{\mathbb{F}_{p^2}}(E_\alpha)$
2. Construct a specific hyper ell. curve $C_\alpha : y^2 = f_0(x) \cdot f_1(x) \cdot f_2(x)$, with $f_i(x)$ derived from α_0, α_1
3. Then we can give a $(2,2)$-isogeny η between W_α and $J_\alpha := \mathrm{Jac}(C_\alpha)$ defined over $\mathbb{F}_p$

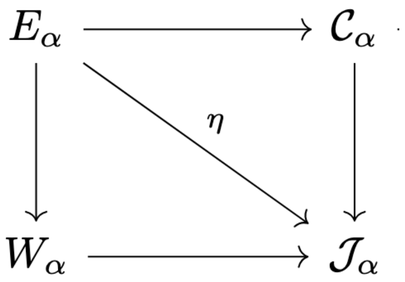
REPHRASED POINT-OF-VIEW

1. The Weil restriction is a specific *glueing*
2. Glue $E_\alpha \times E_\alpha^{(p)}$ along the right 2-torsion
3. This gives us $\eta' : E_\alpha \times E_\alpha^{(p)} \to J_\alpha$

1 Take ell curve over $\mathbb{F}_{p^2}$

2 Take Weil restriction over $\mathbb{F}_p$

3 Re-order restricted roots



2

$$\begin{array}{ccc} \mathcal{J}_\alpha & \xrightarrow{\kappa} & \mathcal{J}_{\lambda,\mu,\nu} \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ \mathcal{K}_\alpha & \xrightarrow{\kappa^*} & \mathcal{K}_{\lambda,\mu,\nu} \end{array}$$

Kummers in Cryptography

Scholten's construction

Any elliptic curve $E_\alpha/\mathbb{F}_{p^2}$ has a genus-2 friend $J_\alpha/\mathbb{F}_p$ which is $(2,2)$-isogenous, where $E_\alpha : y^2 = x(x-\alpha)(x-1/\alpha)$ with $\alpha = \alpha_0 + i \cdot \alpha_1 \in \mathbb{F}_{p^2}$

ORIGINAL POINT-OF-VIEW

1. Take the *Weil restriction* $W_\alpha := W_{\mathbb{F}_p}^{\mathbb{F}_{p^2}}(E_\alpha)$
2. Construct a specific hyper ell. curve $C_\alpha : y^2 = f_0(x) \cdot f_1(x) \cdot f_2(x)$, with $f_i(x)$ derived from α_0, α_1
3. Then we can give a $(2,2)$-isogeny η between W_α and $J_\alpha := \mathrm{Jac}(C_\alpha)$ defined over $\mathbb{F}_p$

REPHRASED POINT-OF-VIEW

1. The Weil restriction is a specific *glueing*
2. Glue $E_\alpha \times E_\alpha^{(p)}$ along the right 2-torsion
3. This gives us $\eta' : E_\alpha \times E_\alpha^{(p)} \to J_\alpha$

1 Take ell curve over $\mathbb{F}_{p^2}$

2 Take Weil restriction over $\mathbb{F}_p$

3 Re-order restricted roots

4 Map to Rosenhain

$$\begin{array}{ccccc} E_\alpha & & \longrightarrow & \mathcal{C}_\alpha & \xrightarrow{\kappa} & \mathcal{C}_{\lambda,\mu,\nu} \\ \downarrow & \searrow^{\eta} & & \downarrow & & \downarrow \\ W_\alpha & & \longrightarrow & \mathcal{J}_\alpha & \xrightarrow{\kappa^*} & \mathcal{J}_{\lambda,\mu,\nu} \end{array}$$

2

$$\begin{array}{ccc} \mathcal{J}_\alpha & \xrightarrow{\kappa} & \mathcal{J}_{\lambda,\mu,\nu} \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ \mathcal{K}_\alpha & \xrightarrow{\kappa^*} & \mathcal{K}_{\lambda,\mu,\nu} \end{array}$$

Kummers in Cryptography

Scholten's construction

Any elliptic curve $E_\alpha/\mathbb{F}_{p^2}$ has a genus-2 friend $J_\alpha/\mathbb{F}_p$ which is (2,2)-isogenous, where $E_\alpha : y^2 = x(x-\alpha)(x-1/\alpha)$ with $\alpha = \alpha_0 + i \cdot \alpha_1 \in \mathbb{F}_{p^2}$

ORIGINAL POINT-OF-VIEW

1. Take the *Weil restriction* $W_\alpha := W_{\mathbb{F}_p}^{\mathbb{F}_{p^2}}(E_\alpha)$
2. Construct a specific hyper ell. curve $C_\alpha : y^2 = f_0(x) \cdot f_1(x) \cdot f_2(x)$, with $f_i(x)$ derived from α_0, α_1
3. Then we can give a (2,2)-isogeny η between W_α and $J_\alpha := \mathrm{Jac}(C_\alpha)$ defined over $\mathbb{F}_p$

REPHRASED POINT-OF-VIEW

1. The Weil restriction is a specific *glueing*
2. Glue $E_\alpha \times E_\alpha^{(p)}$ along the right 2-torsion
3. This gives us $\eta' : E_\alpha \times E_\alpha^{(p)} \to J_\alpha$

1 Take ell curve over $\mathbb{F}_{p^2}$

2 Take Weil restriction over $\mathbb{F}_p$

3 Re-order restricted roots

4 Map to Rosenhain

5 Go to squared Kummer

$$\begin{array}{ccccccc} E_\alpha & & \longrightarrow & & \mathcal{C}_\alpha & \xrightarrow{\kappa} & \mathcal{C}_{\lambda,\mu,\nu} \\ & \searrow^{\eta} & & & & & \\ W_\alpha & & \longrightarrow & & \mathcal{J}_\alpha & \xrightarrow{\kappa^*} & \mathcal{J}_{\lambda,\mu,\nu} \\ & & & & \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ & & & & \mathcal{K}_\alpha^{\mathrm{gen}} & \xrightarrow{\kappa^{**}} & \mathcal{K}_{\lambda,\mu,\nu}^{\mathrm{gen}} \xrightarrow{M} \mathcal{K}_{\lambda,\mu,\nu}^{\mathrm{Sqr}} \end{array}$$

$$\begin{array}{ccc} \mathcal{J}_\alpha & \xrightarrow{\kappa} & \mathcal{J}_{\lambda,\mu,\nu} \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ \mathcal{K}_\alpha & \xrightarrow{\kappa^*} & \mathcal{K}_{\lambda,\mu,\nu} \end{array}$$

Kummers in Cryptography

Scholten's construction

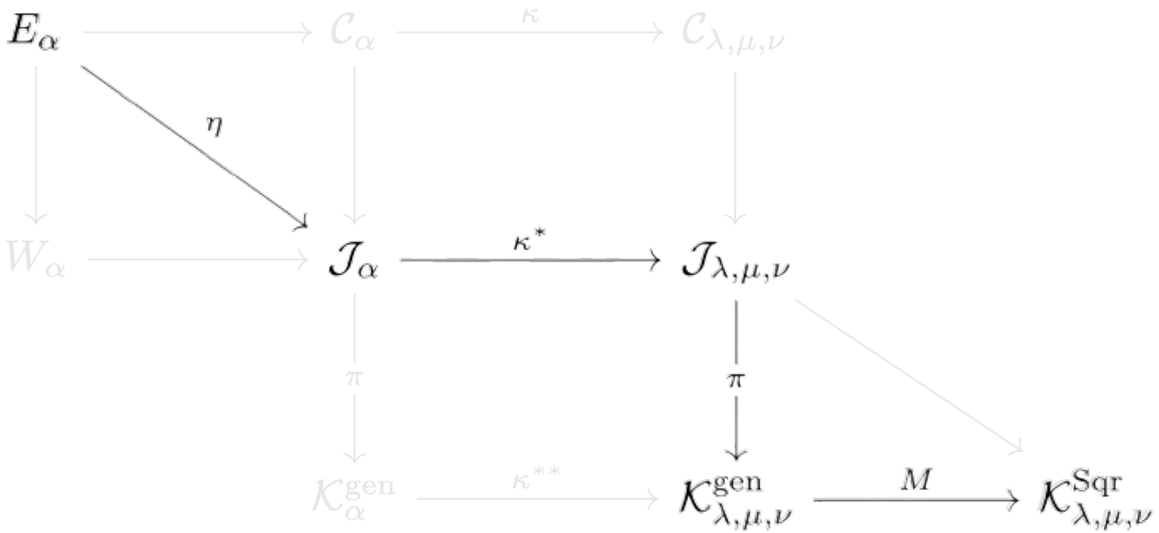
Any elliptic curve $E_\alpha/\mathbb{F}_{p^2}$ has a genus-2 friend $J_\alpha/\mathbb{F}_p$ which is $(2,2)$-isogenous, where $E_\alpha : y^2 = x(x-\alpha)(x-1/\alpha)$ with $\alpha = \alpha_0 + i \cdot \alpha_1 \in \mathbb{F}_{p^2}$

ORIGINAL POINT-OF-VIEW

1. Take the *Weil restriction* $W_\alpha := W_{\mathbb{F}_p}^{\mathbb{F}_{p^2}}(E_\alpha)$
2. Construct a specific hyper ell. curve $C_\alpha : y^2 = f_0(x) \cdot f_1(x) \cdot f_2(x)$, with $f_i(x)$ derived from α_0, α_1
3. Then we can give a $(2,2)$-isogeny η between W_α and $J_\alpha := \mathrm{Jac}(C_\alpha)$ defined over $\mathbb{F}_p$

REPHRASED POINT-OF-VIEW

1. The Weil restriction is a specific *glueing*
2. Glue $E_\alpha \times E_\alpha^{(p)}$ along the right 2-torsion
3. This gives us $\eta' : E_\alpha \times E_\alpha^{(p)} \to J_\alpha$



$$\begin{array}{ccc} \mathcal{J}_\alpha & \xrightarrow{\kappa} & \mathcal{J}_{\lambda,\mu,\nu} \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ \mathcal{K}_\alpha & \xrightarrow{\kappa^*} & \mathcal{K}_{\lambda,\mu,\nu} \end{array}$$

Kummers in Cryptography

Scholten's construction

Any elliptic curve $E_\alpha/\mathbb{F}_{p^2}$ has a genus-2 friend $J_\alpha/\mathbb{F}_p$ which is $(2,2)$-isogenous, where $E_\alpha : y^2 = x(x-\alpha)(x-1/\alpha)$ with $\alpha = \alpha_0 + i \cdot \alpha_1 \in \mathbb{F}_{p^2}$

ORIGINAL POINT-OF-VIEW

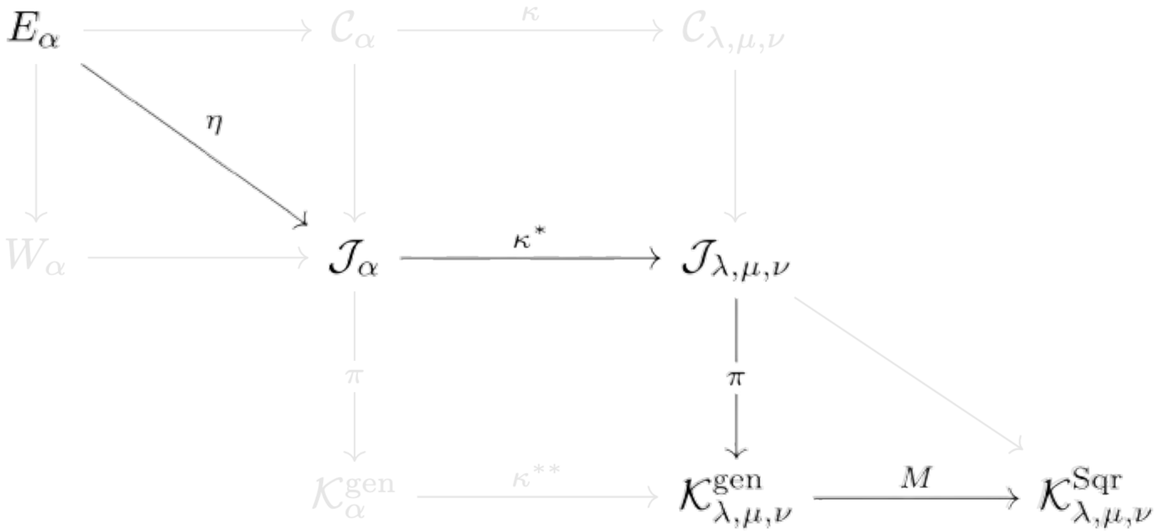
1. Take the *Weil restriction* $W_\alpha := W_{\mathbb{F}_p}^{\mathbb{F}_{p^2}}(E_\alpha)$
2. Construct a specific hyper ell. curve $C_\alpha : y^2 = f_0(x) \cdot f_1(x) \cdot f_2(x)$, with $f_i(x)$ derived from α_0, α_1
3. Then we can give a $(2,2)$-isogeny η between W_α and $J_\alpha := \mathrm{Jac}(C_\alpha)$ defined over $\mathbb{F}_p$

REPHRASED POINT-OF-VIEW

1. The Weil restriction is a specific *glueing*
2. Glue $E_\alpha \times E_\alpha^{(p)}$ along the right 2-torsion
3. This gives us $\eta' : E_\alpha \times E_\alpha^{(p)} \to J_\alpha$

!

For remaining slides, ignore most of this



$$\begin{array}{ccc} \mathcal{J}_\alpha & \xrightarrow{\kappa} & \mathcal{J}_{\lambda,\mu,\nu} \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ \mathcal{K}_\alpha & \xrightarrow{\kappa^*} & \mathcal{K}_{\lambda,\mu,\nu} \end{array}$$

Kummers in Cryptography

Scholten's construction

Any elliptic curve $E_\alpha/\mathbb{F}_{p^2}$ has a genus-2 friend $J_\alpha/\mathbb{F}_p$ which is $(2,2)$-isogenous, where $E_\alpha : y^2 = x(x-\alpha)(x-1/\alpha)$ with $\alpha = \alpha_0 + i \cdot \alpha_1 \in \mathbb{F}_{p^2}$

ORIGINAL POINT-OF-VIEW

1. Take the *Weil restriction* $W_\alpha := W_{\mathbb{F}_p}^{\mathbb{F}_{p^2}}(E_\alpha)$
2. Construct a specific hyper ell. curve $C_\alpha : y^2 = f_0(x) \cdot f_1(x) \cdot f_2(x)$, with $f_i(x)$ derived from α_0, α_1
3. Then we can give a $(2,2)$-isogeny η between W_α and $J_\alpha := \mathrm{Jac}(C_\alpha)$ defined over $\mathbb{F}_p$

REPHRASED POINT-OF-VIEW

1. The Weil restriction is a specific *glueing*
2. Glue $E_\alpha \times E_\alpha^{(p)}$ along the right 2-torsion
3. This gives us $\eta' : E_\alpha \times E_\alpha^{(p)} \to J_\alpha$

!

Just think of $E_\alpha \to K_\alpha$

$$E_\alpha \xrightarrow{\zeta := M \circ \pi \circ \kappa^* \circ \eta} \mathcal{K}_\alpha := \mathcal{K}_{\lambda,\mu,\nu}^{\mathrm{Sqr}}$$

!

For remaining slides, ignore most of this

$$\begin{array}{ccc} \mathcal{J}_\alpha & \xrightarrow{\kappa} & \mathcal{J}_{\lambda,\mu,\nu} \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ \mathcal{K}_\alpha & \xrightarrow{\kappa^*} & \mathcal{K}_{\lambda,\mu,\nu} \end{array}$$

Kummers in Cryptography

Costello's SIDH on Kummer

Any elliptic curve $E_\alpha/\mathbb{F}_{p^2}$ has a $(2,2)$-isogenous Kummer friend $K_\alpha/\mathbb{F}_p$

- The curve E_α has three 2-isogenies, defined either by $P_0, P_\alpha, P_{1/\alpha}$
- The Kummer K_α has corresponding $(2,2)$-isogenies
- By magic, these $(2,2)$'s can be described by single points $P'_0, P'_\alpha, P'_{1/\alpha}$ instead of subgroups!
- Thus, given a point of order 2^n on $K_{\alpha'}$ we can do a $(2^n,2^n)$-isogeny on the Kummers

1 Point P of order 2^{n+2}

E_α, P

$$\begin{array}{ccc} \mathcal{J}_\alpha & \xrightarrow{\kappa} & \mathcal{J}_{\lambda,\mu,\nu} \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ \mathcal{K}_\alpha & \xrightarrow{\kappa^*} & \mathcal{K}_{\lambda,\mu,\nu} \end{array}$$

Kummers in Cryptography

Costello's SIDH on Kummer

Any elliptic curve $E_\alpha/\mathbb{F}_{p^2}$ has a $(2,2)$-isogenous Kummer friend $K_\alpha/\mathbb{F}_p$

- The curve E_α has three 2-isogenies, defined either by $P_0, P_\alpha, P_{1/\alpha}$
- The Kummer K_α has corresponding $(2,2)$-isogenies
- By magic, these $(2,2)$'s can be described by single points $P'_0, P'_\alpha, P'_{1/\alpha}$ instead of subgroups!
- Thus, given a point of order 2^n on $K_{\alpha'}$ we can do a $(2^n,2^n)$-isogeny on the Kummers

1 Point P of order 2^{n+2}

2 maps to $\zeta(P)$ of order 2^{n+1}

$$\begin{array}{c} E_\alpha, P \\ \downarrow{\scriptstyle \zeta} \\ \mathcal{K}_\alpha, \zeta(P) \end{array}$$

$$\begin{array}{ccc} \mathcal{J}_\alpha & \xrightarrow{\kappa} & \mathcal{J}_{\lambda,\mu,\nu} \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ \mathcal{K}_\alpha & \xrightarrow{\kappa^*} & \mathcal{K}_{\lambda,\mu,\nu} \end{array}$$

Kummers in Cryptography

Costello's SIDH on Kummer

Any elliptic curve $E_\alpha/\mathbb{F}_{p^2}$ has a $(2,2)$-isogenous Kummer friend $K_\alpha/\mathbb{F}_p$

- The curve E_α has three 2-isogenies, defined either by $P_0, P_\alpha, P_{1/\alpha}$
- The Kummer K_α has corresponding $(2,2)$-isogenies
- By magic, these $(2,2)$'s can be described by single points $P'_0, P'_\alpha, P'_{1/\alpha}$ instead of subgroups!
- Thus, given a point of order 2^n on $K_{\alpha'}$ we can do a $(2^n,2^n)$-isogeny on the Kummers

1 Point P of order 2^{n+2}

2 maps to $\zeta(P)$ of order 2^{n+1}

$$\begin{array}{ccc} E_\alpha, P & & \\ \downarrow{\scriptstyle \zeta} & & \\ \mathcal{K}_\alpha, \zeta(P) & \xrightarrow{\varphi'} & \mathcal{K}_\alpha/\langle 2\zeta(P)\rangle \end{array}$$

3 gives a $(2^n,2^n)$-isogeny on Kummers

$$\begin{array}{ccc} \mathcal{J}_\alpha & \xrightarrow{\kappa} & \mathcal{J}_{\lambda,\mu,\nu} \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ \mathcal{K}_\alpha & \xrightarrow{\kappa^*} & \mathcal{K}_{\lambda,\mu,\nu} \end{array}$$

Kummers in Cryptography

Costello's SIDH on Kummer

Any elliptic curve $E_\alpha/\mathbb{F}_{p^2}$ has a $(2,2)$-isogenous Kummer friend $K_\alpha/\mathbb{F}_p$

- The curve E_α has three 2-isogenies, defined either by $P_0, P_\alpha, P_{1/\alpha}$
- The Kummer K_α has corresponding $(2,2)$-isogenies
- By magic, these $(2,2)$'s can be described by single points $P'_0, P'_\alpha, P'_{1/\alpha}$ instead of subgroups!
- Thus, given a point of order 2^n on $K_{\alpha'}$ we can do a $(2^n,2^n)$-isogeny on the Kummers

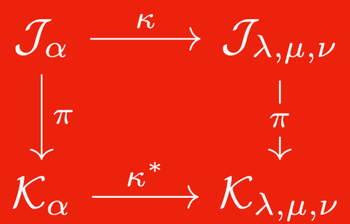
1 Point P of order 2^{n+2}

2 maps to $\zeta(P)$ of order 2^{n+1}

$$\begin{array}{ccc} E_\alpha, P & \xrightarrow{\varphi} & E_\alpha/\langle\langle 4P\rangle\rangle \\ \downarrow{\scriptstyle \zeta} & & \downarrow{\scriptstyle \zeta'} \\ \mathcal{K}_\alpha, \zeta(P) & \xrightarrow{\varphi'} & \mathcal{K}_\alpha/\langle 2\zeta(P)\rangle \end{array}$$

3 gives a $(2^n,2^n)$-isogeny on Kummers

4 which matches up with isogeny generated by $4P$



Kummers in Cryptography

SQIsign on Kummers?

Any elliptic curve $E_\alpha/\mathbb{F}_{p^2}$ has a (2,2)-isogenous Kummer friend $K_\alpha/\mathbb{F}_p$

- Costello gives us the tools to translate $\varphi : E_\alpha \to E'_\alpha$ to Kummer isogeny $\varphi' : K_\alpha \to K'_\alpha$
- Can we then translate SQIsign isogenies $\sigma : E_A \to E_2$ of degree 2^{1000} to Kummers?
- First, try *uncompressed* signatures
- Then, see if we have enough tools to compress signatures

$$\begin{array}{ccc} \mathcal{J}_\alpha & \xrightarrow{\kappa} & \mathcal{J}_{\lambda,\mu,\nu} \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ \mathcal{K}_\alpha & \xrightarrow{\kappa^*} & \mathcal{K}_{\lambda,\mu,\nu} \end{array}$$

Kummers in Cryptography

SQIsign on Kummers?

Any elliptic curve $E_\alpha/\mathbb{F}_{p^2}$ has a (2,2)-isogenous Kummer friend $K_\alpha/\mathbb{F}_p$

- Costello gives us the tools to translate $\varphi : E_\alpha \to E'_\alpha$ to Kummer isogeny $\varphi' : K_\alpha \to K'_\alpha$
- Can we then translate SQIsign isogenies $\sigma : E_A \to E_2$ of degree 2^{1000} to Kummers?
- First, try *uncompressed* signatures
- Then, see if we have enough tools to compress signatures

1 SQIsign signature

$$E_0 \xrightarrow{\sigma_1} E_1 \xrightarrow{\sigma_2} \cdots \xrightarrow{\sigma_n} E_n$$

$$\begin{array}{ccc} \mathcal{J}_\alpha & \xrightarrow{\kappa} & \mathcal{J}_{\lambda,\mu,\nu} \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ \mathcal{K}_\alpha & \xrightarrow{\kappa^*} & \mathcal{K}_{\lambda,\mu,\nu} \end{array}$$

Kummers in Cryptography

SQIsign on Kummers?

Any elliptic curve $E_\alpha/\mathbb{F}_{p^2}$ has a (2,2)-isogenous Kummer friend $K_\alpha/\mathbb{F}_p$

- Costello gives us the tools to translate $\varphi : E_\alpha \to E'_\alpha$ to Kummer isogeny $\varphi' : K_\alpha \to K'_\alpha$
- Can we then translate SQIsign isogenies $\sigma : E_A \to E_2$ of degree 2^{1000} to Kummers?
- First, try *uncompressed* signatures
- Then, see if we have enough tools to compress signatures

1 SQIsign signature

2 Map down starting curve

$$\begin{array}{ccccccc} E_0 & \xrightarrow{\sigma_1} & E_1 & \xrightarrow{\sigma_2} & \cdots & \xrightarrow{\sigma_n} & E_n \\ \downarrow{\scriptstyle \zeta_0} & & & & & & \\ K_0^{\mathrm{Sqr}} & & & & & & \end{array}$$

$$\begin{array}{ccc} \mathcal{J}_\alpha & \xrightarrow{\kappa} & \mathcal{J}_{\lambda,\mu,\nu} \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ \mathcal{K}_\alpha & \xrightarrow{\kappa^*} & \mathcal{K}_{\lambda,\mu,\nu} \end{array}$$

Kummers in Cryptography

SQIsign on Kummers?

Any elliptic curve $E_\alpha/\mathbb{F}_{p^2}$ has a (2,2)-isogenous Kummer friend $K_\alpha/\mathbb{F}_p$

- Costello gives us the tools to translate $\varphi : E_\alpha \to E'_\alpha$ to Kummer isogeny $\varphi' : K_\alpha \to K'_\alpha$
- Can we then translate SQIsign isogenies $\sigma : E_A \to E_2$ of degree 2^{1000} to Kummers?
- First, try *uncompressed* signatures
- Then, see if we have enough tools to compress signatures

1 SQIsign signature

2 Map down starting curve

$$\begin{array}{ccccccc} E_0 & \xrightarrow{\sigma_1} & E_1 & \xrightarrow{\sigma_2} & \cdots & \xrightarrow{\sigma_n} & E_n \\ \downarrow{\scriptstyle \zeta_0} & & & & & & \downarrow{\scriptstyle \zeta_n} \\ K_0^{\mathrm{Sqr}} & \xrightarrow{\sigma'_1} & K_1^{\mathrm{Sqr}} & \xrightarrow{\sigma'_2} & \cdots & \xrightarrow{\sigma'_n} & K_n^{\mathrm{Sqr}} \end{array}$$

3 Generate the right kernel points on K_i

$$\begin{array}{ccc} \mathcal{J}_\alpha & \xrightarrow{\kappa} & \mathcal{J}_{\lambda,\mu,\nu} \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ \mathcal{K}_\alpha & \xrightarrow{\kappa^*} & \mathcal{K}_{\lambda,\mu,\nu} \end{array}$$

Kummers in Cryptography

SQIsign on Kummers?

Any elliptic curve $E_\alpha/\mathbb{F}_{p^2}$ has a (2,2)-isogenous Kummer friend $K_\alpha/\mathbb{F}_p$

- Costello gives us the tools to translate $\varphi : E_\alpha \to E'_\alpha$ to Kummer isogeny $\varphi' : K_\alpha \to K'_\alpha$
- Can we then translate SQIsign isogenies $\sigma : E_A \to E_2$ of degree 2^{1000} to Kummers?
- First, try *uncompressed* signatures
- Then, see if we have enough tools to compress signatures

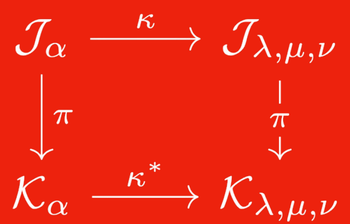
1 SQIsign signature

2 Map down starting curve

$$\begin{array}{ccccccccc} E_0 & \xrightarrow{\sigma_1} & E_1 & \xrightarrow{\sigma_2} & \cdots & \xrightarrow{\sigma_n} & E_n \\ \downarrow{\scriptstyle \zeta_0} & & & & & & \downarrow{\scriptstyle \zeta_n} \\ K_0^{\mathrm{Sqr}} & \xrightarrow{\sigma'_1} & K_1^{\mathrm{Sqr}} & \xrightarrow{\sigma'_2} & \cdots & \xrightarrow{\sigma'_n} & K_n^{\mathrm{Sqr}} \end{array}$$

3 Generate the right kernel points on K_i

4 SQIsign on Kummers!



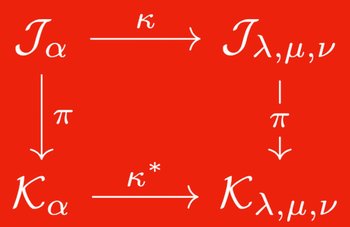
Kummers in Cryptography

Compressed SQIsign

Elliptic Curves

- instead of $\varphi : E \to E'$ given by kernel $R \in E[2^f]$
- find deterministic basis P, Q of $E[2^f]$
- then find $s \in [1..2^f]$ such that $\langle R \rangle = \langle P + sQ \rangle$
- then φ is compressed to s, which takes f bits

  from R, which takes $2 \log p$ bits



Kummers in Cryptography

Compressed SQIsign

Elliptic Curves

- instead of $\varphi : E \to E'$ given by kernel $R \in E[2^f]$
- find deterministic basis P, Q of $E[2^f]$
- then find $s \in [1..2^f]$ such that $\langle R \rangle = \langle P + sQ \rangle$
- then φ is compressed to s, which takes f bits from R, which takes $2 \log p$ bits

Kummer Surfaces

- instead of $\varphi : K \to K'$ given by kernel $R \in K[2^f]$
- find deterministic basis of K ?
- can we express R simply in these terms?
- we are missing many **essential** tools to do these protocols on Kummer surfaces!

2

$$\begin{array}{ccc} \mathcal{J}_\alpha & \xrightarrow{\kappa} & \mathcal{J}_{\lambda,\mu,\nu} \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ \mathcal{K}_\alpha & \xrightarrow{\kappa^*} & \mathcal{K}_{\lambda,\mu,\nu} \end{array}$$

Kummers in Cryptography

Compressed SQIsign

Elliptic Curves

- instead of $\varphi : E \to E'$ given by kernel $R \in E[2^f]$
- find deterministic basis P, Q of $E[2^f]$
- then find $s \in [1..2^f]$ such that $\langle R \rangle = \langle P + sQ \rangle$
- then φ is compressed to s, which takes f bits from R, which takes $2 \log p$ bits

Kummer Surfaces

- instead of $\varphi : K \to K'$ given by kernel $R \in K[2^f]$
- find deterministic basis of K ?
- can we express R simply in these terms?
- we are missing many **essential** tools to do these protocols on Kummer surfaces!

1

CheckOrigin
given $P \in K$, is origin $J(\mathbb{F}_p)$ or $J^T(\mathbb{F}_p)$?

2

$$\begin{array}{ccc} \mathcal{J}_\alpha & \xrightarrow{\kappa} & \mathcal{J}_{\lambda,\mu,\nu} \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ \mathcal{K}_\alpha & \xrightarrow{\kappa^*} & \mathcal{K}_{\lambda,\mu,\nu} \end{array}$$

Kummers in Cryptography

Compressed SQIsign

Elliptic Curves

- instead of $\varphi : E \to E'$ given by kernel $R \in E[2^f]$
- find deterministic basis P, Q of $E[2^f]$
- then find $s \in [1..2^f]$ such that $\langle R \rangle = \langle P + sQ \rangle$
- then φ is compressed to s, which takes f bits from R, which takes $2 \log p$ bits

Kummer Surfaces

- instead of $\varphi : K \to K'$ given by kernel $R \in K[2^f]$
- find deterministic basis of K ?
- can we express R simply in these terms?
- we are missing many **essential** tools to do these protocols on Kummer surfaces!

1

CheckOrigin
given $P \in K$, is origin $J(\mathbb{F}_p)$ or $J^T(\mathbb{F}_p)$?

2

PointDiff
given $P, Q \in K$, compute $P - Q \in K$

2

$$\begin{array}{ccc} \mathcal{J}_\alpha & \xrightarrow{\kappa} & \mathcal{J}_{\lambda,\mu,\nu} \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ \mathcal{K}_\alpha & \xrightarrow{\kappa^*} & \mathcal{K}_{\lambda,\mu,\nu} \end{array}$$

Kummers in Cryptography

Compressed SQIsign

Elliptic Curves

- instead of $\varphi : E \to E'$ given by kernel $R \in E[2^f]$
- find deterministic basis P, Q of $E[2^f]$
- then find $s \in [1..2^f]$ such that $\langle R \rangle = \langle P + sQ \rangle$
- then φ is compressed to s, which takes f bits from R, which takes $2 \log p$ bits

Kummer Surfaces

- instead of $\varphi : K \to K'$ given by kernel $R \in K[2^f]$
- find deterministic basis of K ?
- can we express R simply in these terms?
- we are missing many **essential** tools to do these protocols on Kummer surfaces!

1 **CheckOrigin**
given $P \in K$, is origin $J(\mathbb{F}_p)$ or $J^T(\mathbb{F}_p)$?

2 **PointDiff**
given $P, Q \in K$, compute $P - Q \in K$

3 **Sample 2^f-torsion**
given K, find points with 2^f-torsion

2

$$\begin{array}{ccc} \mathcal{J}_\alpha & \xrightarrow{\kappa} & \mathcal{J}_{\lambda,\mu,\nu} \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ \mathcal{K}_\alpha & \xrightarrow{\kappa^*} & \mathcal{K}_{\lambda,\mu,\nu} \end{array}$$

Kummers in Cryptography

Compressed SQIsign

Elliptic Curves

- instead of $\varphi : E \to E'$ given by kernel $R \in E[2^f]$
- find deterministic basis P, Q of $E[2^f]$
- then find $s \in [1..2^f]$ such that $\langle R \rangle = \langle P + sQ \rangle$
- then φ is compressed to s, which takes f bits from R, which takes $2 \log p$ bits

Kummer Surfaces

- instead of $\varphi : K \to K'$ given by kernel $R \in K[2^f]$
- find deterministic basis of K ?
- can we express R simply in these terms?
- we are missing many **essential** tools to do these protocols on Kummer surfaces!

1 **CheckOrigin**
given $P \in K$, is origin $J(\mathbb{F}_p)$ or $J^T(\mathbb{F}_p)$?

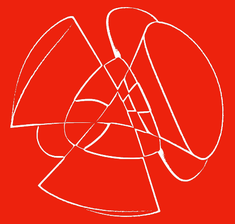
2 **PointDiff**
given $P, Q \in K$, compute $P - Q \in K$

3 **Sample 2^f-torsion**
given K, find points with 2^f-torsion

we need to talk about **pairings**

Return of the Kummer

✓



Kummer Surfaces

✓

$$\begin{array}{ccc} \mathcal{J}_\alpha & \xrightarrow{\kappa} & \mathcal{J}_{\lambda,\mu,\nu} \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ \mathcal{K}_\alpha & \xrightarrow{\kappa^*} & \mathcal{K}_{\lambda,\mu,\nu} \end{array}$$

Kummers In Cryptography

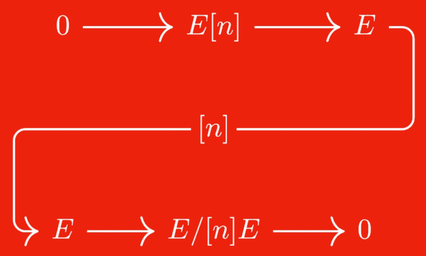
3

$$\begin{array}{ccccc} 0 & \longrightarrow & E[n] & \longrightarrow & E \\ & & & & \downarrow{\scriptstyle [n]} \\ E & \longrightarrow & E/[n]E & \longrightarrow & 0 \end{array}$$

Pairings on Kummers

Pairings (on Kummers)

3



Pairings on Kummers

genus 1 example

Let $E : y^2 = x^3 + Ax^2 + x$ be a supersingular curve over $\mathbb{F}_{p^2}$, with $E(\mathbb{F}_{p^2}) \cong \mathbb{Z}_{p+1} \times \mathbb{Z}_{p+1}$ for $p = 2^a \cdot 3^b - 1$.

1 Fun facts for elliptic curve friends

2 Decompose cokernel using pairings

3 Higher genus fun facts for Jacobian friends

3

$$0 \longrightarrow E[n] \longrightarrow E \xrightarrow{[n]} E \longrightarrow E/[n]E \longrightarrow 0$$

Pairings on Kummers

genus 1 example

Let $E : y^2 = x^3 + Ax^2 + x$ be a supersingular curve over $\mathbb{F}_{p^2}$, with $E(\mathbb{F}_{p^2}) \cong \mathbb{Z}_{p+1} \times \mathbb{Z}_{p+1}$ for $p = 2^a \cdot 3^b - 1$.

fun fact

To find $P \in E(\mathbb{F}_{p^2})$ with ``full 2^a-torsion'':

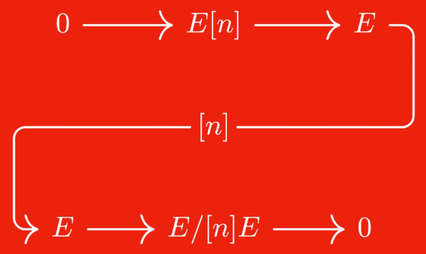
It is enough to find $P \in E(\mathbb{F}_{p^2})$ with x_P **non-square**

1 Fun facts for elliptic curve friends

2 Decompose cokernel using pairings

3 Higher genus fun facts for Jacobian friends

3



Pairings on Kummers

genus 1 example

Let $E : y^2 = x^3 + Ax^2 + x$ be a supersingular curve over $\mathbb{F}_{p^2}$, with $E(\mathbb{F}_{p^2}) \cong \mathbb{Z}_{p+1} \times \mathbb{Z}_{p+1}$ for $p = 2^a \cdot 3^b - 1$.

fun fact

To find $P \in E(\mathbb{F}_{p^2})$ with ``full 2^a-torsion'':

It is enough to find $P \in E(\mathbb{F}_{p^2})$ with x_P **non-square**

why? →

theorem

The image $[2]E$ is given by all points $(x, y) \in E(\mathbb{F}_{p^2})$ with

$x, x - \alpha, x - \frac{1}{\alpha}$ square

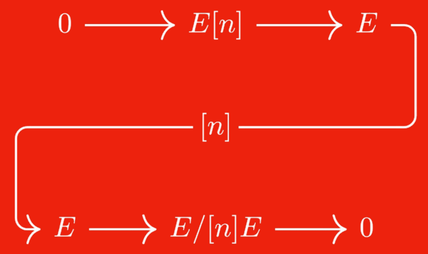
with α root of $x^2 + Ax + 1$

1 Fun facts for elliptic curve friends

2 Decompose cokernel using pairings

3 Higher genus fun facts for Jacobian friends

3



Pairings on Kummers

genus 1 example

Let $E : y^2 = x^3 + Ax^2 + x$ be a supersingular curve over $\mathbb{F}_{p^2}$, with $E(\mathbb{F}_{p^2}) \cong \mathbb{Z}_{p+1} \times \mathbb{Z}_{p+1}$ for $p = 2^a \cdot 3^b - 1$.

fun fact

To find $P \in E(\mathbb{F}_{p^2})$ with ``full 2^a-torsion'':

It is enough to find $P \in E(\mathbb{F}_{p^2})$ with x_P **non-square**

why? →

theorem

The image $[2]E$ is given by all points $(x, y) \in E(\mathbb{F}_{p^2})$ with

$x, x - \alpha, x - \frac{1}{\alpha}$ square

with α root of $x^2 + Ax + 1$

why? →

intuition

The image $[2]E$ is naturally linked to the level 2 red. Tate pairing.

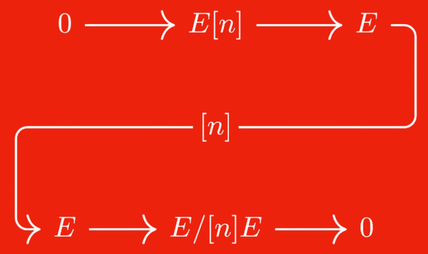
$P \in [2]E \Leftrightarrow t_2(L_i, P) = 1$ for $L_i \in E[2]$

1 Fun facts for elliptic curve friends

2 Decompose cokernel using pairings

3 Higher genus fun facts for Jacobian friends

3



Pairings on Kummers

genus 1 example

Let $E : y^2 = x^3 + Ax^2 + x$ be a supersingular curve over $\mathbb{F}_{p^2}$, with $E(\mathbb{F}_{p^2}) \cong \mathbb{Z}_{p+1} \times \mathbb{Z}_{p+1}$ for $p = 2^a \cdot 3^b - 1$.

fun fact

To find $P \in E(\mathbb{F}_{p^2})$ with ``full 2^a-torsion'':

It is enough to find $P \in E(\mathbb{F}_{p^2})$ with x_P **non-square**

why? →

theorem

The image $[2]E$ is given by all points $(x, y) \in E(\mathbb{F}_{p^2})$ with

$x, x - \alpha, x - \frac{1}{\alpha}$ square with α root of $x^2 + Ax + 1$

why? →

intuition

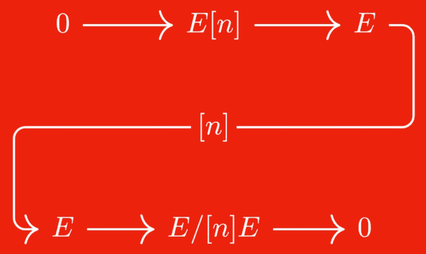
The image $[2]E$ is naturally linked to the level 2 red. Tate pairing.

$P \in [2]E \Leftrightarrow t_2(L_i, P) = 1$ for $L_i \in E[2]$

1. Fun facts for elliptic curve friends
2. Decompose cokernel using pairings
3. Higher genus fun facts for Jacobian friends

$$t_2 : \quad E(\mathbb{F}_{p^2})[2] \quad \times \quad E(\mathbb{F}_{p^2})/[2]E(\mathbb{F}_{p^2}) \longrightarrow \mu_2$$

3



Pairings on Kummers

genus 1 example

Let $E : y^2 = x^3 + Ax^2 + x$ be a supersingular curve over $\mathbb{F}_{p^2}$, with $E(\mathbb{F}_{p^2}) \cong \mathbb{Z}_{p+1} \times \mathbb{Z}_{p+1}$ for $p = 2^a \cdot 3^b - 1$.

fun fact

To find $P \in E(\mathbb{F}_{p^2})$ with ``full 2^a-torsion'':

It is enough to find $P \in E(\mathbb{F}_{p^2})$ with x_P **non-square**

why? →

theorem

The image $[2]E$ is given by all points $(x, y) \in E(\mathbb{F}_{p^2})$ with

$x, x - \alpha, x - \frac{1}{\alpha}$ square

with α root of $x^2 + Ax + 1$

why? →

intuition

The image $[2]E$ is naturally linked to the level 2 red. Tate pairing.

$P \in [2]E \Leftrightarrow t_2(L_i, P) = 1$ for $L_i \in E[2]$

MISTAKE 1

DON'T: think of this as $E(\mathbb{F}_{p^2})$ or $E(\mathbb{F}_{p^2})[2]$

DO: think of this as cosets, $P + [2]E(\mathbb{F}_{p^2})$

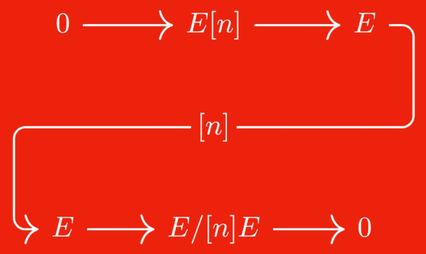
$$t_2 : \quad E(\mathbb{F}_{p^2})[2] \quad \times \quad E(\mathbb{F}_{p^2})/[2]E(\mathbb{F}_{p^2}) \longrightarrow \mu_2$$

1 Fun facts for elliptic curve friends

2 Decompose cokernel using pairings

3 Higher genus fun facts for Jacobian friends

3



Pairings on Kummers

1. Fun facts for elliptic curve friends
2. Decompose cokernel using pairings
3. Higher genus fun facts for Jacobian friends

genus 1 example

Let $E : y^2 = x^3 + Ax^2 + x$ be a supersingular curve over $\mathbb{F}_{p^2}$, with $E(\mathbb{F}_{p^2}) \cong \mathbb{Z}_{p+1} \times \mathbb{Z}_{p+1}$ for $p = 2^a \cdot 3^b - 1$.

fun fact

To find $P \in E(\mathbb{F}_{p^2})$ with ``full 2^a-torsion'':

It is enough to find $P \in E(\mathbb{F}_{p^2})$ with x_P **non-square**

why? →

theorem

The image $[2]E$ is given by all points $(x, y) \in E(\mathbb{F}_{p^2})$ with

$x, x - \alpha, x - \frac{1}{\alpha}$ square

with α root of $x^2 + Ax + 1$

why? →

intuition

The image $[2]E$ is naturally linked to the level 2 red. Tate pairing.

$P \in [2]E \Leftrightarrow t_2(L_i, P) = 1$ for $L_i \in E[2]$

MISTAKE 1

DON'T: think of this as $E(\mathbb{F}_{p^2})$ or $E(\mathbb{F}_{p^2})[2]$

DO: think of this as cosets, $P + [2]E(\mathbb{F}_{p^2})$

$$t_2 : \quad E(\mathbb{F}_{p^2})[2] \quad \times \quad E(\mathbb{F}_{p^2})/[2]E(\mathbb{F}_{p^2}) \longrightarrow \mu_2$$

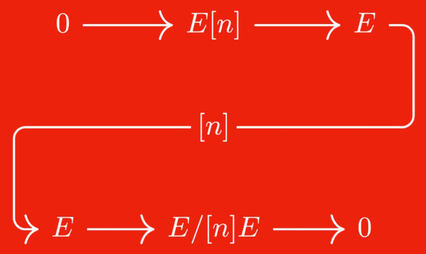
In SQIsign, SIDH/SIKE, we have E supersingular over $\mathbb{F}_{p^2}$ with $2^f \mid p + 1$, think of

$$E(\mathbb{F}_{p^2}) \cong \mathbb{Z}_{2^f} \times \mathbb{Z}_{2^f} \times \mathbb{Z}_h \times \mathbb{Z}_h$$

For P, Q basis of $E[2^f]$, these cosets are essentially

$$\mathcal{O} + [2]E(\mathbb{F}_{p^2}), \quad P + [2]E(\mathbb{F}_{p^2}), \quad Q + [2]E(\mathbb{F}_{p^2}), \quad (P + Q) + [2]E(\mathbb{F}_{p^2})$$

3



Pairings on Kummers

1. Fun facts for elliptic curve friends
2. Decompose cokernel using pairings
3. Higher genus fun facts for Jacobian friends

genus 1 example

Let $E : y^2 = x^3 + Ax^2 + x$ be a supersingular curve over $\mathbb{F}_{p^2}$, with $E(\mathbb{F}_{p^2}) \cong \mathbb{Z}_{p+1} \times \mathbb{Z}_{p+1}$ for $p = 2^a \cdot 3^b - 1$.

fun fact

To find $P \in E(\mathbb{F}_{p^2})$ with ``full 2^a-torsion'':

It is enough to find $P \in E(\mathbb{F}_{p^2})$ with x_P **non-square**

why?

theorem

The image $[2]E$ is given by all points $(x, y) \in E(\mathbb{F}_{p^2})$ with

$x, x - \alpha, x - \frac{1}{\alpha}$ square

with α root of $x^2 + Ax + 1$

why?

intuition

The image $[2]E$ is naturally linked to the level 2 red. Tate pairing.

$P \in [2]E \Leftrightarrow t_2(L_i, P) = 1$ for $L_i \in E[2]$

MISTAKE 1

DON'T: think of this as $E(\mathbb{F}_{p^2})$ or $E(\mathbb{F}_{p^2})[2]$

DO: think of this as cosets, $P + [2]E(\mathbb{F}_{p^2})$

$$t_2 : \quad E(\mathbb{F}_{p^2})[2] \quad \times \quad E(\mathbb{F}_{p^2})/[2]E(\mathbb{F}_{p^2}) \longrightarrow \mu_2$$

In SQIsign, SIDH/SIKE, we have E supersingular over $\mathbb{F}_{p^2}$ with $2^f \mid p + 1$, think of

$$E(\mathbb{F}_{p^2}) \cong \mathbb{Z}_{2^f} \times \mathbb{Z}_{2^f} \times \mathbb{Z}_h \times \mathbb{Z}_h$$

For P, Q basis of $E[2^f]$, these cosets are essentially

$$\mathcal{O} + [2]E(\mathbb{F}_{p^2}), \quad P + [2]E(\mathbb{F}_{p^2}), \quad Q + [2]E(\mathbb{F}_{p^2}), \quad (P + Q) + [2]E(\mathbb{F}_{p^2})$$

So $R \in [2]E(\mathbb{F}_{p^2})$ whenever $t_2(K, R) = 1$ for all points $K \in E(\mathbb{F}_{p^2})[2]$

3

$$0 \longrightarrow E[n] \longrightarrow E \xrightarrow{[n]} E \longrightarrow E/[n]E \longrightarrow 0$$

Pairings on Kummers

1. Fun facts for elliptic curve friends
2. Decompose cokernel using pairings
3. Higher genus fun facts for Jacobian friends

genus 1 example

Let $E : y^2 = x^3 + Ax^2 + x$ be a supersingular curve over $\mathbb{F}_{p^2}$, with $E(\mathbb{F}_{p^2}) \cong \mathbb{Z}_{p+1} \times \mathbb{Z}_{p+1}$ for $p = 2^a \cdot 3^b - 1$.

fun fact

To find $P \in E(\mathbb{F}_{p^2})$ with ``full 2^a-torsion'':

It is enough to find $P \in E(\mathbb{F}_{p^2})$ with x_P **non-square**

why? →

theorem

The image $[2]E$ is given by all points $(x, y) \in E(\mathbb{F}_{p^2})$ with

$x, x - \alpha, x - \frac{1}{\alpha}$ square

with α root of $x^2 + Ax + 1$

why? →

intuition

The image $[2]E$ is naturally linked to the level 2 red. Tate pairing.

$P \in [2]E \Leftrightarrow t_2(L_i, P) = 1$ for $L_i \in E[2]$

MISTAKE 1

DON'T: think of this as $E(\mathbb{F}_{p^2})$ or $E(\mathbb{F}_{p^2})[2]$

DO: think of this as cosets, $P + [2]E(\mathbb{F}_{p^2})$

$$t_2 : \quad E(\mathbb{F}_{p^2})[2] \quad \times \quad E(\mathbb{F}_{p^2})/[2]E(\mathbb{F}_{p^2}) \longrightarrow \mu_2$$

In SQIsign, SIDH/SIKE, we have E supersingular over $\mathbb{F}_{p^2}$ with $2^f \mid p + 1$, think of

$$E(\mathbb{F}_{p^2}) \cong \mathbb{Z}_{2^f} \times \mathbb{Z}_{2^f} \times \mathbb{Z}_h \times \mathbb{Z}_h$$

For P, Q basis of $E[2^f]$, these cosets are essentially

$$\mathcal{O} + [2]E(\mathbb{F}_{p^2}), \quad P + [2]E(\mathbb{F}_{p^2}), \quad Q + [2]E(\mathbb{F}_{p^2}), \quad (P + Q) + [2]E(\mathbb{F}_{p^2})$$

So $R \in [2]E(\mathbb{F}_{p^2})$ whenever $t_2(K, R) = 1$ for all points $K \in E(\mathbb{F}_{p^2})[2]$

profile

For $R \in E(\mathbb{F}_{p^2})$, the **profile** of R is the array

$$(t_2(K_1, R), t_2(K_2, R), \ldots, t_2(K_n, R))$$

for a fixed basis K_i of $E(\mathbb{F}_{p^2})[2]$

3

$$0 \longrightarrow E[n] \longrightarrow E \xrightarrow{[n]} E \longrightarrow E/[n]E \longrightarrow 0$$

Pairings on Kummers

genus 1 example

Let $E : y^2 = x^3 + Ax^2 + x$ be a supersingular curve over $\mathbb{F}_{p^2}$, with $E(\mathbb{F}_{p^2}) \cong \mathbb{Z}_{p+1} \times \mathbb{Z}_{p+1}$ for $p = 2^a \cdot 3^b - 1$.

fun fact

To find $P \in E(\mathbb{F}_{p^2})$ with ``full 2^a-torsion'':

It is enough to find $P \in E(\mathbb{F}_{p^2})$ with x_P **non-square**

why? →

theorem

The image $[2]E$ is given by all points $(x, y) \in E(\mathbb{F}_{p^2})$ with

$x, x - \alpha, x - \frac{1}{\alpha}$ square

with α root of $x^2 + Ax + 1$

why? →

intuition

The image $[2]E$ is naturally linked to the level 2 red. Tate pairing.

$P \in [2]E \Leftrightarrow t_2(L_i, P) = 1$ for $L_i \in E[2]$

MISTAKE 1

DON'T: think of this as $E(\mathbb{F}_{p^2})$ or $E(\mathbb{F}_{p^2})[2]$

DO: think of this as cosets, $P + [2]E(\mathbb{F}_{p^2})$

$$t_2 : \quad E(\mathbb{F}_{p^2})[2] \quad \times \quad E(\mathbb{F}_{p^2})/[2]E(\mathbb{F}_{p^2}) \longrightarrow \mu_2$$

In SQIsign, SIDH/SIKE, we have E supersingular over $\mathbb{F}_{p^2}$ with $2^f \mid p + 1$, think of

$$E(\mathbb{F}_{p^2}) \cong \mathbb{Z}_{2^f} \times \mathbb{Z}_{2^f} \times \mathbb{Z}_h \times \mathbb{Z}_h$$

For P, Q basis of $E[2^f]$, these cosets are essentially

$$\mathcal{O} + [2]E(\mathbb{F}_{p^2}), \quad P + [2]E(\mathbb{F}_{p^2}), \quad Q + [2]E(\mathbb{F}_{p^2}), \quad (P + Q) + [2]E(\mathbb{F}_{p^2})$$

So $R \in [2]E(\mathbb{F}_{p^2})$ whenever $t_2(K, R) = 1$ for all points $K \in E(\mathbb{F}_{p^2})[2]$

profile

For $R \in E(\mathbb{F}_{p^2})$, the **profile** of R is the array

$$(t_2(K_1, R), t_2(K_2, R), \ldots, t_2(K_n, R))$$

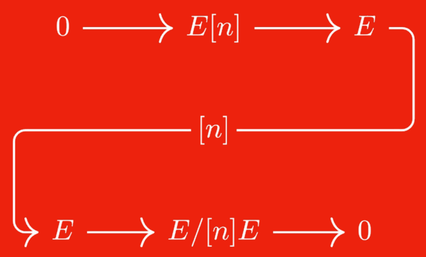
for a fixed basis K_i of $E(\mathbb{F}_{p^2})[2]$

!

$R \in [2]E$ if and only if profile of R is trivial: (1,1)

1. Fun facts for elliptic curve friends
2. Decompose cokernel using pairings
3. Higher genus fun facts for Jacobian friends

3



Pairings on Kummers

genus 1 example

Let $E : y^2 = x^3 + Ax^2 + x$ be a supersingular curve over $\mathbb{F}_{p^2}$, with $E(\mathbb{F}_{p^2}) \cong \mathbb{Z}_{p+1} \times \mathbb{Z}_{p+1}$ for $p = 2^a \cdot 3^b - 1$.

fun fact

To find $P \in E(\mathbb{F}_{p^2})$ with ``full 2^a-torsion'':

It is enough to find $P \in E(\mathbb{F}_{p^2})$ with x_P **non-square**

why?

theorem

The image $[2]E$ is given by all points $(x, y) \in E(\mathbb{F}_{p^2})$ with

$x, x - \alpha, x - \frac{1}{\alpha}$ square

with α root of $x^2 + Ax + 1$

why?

intuition

The image $[2]E$ is naturally linked to the level 2 red. Tate pairing.

$P \in [2]E \Leftrightarrow t_2(L_i, P) = 1$ for $L_i \in E[2]$

MISTAKE 1

DON'T: think of this as $E(\mathbb{F}_{p^2})$ or $E(\mathbb{F}_{p^2})[2]$

DO: think of this as cosets, $P + [2]E(\mathbb{F}_{p^2})$

$$t_2 : \quad E(\mathbb{F}_{p^2})[2] \quad \times \quad E(\mathbb{F}_{p^2})/[2]E(\mathbb{F}_{p^2}) \longrightarrow \mu_2$$

In SQIsign, SIDH/SIKE, we have E supersingular over $\mathbb{F}_{p^2}$ with $2^f \mid p + 1$, think of

$$E(\mathbb{F}_{p^2}) \cong \mathbb{Z}_{2^f} \times \mathbb{Z}_{2^f} \times \mathbb{Z}_h \times \mathbb{Z}_h$$

For P, Q basis of $E[2^f]$, these cosets are essentially

$$\mathcal{O} + [2]E(\mathbb{F}_{p^2}), \quad P + [2]E(\mathbb{F}_{p^2}), \quad Q + [2]E(\mathbb{F}_{p^2}), \quad (P + Q) + [2]E(\mathbb{F}_{p^2})$$

So $R \in [2]E(\mathbb{F}_{p^2})$ whenever $t_2(K, R) = 1$ for all points $K \in E(\mathbb{F}_{p^2})[2]$

profile

For $R \in E(\mathbb{F}_{p^2})$, the **profile** of R is the array

$(t_2(K_1, R), t_2(K_2, R), \ldots, t_2(K_n, R))$

for a fixed basis K_i of $E(\mathbb{F}_{p^2})[2]$

! $R \in [2]E$ if and only if profile of R is trivial: (1,1)

! profile of R determines coset $R \in P + [2]E$

1. Fun facts for elliptic curve friends
2. Decompose cokernel using pairings
3. Higher genus fun facts for Jacobian friends

3

$$0 \longrightarrow E[n] \longrightarrow E \xrightarrow{[n]} E \longrightarrow E/[n]E \longrightarrow 0$$

Pairings on Kummers

genus 1 example

Let $E : y^2 = x^3 + Ax^2 + x$ be a supersingular curve over $\mathbb{F}_{p^2}$, with $E(\mathbb{F}_{p^2}) \cong \mathbb{Z}_{p+1} \times \mathbb{Z}_{p+1}$ for $p = 2^a \cdot 3^b - 1$.

fun fact

To find $P \in E(\mathbb{F}_{p^2})$ with ``full 2^a-torsion'':

It is enough to find $P \in E(\mathbb{F}_{p^2})$ with x_P **non-square**

why?

theorem

The image $[2]E$ is given by all points $(x, y) \in E(\mathbb{F}_{p^2})$ with

$x, x - \alpha, x - \frac{1}{\alpha}$ square

with α root of $x^2 + Ax + 1$

why?

intuition

The image $[2]E$ is naturally linked to the level 2 red. Tate pairing.

$P \in [2]E \Leftrightarrow t_2(L_i, P) = 1$ for $L_i \in E[2]$

1 Fun facts for elliptic curve friends

2 Decompose cokernel using pairings

3 Higher genus fun facts for Jacobian friends

MISTAKE 1

DON'T: think of this as $E(\mathbb{F}_{p^2})$ or $E(\mathbb{F}_{p^2})[2]$

DO: think of this as cosets, $P + [2]E(\mathbb{F}_{p^2})$

$$t_2 : \quad E(\mathbb{F}_{p^2})[2] \quad \times \quad E(\mathbb{F}_{p^2})/[2]E(\mathbb{F}_{p^2}) \longrightarrow \mu_2$$

In SQIsign, SIDH/SIKE, we have E supersingular over $\mathbb{F}_{p^2}$ with $2^f \mid p + 1$, think of

$$E(\mathbb{F}_{p^2}) \cong \mathbb{Z}_{2^f} \times \mathbb{Z}_{2^f} \times \mathbb{Z}_h \times \mathbb{Z}_h$$

For P, Q basis of $E[2^f]$, these cosets are essentially

$$\mathcal{O} + [2]E(\mathbb{F}_{p^2}), \quad P + [2]E(\mathbb{F}_{p^2}), \quad Q + [2]E(\mathbb{F}_{p^2}), \quad (P + Q) + [2]E(\mathbb{F}_{p^2})$$

So $R \in [2]E(\mathbb{F}_{p^2})$ whenever $t_2(K, R) = 1$ for all points $K \in E(\mathbb{F}_{p^2})[2]$

profile

For $R \in E(\mathbb{F}_{p^2})$, the **profile** of R is the array

$(t_2(K_1, R), t_2(K_2, R), \ldots, t_2(K_n, R))$

for a fixed basis K_i of $E(\mathbb{F}_{p^2})[2]$

MISTAKE 2

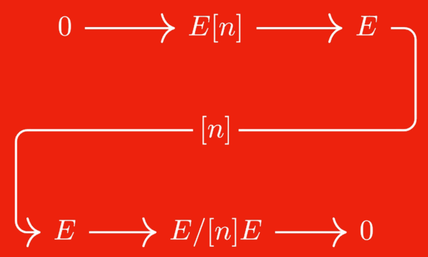
DON'T: think of the Tate-Lichtenbaum pairing as single value

DO: think of an array of values, e.g. evaluated on *all* of $\ker[2]$

$R \in [2]E$ if and only if profile of R is trivial: (1,1)

profile of R determines coset $R \in P + [2]E$

3



Pairings on Kummers

1 Fun facts for elliptic curve friends

2 Decompose cokernel using pairings

3 Higher genus fun facts for Jacobian friends

generalized Tate pairing (Bruin, 2011)

Let $\varphi : J \to J'$ be an isogeny* between Jacobians** of curves, then there exists a perfect pairing

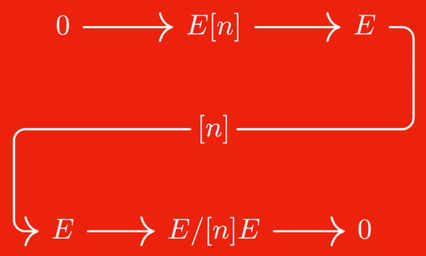
$$t_\varphi : \ker \varphi(k) \times \operatorname{coker} \hat{\varphi}(k) \to k^*$$

where $\operatorname{coker}\hat{\varphi}(\mathrm{k})$ is $J \,/\, \operatorname{Im} \hat{\varphi}(k)$.

Radboud University

*φ needs to be separable, with $\ker \varphi$ annihilated by $q - 1$
**more generally $\varphi : A \to B$ with A, B abelian varieties

3



Pairings on Kummers

1 Fun facts for elliptic curve friends

2 Decompose cokernel using pairings

3 Higher genus fun facts for Jacobian friends

generalized Tate pairing (Bruin, 2011)

Let $\varphi : J \to J'$ be an isogeny* between Jacobians** of curves, then there exists a perfect pairing

$$t_\varphi : \ker \varphi(k) \times \operatorname{coker} \hat{\varphi}(k) \to k^*$$

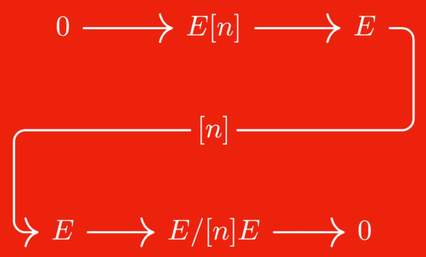
where $\operatorname{coker}\hat{\varphi}(\mathrm{k})$ is $J \,/\, \operatorname{Im} \hat{\varphi}(k)$.

Define **profile** $t_\varphi(R)$ as $(\; t_\varphi(K_i, R) \;)_i$ for K_i basis of $\ker \varphi(k)$

Radboud University

*φ needs to be separable, with $\ker \varphi$ annihilated by $q - 1$
**more generally $\varphi : A \to B$ with A, B abelian varieties

3



Pairings on Kummers

1 Fun facts for elliptic curve friends

2 Decompose cokernel using pairings

3 Higher genus fun facts for Jacobian friends

generalized Tate pairing (Bruin, 2011)

Let $\varphi : J \to J'$ be an isogeny* between Jacobians** of curves, then there exists a perfect pairing

$$t_\varphi : \ker \varphi(k) \times \operatorname{coker} \hat{\varphi}(k) \to k^*$$

where $\operatorname{coker}\hat{\varphi}(\mathrm{k})$ is $J \,/\, \operatorname{Im} \hat{\varphi}(k)$.

Define **profile** $t_\varphi(R)$ as $(\; t_\varphi(K_i, R) \;)_i$ for K_i basis of $\ker \varphi(k)$

decompose J

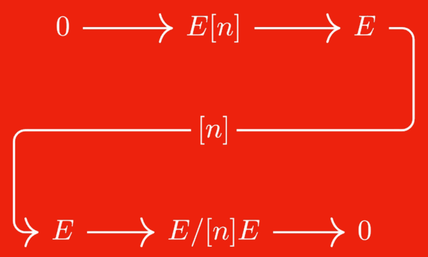
Again, profile **determines** coset:

$$R \in \operatorname{Im}(\hat{\varphi}) \;\Leftrightarrow\; t_\varphi(R) \text{ is trivial}$$

Radboud University

*φ needs to be separable, with $\ker \varphi$ annihilated by $q-1$
**more generally $\varphi : A \to B$ with A, B abelian varieties

3



Pairings on Kummers

1 Fun facts for elliptic curve friends

2 Decompose cokernel using pairings

3 Higher genus fun facts for Jacobian friends

generalized Tate pairing (Bruin, 2011)

Let $\varphi : J \to J'$ be an isogeny* between Jacobians** of curves, then there exists a perfect pairing

$$t_\varphi : \ker \varphi(k) \times \operatorname{coker} \hat{\varphi}(k) \to k^*$$

where $\operatorname{coker}\hat{\varphi}(\mathrm{k})$ is $J \,/\, \operatorname{Im} \hat{\varphi}(k)$.

Define **profile** $t_\varphi(R)$ as $(\; t_\varphi(K_i, R) \;)_i$ for K_i basis of $\ker \varphi(k)$

decompose J

Again, profile **determines** coset:

$$R \in \operatorname{Im}(\hat{\varphi}) \;\Leftrightarrow\; t_\varphi(R) \text{ is trivial}$$

And the even stronger result

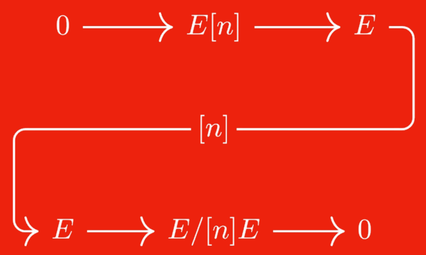
$$R \in P_i + \operatorname{Im}(\hat{\varphi}) \;\Leftrightarrow\; t_\varphi(R) = t_\varphi(P_i)$$

for P_i basis of these cosets

Radboud University

*φ needs to be separable, with $\ker \varphi$ annihilated by $q - 1$
**more generally $\varphi : A \to B$ with A, B abelian varieties

3



Pairings on Kummers

1. Fun facts for elliptic curve friends
2. Decompose cokernel using pairings
3. Higher genus fun facts for Jacobian friends

generalized Tate pairing (Bruin, 2011)

Let $\varphi : J \to J'$ be an isogeny* between Jacobians** of curves, then there exists a perfect pairing

$$t_\varphi : \ker \varphi(k) \times \operatorname{coker} \hat{\varphi}(k) \to k^*$$

where $\operatorname{coker}\hat{\varphi}(\mathrm{k})$ is J / $\operatorname{Im}\hat{\varphi}(k)$.

Define **profile** $t_\varphi(R)$ as $(t_\varphi(K_i, R))_i$ for K_i basis of $\ker \varphi(k)$

decompose J

Again, profile **determines** coset:

$$R \in \operatorname{Im}(\hat{\varphi}) \iff t_\varphi(R) \text{ is trivial}$$

And the even stronger result

$$R \in P_i + \operatorname{Im}(\hat{\varphi}) \iff t_\varphi(R) = t_\varphi(P_i)$$

for P_i basis of these cosets

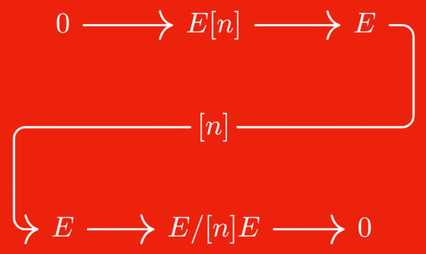
repeating genus 1 example

Let $E : y^2 = x \cdot (x - \alpha) \cdot (x - \bar{\alpha})$, with $\bar{\alpha} = 1/\alpha$ be a supersingular curve over $\mathbb{F}_{p^2}$, with $E(\mathbb{F}_{p^2}) \cong \mathbb{Z}_{p+1} \times \mathbb{Z}_{p+1}$ for $p = 2^a \cdot 3^b - 1$.

Let $L_0 = (0,0)$, $L_\alpha = (\alpha,0)$ and $L_{\bar{\alpha}} = (\bar{\alpha},0)$ the 2-torsion points. Let P_0 and P_α and $P_{\bar{\alpha}}$ points of order 2^f, each over respective L_i.

*φ needs to be separable, with $\ker \varphi$ annihilated by $q - 1$
**more generally $\varphi : A \to B$ with A, B abelian varieties

3



Pairings on Kummers

1 Fun facts for elliptic curve friends

2 Decompose cokernel using pairings

3 Higher genus fun facts for Jacobian friends

generalized Tate pairing (Bruin, 2011)

Let $\varphi : J \to J'$ be an isogeny* between Jacobians** of curves, then there exists a perfect pairing

$$t_\varphi : \ker \varphi(k) \times \operatorname{coker} \hat{\varphi}(k) \to k^*$$

where $\operatorname{coker}\hat{\varphi}(\mathrm{k})$ is J / $\operatorname{Im} \hat{\varphi}(k)$.

Define **profile** $t_\varphi(R)$ as $(t_\varphi(K_i, R))_i$ for K_i basis of $\ker \varphi(k)$

decompose J

Again, profile **determines** coset:

$$R \in \operatorname{Im}(\hat{\varphi}) \iff t_\varphi(R) \text{ is trivial}$$

And the even stronger result

$$R \in P_i + \operatorname{Im}(\hat{\varphi}) \iff t_\varphi(R) = t_\varphi(P_i)$$

for P_i basis of these cosets

repeating genus 1 example

Let $E : y^2 = x \cdot (x - \alpha) \cdot (x - \bar{\alpha})$, with $\bar{\alpha} = 1/\alpha$ be a supersingular curve over $\mathbb{F}_{p^2}$, with $E(\mathbb{F}_{p^2}) \cong \mathbb{Z}_{p+1} \times \mathbb{Z}_{p+1}$ for $p = 2^a \cdot 3^b - 1$.
Let $L_0 = (0,0)$, $L_\alpha = (\alpha,0)$ and $L_{\bar{\alpha}} = (\bar{\alpha},0)$ the 2-torsion points. Let P_0 and P_α and $P_{\bar{\alpha}}$ points of order 2^f, each over respective L_i.

Take $\varphi = [2]$, then $\ker \varphi(k) = E(\mathbb{F}_{p^2})[2]$ and $\operatorname{coker} \hat{\varphi}(k) = E(\mathbb{F}_{p^2})$ / $[2]E(\mathbb{F}_{p^2})$

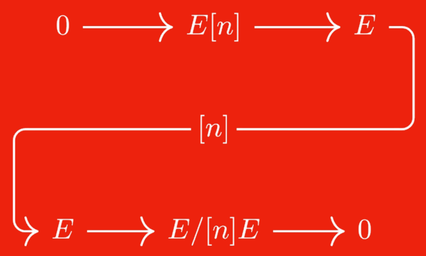
Full profile w.r.t. isogeny $[2] : E \to E$ over $\mathbb{F}_{p^2}$

$$t_2(R) = (t_2(L_0, R),\ t_2(L_\alpha, R), t_2(L_{\bar{\alpha}}, R))$$

Radboud University

*φ needs to be separable, with $\ker \varphi$ annihilated by $q - 1$
**more generally $\varphi : A \to B$ with A, B abelian varieties

3



Pairings on Kummers

1 Fun facts for elliptic curve friends

2 Decompose cokernel using pairings

3 Higher genus fun facts for Jacobian friends

generalized Tate pairing (Bruin, 2011)

Let $\varphi : J \to J'$ be an isogeny* between Jacobians** of curves, then there exists a perfect pairing

$$t_\varphi : \ker \varphi(k) \times \operatorname{coker} \hat{\varphi}(k) \to k^*$$

where $\operatorname{coker}\hat{\varphi}(\mathrm{k})$ is J / $\operatorname{Im}\hat{\varphi}(k)$.

Define **profile** $t_\varphi(R)$ as $(t_\varphi(K_i, R))_i$ for K_i basis of $\ker \varphi(k)$

decompose J

Again, profile **determines** coset:

$$R \in \operatorname{Im}(\hat{\varphi}) \;\Leftrightarrow\; t_\varphi(R) \text{ is trivial}$$

And the even stronger result

$$R \in P_i + \operatorname{Im}(\hat{\varphi}) \;\Leftrightarrow\; t_\varphi(R) = t_\varphi(P_i)$$

for P_i basis of these cosets

repeating genus 1 example

Let $E : y^2 = x \cdot (x - \alpha) \cdot (x - \bar{\alpha})$, with $\bar{\alpha} = 1/\alpha$ be a supersingular curve over $\mathbb{F}_{p^2}$, with $E(\mathbb{F}_{p^2}) \cong \mathbb{Z}_{p+1} \times \mathbb{Z}_{p+1}$ for $p = 2^a \cdot 3^b - 1$.
Let $L_0 = (0,0)$, $L_\alpha = (\alpha,0)$ and $L_{\bar{\alpha}} = (\bar{\alpha},0)$ the 2-torsion points. Let P_0 and P_α and $P_{\bar{\alpha}}$ points of order 2^f, each over respective L_i.

Take $\varphi = [2]$, then $\ker \varphi(k) = E(\mathbb{F}_{p^2})[2]$ and $\operatorname{coker} \hat{\varphi}(k) = E(\mathbb{F}_{p^2})$ / $[2]E(\mathbb{F}_{p^2})$

Full profile w.r.t. isogeny $[2] : E \to E$ over $\mathbb{F}_{p^2}$

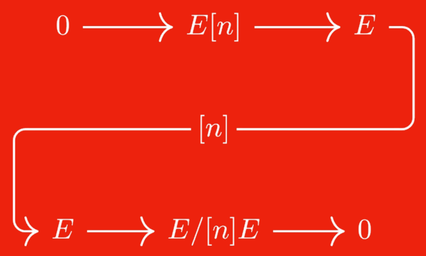
$$t_2(R) = (t_2(L_0, R),\ t_2(L_\alpha, R), t_2(L_{\bar{\alpha}}, R))$$

So, trivial profile implies $R \in [2]E(\mathbb{F}_{p^2})$, but even more:

$t_2(R) = (1, -1, -1)$ implies $R \in P_0 + [2]E$ implies R above L_0
$t_2(R) = (-1, 1, -1)$ implies $R \in P_\alpha + [2]E$ implies R above L_α
$t_2(R) = (-1, -1, 1)$ implies $R \in P_{\bar{\alpha}} + [2]E$ implies R above $L_{\bar{\alpha}}$

*φ needs to be separable, with $\ker \varphi$ annihilated by $q - 1$
**more generally $\varphi : A \to B$ with A, B abelian varieties

3



Pairings on Kummers

1. Fun facts for elliptic curve friends
2. Decompose cokernel using pairings
3. Higher genus fun facts for Jacobian friends

generalized Tate pairing (Bruin, 2011)

Let $\varphi : J \to J'$ be an isogeny* between Jacobians** of curves, then there exists a perfect pairing

$$t_\varphi : \ker \varphi(k) \times \operatorname{coker} \hat{\varphi}(k) \to k^*$$

where $\operatorname{coker}\hat{\varphi}(\mathrm{k})$ is J / $\operatorname{Im} \hat{\varphi}(k)$.

Define **profile** $t_\varphi(R)$ as $(t_\varphi(K_i, R))_i$ for K_i basis of $\ker \varphi(k)$

decompose J

Again, profile **determines** coset:

$$R \in \operatorname{Im}(\hat{\varphi}) \;\Leftrightarrow\; t_\varphi(R) \text{ is trivial}$$

And the even stronger result

$$R \in P_i + \operatorname{Im}(\hat{\varphi}) \;\Leftrightarrow\; t_\varphi(R) = t_\varphi(P_i)$$

for P_i basis of these cosets

repeating genus 1 example

Let $E : y^2 = x \cdot (x - \alpha) \cdot (x - \bar{\alpha})$, with $\bar{\alpha} = 1/\alpha$ be a supersingular curve over $\mathbb{F}_{p^2}$, with $E(\mathbb{F}_{p^2}) \cong \mathbb{Z}_{p+1} \times \mathbb{Z}_{p+1}$ for $p = 2^a \cdot 3^b - 1$.
Let $L_0 = (0,0)$, $L_\alpha = (\alpha,0)$ and $L_{\bar{\alpha}} = (\bar{\alpha},0)$ the 2-torsion points. Let P_0 and P_α and $P_{\bar{\alpha}}$ points of order 2^f, each over respective L_i.

Take $\varphi = [2]$, then $\ker \varphi(k) = E(\mathbb{F}_{p^2})[2]$ and $\operatorname{coker} \hat{\varphi}(k) = E(\mathbb{F}_{p^2})$ / $[2]E(\mathbb{F}_{p^2})$

Full profile w.r.t. isogeny $[2] : E \to E$ over $\mathbb{F}_{p^2}$

$$t_2(R) = (t_2(L_0, R),\ t_2(L_\alpha, R), t_2(L_{\bar{\alpha}}, R))$$

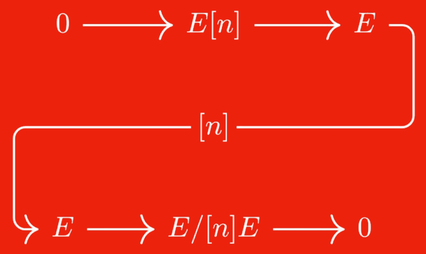
So, trivial profile implies $R \in [2]E(\mathbb{F}_{p^2})$, but even more:

$t_2(R) = (1, -1, -1)$ implies $R \in P_0 + [2]E$ implies R above L_0
$t_2(R) = (-1, 1, -1)$ implies $R \in P_\alpha + [2]E$ implies R above L_α
$t_2(R) = (-1, -1, 1)$ implies $R \in P_{\bar{\alpha}} + [2]E$ implies R above $L_{\bar{\alpha}}$

Radboud University

*φ needs to be separable, with $\ker \varphi$ annihilated by $q - 1$
**more generally $\varphi : A \to B$ with A, B abelian varieties

3



Pairings on Kummers

1 Fun facts for elliptic curve friends

2 Decompose cokernel using pairings

3 Higher genus fun facts for Jacobian friends

generalized Tate pairing (Bruin, 2011)

Let $\varphi : J \to J'$ be an isogeny* between Jacobians** of curves, then there exists a perfect pairing

$$t_\varphi : \ker \varphi(k) \times \operatorname{coker} \hat{\varphi}(k) \to k^*$$

where $\operatorname{coker}\hat{\varphi}(\mathrm{k})$ is J / $\operatorname{Im}\hat{\varphi}(k)$.

Define **profile** $t_\varphi(R)$ as $(t_\varphi(K_i, R))_i$ for K_i basis of $\ker \varphi(k)$

decompose J

Again, profile **determines** coset:

$$R \in \operatorname{Im}(\hat{\varphi}) \;\Leftrightarrow\; t_\varphi(R) \text{ is trivial}$$

And the even stronger result

$$R \in P_i + \operatorname{Im}(\hat{\varphi}) \;\Leftrightarrow\; t_\varphi(R) = t_\varphi(P_i)$$

for P_i basis of these cosets

repeating genus 1 example

Let $E : y^2 = x \cdot (x - \alpha) \cdot (x - \bar{\alpha})$, with $\bar{\alpha} = 1/\alpha$ be a supersingular curve over $\mathbb{F}_{p^2}$, with $E(\mathbb{F}_{p^2}) \cong \mathbb{Z}_{p+1} \times \mathbb{Z}_{p+1}$ for $p = 2^a \cdot 3^b - 1$.
Let $L_0 = (0,0)$, $L_\alpha = (\alpha,0)$ and $L_{\bar{\alpha}} = (\bar{\alpha},0)$ the 2-torsion points. Let P_0 and P_α and $P_{\bar{\alpha}}$ points of order 2^f, each over respective L_i.

Take $\varphi = [2]$, then $\ker \varphi(k) = E(\mathbb{F}_{p^2})[2]$ and $\operatorname{coker} \hat{\varphi}(k) = E(\mathbb{F}_{p^2})$ / $[2]E(\mathbb{F}_{p^2})$

Full profile w.r.t. isogeny $[2] : E \to E$ over $\mathbb{F}_{p^2}$

$$t_2(R) = (t_2(L_0, R),\ t_2(L_\alpha, R), t_2(L_{\bar{\alpha}}, R))$$

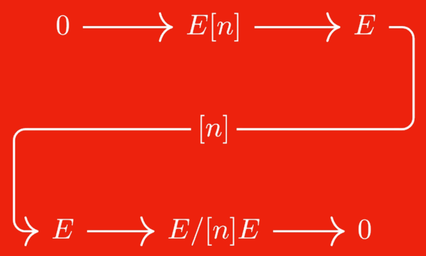
So, trivial profile implies $R \in [2]E(\mathbb{F}_{p^2})$, but even more:

$t_2(R) = (1, -1, -1)$ implies $R \in P_0 + [2]E$ implies R above L_0
$t_2(R) = (-1, 1, -1)$ implies $R \in P_\alpha + [2]E$ implies R above L_α
$t_2(R) = (-1, -1, 1)$ implies $R \in P_{\bar{\alpha}} + [2]E$ implies R above $L_{\bar{\alpha}}$

Radboud University

*φ needs to be separable, with $\ker \varphi$ annihilated by $q - 1$
**more generally $\varphi : A \to B$ with A, B abelian varieties

3



Pairings on Kummers

1 Fun facts for elliptic curve friends

2 Decompose cokernel using pairings

3 Higher genus fun facts for Jacobian friends

generalized Tate pairing (Bruin, 2011)

Let $\varphi : J \to J'$ be an isogeny* between Jacobians** of curves, then there exists a perfect pairing

$$t_\varphi : \ker \varphi(k) \times \operatorname{coker} \hat{\varphi}(k) \to k^*$$

where $\operatorname{coker}\hat{\varphi}(k)$ is J / $\operatorname{Im}\hat{\varphi}(k)$.

Define **profile** $t_\varphi(R)$ as $(t_\varphi(K_i, R))_i$ for K_i basis of $\ker \varphi(k)$

decompose J

Again, profile **determines** coset:

$$R \in \operatorname{Im}(\hat{\varphi}) \iff t_\varphi(R) \text{ is trivial}$$

And the even stronger result

$$R \in P_i + \operatorname{Im}(\hat{\varphi}) \iff t_\varphi(R) = t_\varphi(P_i)$$

for P_i basis of these cosets

repeating genus 1 example

Let $E : y^2 = x \cdot (x - \alpha) \cdot (x - \bar{\alpha})$, with $\bar{\alpha} = 1/\alpha$ be a supersingular curve over $\mathbb{F}_{p^2}$, with $E(\mathbb{F}_{p^2}) \cong \mathbb{Z}_{p+1} \times \mathbb{Z}_{p+1}$ for $p = 2^a \cdot 3^b - 1$.
Let $L_0 = (0,0)$, $L_\alpha = (\alpha,0)$ and $L_{\bar{\alpha}} = (\bar{\alpha},0)$ the 2-torsion points. Let P_0 and P_α and $P_{\bar{\alpha}}$ points of order 2^f, each over respective L_i.

Take $\varphi = [2]$, then $\ker \varphi(k) = E(\mathbb{F}_{p^2})[2]$ and $\operatorname{coker} \hat{\varphi}(k) = E(\mathbb{F}_{p^2})$ / $[2]E(\mathbb{F}_{p^2})$

Full profile w.r.t. isogeny $[2] : E \to E$ over $\mathbb{F}_{p^2}$

$$t_2(R) = (t_2(L_0, R),\ t_2(L_\alpha, R), t_2(L_{\bar{\alpha}}, R))$$

So, trivial profile implies $R \in [2]E(\mathbb{F}_{p^2})$, but even more:

$t_2(R) = (1, -1, -1)$ implies $R \in P_0 + [2]E$ implies R above L_0
$t_2(R) = (-1, 1, -1)$ implies $R \in P_\alpha + [2]E$ implies R above L_α
$t_2(R) = (-1, -1, 1)$ implies $R \in P_{\bar{\alpha}} + [2]E$ implies R above $L_{\bar{\alpha}}$

Take φ_α isogeny given by kernel L_α.
Fact: as φ_α divides [2], we get $t_{\varphi_\alpha} = t_{[2]}$

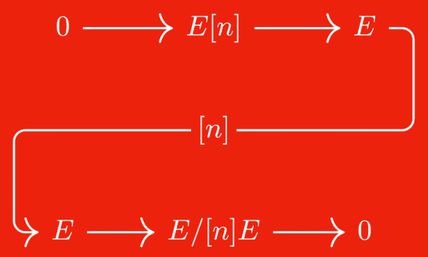
Now, $\ker \varphi_\alpha(\mathbb{F}_{p^2})$ just given by L_α, but (!)

$$\operatorname{coker} \hat{\varphi}_\alpha(\mathbb{F}_{p^2}) = E(\mathbb{F}_{p^2}) \text{ / } \hat{\varphi}_\alpha(E'(\mathbb{F}_{p^2}))$$

Radboud University

*φ needs to be separable, with $\ker \varphi$ annihilated by $q - 1$
**more generally $\varphi : A \to B$ with A, B abelian varieties

3



Pairings on Kummers

1 Fun facts for elliptic curve friends

2 Decompose cokernel using pairings

3 Higher genus fun facts for Jacobian friends

generalized Tate pairing (Bruin, 2011)

Let $\varphi : J \to J'$ be an isogeny* between Jacobians** of curves, then there exists a perfect pairing

$$t_\varphi : \ker \varphi(k) \times \operatorname{coker} \hat{\varphi}(k) \to k^*$$

where $\operatorname{coker}\hat{\varphi}(k)$ is J / $\operatorname{Im}\hat{\varphi}(k)$.

Define **profile** $t_\varphi(R)$ as $(t_\varphi(K_i, R))_i$ for K_i basis of $\ker \varphi(k)$

decompose J

Again, profile **determines** coset:

$$R \in \operatorname{Im}(\hat{\varphi}) \iff t_\varphi(R) \text{ is trivial}$$

And the even stronger result

$$R \in P_i + \operatorname{Im}(\hat{\varphi}) \iff t_\varphi(R) = t_\varphi(P_i)$$

for P_i basis of these cosets

repeating genus 1 example

Let $E : y^2 = x \cdot (x - \alpha) \cdot (x - \bar{\alpha})$, with $\bar{\alpha} = 1/\alpha$ be a supersingular curve over $\mathbb{F}_{p^2}$, with $E(\mathbb{F}_{p^2}) \cong \mathbb{Z}_{p+1} \times \mathbb{Z}_{p+1}$ for $p = 2^a \cdot 3^b - 1$.
Let $L_0 = (0,0)$, $L_\alpha = (\alpha,0)$ and $L_{\bar{\alpha}} = (\bar{\alpha},0)$ the 2-torsion points. Let P_0 and P_α and $P_{\bar{\alpha}}$ points of order 2^f, each over respective L_i.

Take $\varphi = [2]$, then $\ker \varphi(k) = E(\mathbb{F}_{p^2})[2]$ and $\operatorname{coker} \hat{\varphi}(k) = E(\mathbb{F}_{p^2})$ / $[2]E(\mathbb{F}_{p^2})$

Full profile w.r.t. isogeny $[2] : E \to E$ over $\mathbb{F}_{p^2}$

$$t_2(R) = (t_2(L_0, R),\ t_2(L_\alpha, R), t_2(L_{\bar{\alpha}}, R))$$

So, trivial profile implies $R \in [2]E(\mathbb{F}_{p^2})$, but even more:

$t_2(R) = (1, -1, -1)$ implies $R \in P_0 + [2]E$ implies R above L_0
$t_2(R) = (-1, 1, -1)$ implies $R \in P_\alpha + [2]E$ implies R above L_α
$t_2(R) = (-1, -1, 1)$ implies $R \in P_{\bar{\alpha}} + [2]E$ implies R above $L_{\bar{\alpha}}$

Take φ_α isogeny given by kernel L_α.
Fact: as φ_α divides [2], we get $t_{\varphi_\alpha} = t_{[2]}$

Now, $\ker \varphi_\alpha(\mathbb{F}_{p^2})$ just given by L_α, but (!)

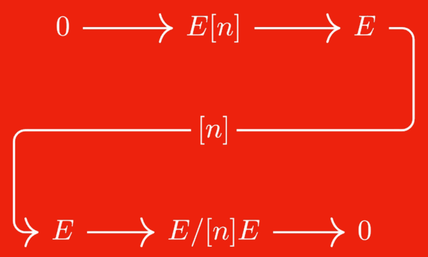
$$\operatorname{coker} \hat{\varphi}_\alpha(\mathbb{F}_{p^2}) = E(\mathbb{F}_{p^2}) \,/\, \hat{\varphi}_\alpha(E'(\mathbb{F}_{p^2}))$$

Brain teaser: think on $\hat{\varphi}_\alpha(E'(\mathbb{F}_{p^2}))$ and realise, for R with 2^f-torsion:

$$t_{\varphi_\alpha}(R) = (1) \text{ iff } R \text{ above } L_\alpha$$

*φ needs to be separable, with $\ker \varphi$ annihilated by $q - 1$
**more generally $\varphi : A \to B$ with A, B abelian varieties

3



Pairings on Kummers

1 Fun facts for elliptic curve friends

2 Decompose cokernel using pairings

3 Higher genus fun facts for Jacobian friends

generalized Tate pairing (Bruin, 2011)

Let $\varphi : J \to J'$ be an isogeny* between Jacobians** of curves, then there exists a perfect pairing

$$t_\varphi : \ker \varphi(k) \times \operatorname{coker} \hat{\varphi}(k) \to k^*$$

where $\operatorname{coker}\hat{\varphi}(k)$ is J / $\operatorname{Im}\hat{\varphi}(k)$.

Define **profile** $t_\varphi(R)$ as $(t_\varphi(K_i, R))_i$ for K_i basis of $\ker \varphi(k)$

decompose J

Again, profile **determines** coset:

$$R \in \operatorname{Im}(\hat{\varphi}) \;\Leftrightarrow\; t_\varphi(R) \text{ is trivial}$$

And the even stronger result

$$R \in P_i + \operatorname{Im}(\hat{\varphi}) \;\Leftrightarrow\; t_\varphi(R) = t_\varphi(P_i)$$

for P_i basis of these cosets

repeating genus 1 example

Let $E : y^2 = x \cdot (x - \alpha) \cdot (x - \bar{\alpha})$, with $\bar{\alpha} = 1/\alpha$ be a supersingular curve over $\mathbb{F}_{p^2}$, with $E(\mathbb{F}_{p^2}) \cong \mathbb{Z}_{p+1} \times \mathbb{Z}_{p+1}$ for $p = 2^a \cdot 3^b - 1$.
Let $L_0 = (0,0)$, $L_\alpha = (\alpha,0)$ and $L_{\bar{\alpha}} = (\bar{\alpha},0)$ the 2-torsion points. Let P_0 and P_α and $P_{\bar{\alpha}}$ points of order 2^f, each over respective L_i.

Take $\varphi = [2]$, then $\ker \varphi(k) = E(\mathbb{F}_{p^2})[2]$ and $\operatorname{coker} \hat{\varphi}(k) = E(\mathbb{F}_{p^2})$ / $[2]E(\mathbb{F}_{p^2})$

Full profile w.r.t. isogeny $[2] : E \to E$ over $\mathbb{F}_{p^2}$

$$t_2(R) = (t_2(L_0, R),\ t_2(L_\alpha, R), t_2(L_{\bar{\alpha}}, R))$$

So, trivial profile implies $R \in [2]E(\mathbb{F}_{p^2})$, but even more:

$t_2(R) = (1, -1, -1)$ implies $R \in P_0 + [2]E$ implies R above L_0
$t_2(R) = (-1, 1, -1)$ implies $R \in P_\alpha + [2]E$ implies R above L_α
$t_2(R) = (-1, -1, 1)$ implies $R \in P_{\bar{\alpha}} + [2]E$ implies R above $L_{\bar{\alpha}}$

Take φ_α isogeny given by kernel L_α.
Fact: as φ_α divides [2], we get $t_{\varphi_\alpha} = t_{[2]}$

Now, $\ker \varphi_\alpha(\mathbb{F}_{p^2})$ just given by L_α, but (!)

$$\operatorname{coker} \hat{\varphi}_\alpha(\mathbb{F}_{p^2}) = E(\mathbb{F}_{p^2}) \,/\, \hat{\varphi}_\alpha(E'(\mathbb{F}_{p^2}))$$

Brain teaser: think on $\hat{\varphi}_\alpha(E'(\mathbb{F}_{p^2}))$ and realise, for R with 2^f-torsion:

$$t_{\varphi_\alpha}(R) = (1) \text{ iff } R \text{ above } L_\alpha$$

! TAKE AWAYS

1. for φ dividing $[n]$, the profile t_φ is essentially a "sub-profile" of $t_{[n]}$
2. the profile $t_\varphi(R)$ allows us to identify a coset $P_i + \operatorname{im}\hat{\varphi}(E'(\mathbb{F}_{p^2}))$
3. in particular, easy to identify $R \notin \operatorname{im}\hat{\varphi}$, we just need one non-trivial $t_\varphi(K_i, R)$

Radboud University

*φ needs to be separable, with $\ker\varphi$ annihilated by $q - 1$
**more generally $\varphi : A \to B$ with A, B abelian varieties

3

$$0 \longrightarrow E[n] \longrightarrow E \xrightarrow{[n]} E \longrightarrow E/[n]E \longrightarrow 0$$

Pairings on Kummers

genus 2 example

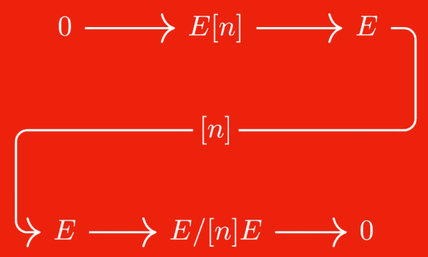
Let E_α be a supersingular curve as before over $\mathbb{F}_{p^2}$, and J_α be its genus-2 friend over $\mathbb{F}_p$. Then $J_\alpha \cong \mathbb{Z}_{\frac{p+1}{2}} \times \mathbb{Z}_{\frac{p+1}{2}} \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

1 Fun facts for elliptic curve friends

2 Decompose cokernel using pairings

3 Higher genus fun facts for Jacobian friends

3



Pairings on Kummers

genus 2 example

Let E_α be a supersingular curve as before over $\mathbb{F}_{p^2}$, and J_α be its genus-2 friend over $\mathbb{F}_p$. Then $J_\alpha \cong \mathbb{Z}_{\frac{p+1}{2}} \times \mathbb{Z}_{\frac{p+1}{2}} \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

problem

The image of E_α is the part $\mathbb{Z}_{\frac{p+1}{2}} \times \mathbb{Z}_{\frac{p+1}{2}}$.

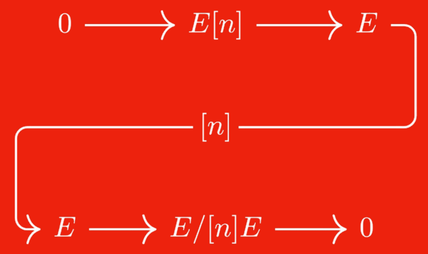
For basis P_1, P_2, P_3, P_4 of J_α, we want $R \in \mathrm{im}(E_\alpha) = \langle P_1, P_2 \rangle$ with full 2-torsion

1 Fun facts for elliptic curve friends

2 Decompose cokernel using pairings

3 Higher genus fun facts for Jacobian friends

3



Pairings on Kummers

genus 2 example

Let E_α be a supersingular curve as before over $\mathbb{F}_{p^2}$, and J_α be its genus-2 friend over $\mathbb{F}_p$. Then $J_\alpha \cong \mathbb{Z}_{\frac{p+1}{2}} \times \mathbb{Z}_{\frac{p+1}{2}} \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

problem

The image of E_α is the part $\mathbb{Z}_{\frac{p+1}{2}} \times \mathbb{Z}_{\frac{p+1}{2}}$.

For basis P_1, P_2, P_3, P_4 of J_α, we want $R \in \mathrm{im}(E_\alpha) = \langle P_1, P_2 \rangle$ with full 2-torsion

how? →

profiles

In genus 1:
find $R \in E \backslash [2]E$
$\Rightarrow$ non-triv profile

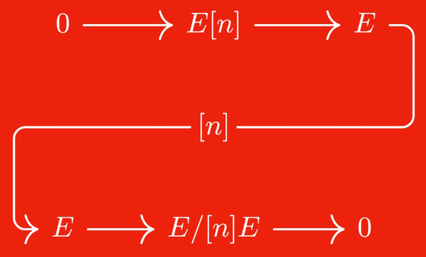
In genus 2:
$R \in J_\alpha \backslash [2]J_\alpha$ might not have full 2-torsion!

1 Fun facts for elliptic curve friends

2 Decompose cokernel using pairings

3 Higher genus fun facts for Jacobian friends

3



Pairings on Kummers

1 Fun facts for elliptic curve friends

2 Decompose cokernel using pairings

3 Higher genus fun facts for Jacobian friends

genus 2 example

Let E_α be a supersingular curve as before over $\mathbb{F}_{p^2}$, and J_α be its genus-2 friend over $\mathbb{F}_p$. Then $J_\alpha \cong \mathbb{Z}_{\frac{p+1}{2}} \times \mathbb{Z}_{\frac{p+1}{2}} \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

problem

The image of E_α is the part $\mathbb{Z}_{\frac{p+1}{2}} \times \mathbb{Z}_{\frac{p+1}{2}}$.

For basis P_1, P_2, P_3, P_4 of J_α, we want $R \in \mathrm{im}(E_\alpha) = \langle P_1, P_2 \rangle$ with full 2-torsion

how? →

profiles

In genus 1: find $R \in E \backslash [2]E$ ⇒ non-triv profile

In genus 2: $R \in J_\alpha \backslash [2]J_\alpha$ might not have full 2-torsion!

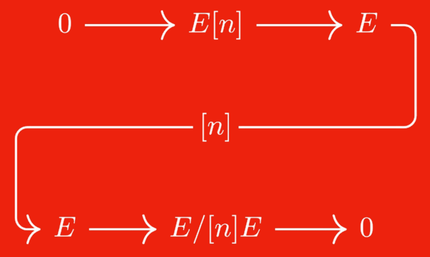
how? →

instead

Compute profiles $t_2(P_1)$ and $t_2(P_2)$, and find R with such a profile

Not only R has full 2-torsion, but shows that $R \in \mathrm{im}\, E_\alpha$

3



Pairings on Kummers

1 Fun facts for elliptic curve friends

2 Decompose cokernel using pairings

3 Higher genus fun facts for Jacobian friends

genus 2 example

Let E_α be a supersingular curve as before over $\mathbb{F}_{p^2}$, and J_α be its genus-2 friend over $\mathbb{F}_p$. Then $J_\alpha \cong \mathbb{Z}_{\frac{p+1}{2}} \times \mathbb{Z}_{\frac{p+1}{2}} \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

problem

The image of E_α is the part $\mathbb{Z}_{\frac{p+1}{2}} \times \mathbb{Z}_{\frac{p+1}{2}}$.

For basis P_1, P_2, P_3, P_4 of J_α, we want $R \in \mathrm{im}(E_\alpha) = \langle P_1, P_2 \rangle$ with full 2-torsion

how? →

profiles

In genus 1: find $R \in E \backslash [2]E$ ⇒ non-triv profile

In genus 2: $R \in J_\alpha \backslash [2]J_\alpha$ might not have full 2-torsion!

how? →

instead

Compute profiles $t_2(P_1)$ and $t_2(P_2)$, and find R with such a profile

Not only R has full 2-torsion, but shows that $R \in \mathrm{im}\, E_\alpha$

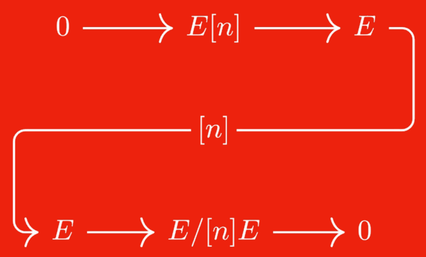
decomposition

Have $J_\alpha(\mathbb{F}_p) \cong \mathbb{Z}_{\frac{p+1}{2}} \times \mathbb{Z}_{\frac{p+1}{2}} \times \mathbb{Z}_2 \times \mathbb{Z}_2$ with basis P_1, P_2, P_3, P_4 of order $\frac{p+1}{2}, \frac{p+1}{2}, 2, 2$.

Image of doubling is

$$[2]J_\alpha = a \cdot [2]P_1 + b \cdot [2]P_2 \quad \text{with} \quad a, b \in \{1, \ldots, \frac{p+1}{4}\}$$

3



Pairings on Kummers

1 Fun facts for elliptic curve friends

2 Decompose cokernel using pairings

3 Higher genus fun facts for Jacobian friends

genus 2 example

Let E_α be a supersingular curve as before over $\mathbb{F}_{p^2}$, and J_α be its genus-2 friend over $\mathbb{F}_p$. Then $J_\alpha \cong \mathbb{Z}_{\frac{p+1}{2}} \times \mathbb{Z}_{\frac{p+1}{2}} \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

problem

The image of E_α is the part $\mathbb{Z}_{\frac{p+1}{2}} \times \mathbb{Z}_{\frac{p+1}{2}}$.

For basis P_1, P_2, P_3, P_4 of J_α, we want $R \in \mathrm{im}(E_\alpha) = \langle P_1, P_2 \rangle$ with full 2-torsion

how? →

profiles

In genus 1: find $R \in E \backslash [2]E$ ⇒ non-triv profile

In genus 2: $R \in J_\alpha \backslash [2]J_\alpha$ might not have full 2-torsion!

how? →

instead

Compute profiles $t_2(P_1)$ and $t_2(P_2)$, and find R with such a profile

Not only R has full 2-torsion, but shows that $R \in \mathrm{im}\, E_\alpha$

decomposition

Have $J_\alpha(\mathbb{F}_p) \cong \mathbb{Z}_{\frac{p+1}{2}} \times \mathbb{Z}_{\frac{p+1}{2}} \times \mathbb{Z}_2 \times \mathbb{Z}_2$ with basis P_1, P_2, P_3, P_4 of order $\frac{p+1}{2}, \frac{p+1}{2}, 2, 2$.

Image of doubling is

$$[2]J_\alpha = a \cdot [2]P_1 + b \cdot [2]P_2 \quad \text{with} \quad a, b \in \{1, \ldots, \frac{p+1}{4}\}$$

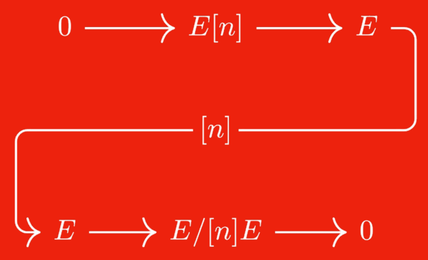
Decomposition into 16 cosets is given by

$$a \cdot P_1 + b \cdot P_2 + c \cdot P_3 + d \cdot P_4 + [2]J_\alpha \quad \text{with} \quad a, b, c, d \in \{0,1\}$$

gives group structure $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \cong J_\alpha[2]$.

Points $R \in \mathrm{im}\, E_\alpha$ with full 2-torsion are the cosets with $c = d = 0$.

3



Pairings on Kummers

1 Fun facts for elliptic curve friends

2 Decompose cokernel using pairings

3 Higher genus fun facts for Jacobian friends

genus 2 example

Let E_α be a supersingular curve as before over $\mathbb{F}_{p^2}$, and J_α be its genus-2 friend over $\mathbb{F}_p$. Then $J_\alpha \cong \mathbb{Z}_{\frac{p+1}{2}} \times \mathbb{Z}_{\frac{p+1}{2}} \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

problem

The image of E_α is the part $\mathbb{Z}_{\frac{p+1}{2}} \times \mathbb{Z}_{\frac{p+1}{2}}$.

For basis P_1, P_2, P_3, P_4 of J_α, we want $R \in \mathrm{im}(E_\alpha) = \langle P_1, P_2 \rangle$ with full 2-torsion

how? →

profiles

In genus 1: find $R \in E \backslash [2]E$ ⇒ non-triv profile

In genus 2: $R \in J_\alpha \backslash [2]J_\alpha$ might not have full 2-torsion!

how? →

instead

Compute profiles $t_2(P_1)$ and $t_2(P_2)$, and find R with such a profile

Not only R has full 2-torsion, but shows that $R \in \mathrm{im}\, E_\alpha$

decomposition

Have $J_\alpha(\mathbb{F}_p) \cong \mathbb{Z}_{\frac{p+1}{2}} \times \mathbb{Z}_{\frac{p+1}{2}} \times \mathbb{Z}_2 \times \mathbb{Z}_2$ with basis P_1, P_2, P_3, P_4 of order $\frac{p+1}{2}, \frac{p+1}{2}, 2, 2$.

Image of doubling is

$$[2]J_\alpha = a \cdot [2]P_1 + b \cdot [2]P_2 \quad \text{with} \quad a, b \in \{1, \ldots, \frac{p+1}{4}\}$$

Decomposition into 16 cosets is given by

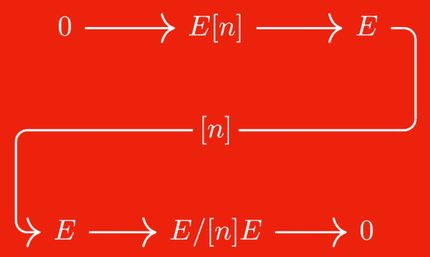
$$a \cdot P_1 + b \cdot P_2 + c \cdot P_3 + d \cdot P_4 + [2]J_\alpha \quad \text{with} \quad a, b, c, d \in \{0,1\}$$

gives group structure $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \cong J_\alpha[2]$.

Points $R \in \mathrm{im}\, E_\alpha$ with full 2-torsion are the cosets with $c = d = 0$.

Advanced tricks: can identify such points by *sub-profile*, don't need full profile $t_2(R)$.
(abstract interpretation: there is an isogeny φ with $t_\varphi(R)$ non-trivial $\Leftrightarrow R \in \mathrm{im}\, E_\alpha$ with full 2-torsion)

3



Pairings on Kummers

1 Fun facts for elliptic curve friends

2 Decompose cokernel using pairings

3 Higher genus fun facts for Jacobian friends

genus 2 example

Let E_α be a supersingular curve as before over $\mathbb{F}_{p^2}$, and J_α be its genus-2 friend over $\mathbb{F}_p$. Then $J_\alpha \cong \mathbb{Z}_{\frac{p+1}{2}} \times \mathbb{Z}_{\frac{p+1}{2}} \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

problem

The image of E_α is the part $\mathbb{Z}_{\frac{p+1}{2}} \times \mathbb{Z}_{\frac{p+1}{2}}$.

For basis P_1, P_2, P_3, P_4 of J_α, we want $R \in \mathrm{im}(E_\alpha) = \langle P_1, P_2 \rangle$ with full 2-torsion

how? →

profiles

In genus 1: find $R \in E \backslash [2]E$ ⇒ non-triv profile

In genus 2: $R \in J_\alpha \backslash [2]J_\alpha$ might not have full 2-torsion!

how? →

instead

Compute profiles $t_2(P_1)$ and $t_2(P_2)$, and find R with such a profile

Not only R has full 2-torsion, but shows that $R \in \mathrm{im}\, E_\alpha$

decomposition

Have $J_\alpha(\mathbb{F}_p) \cong \mathbb{Z}_{\frac{p+1}{2}} \times \mathbb{Z}_{\frac{p+1}{2}} \times \mathbb{Z}_2 \times \mathbb{Z}_2$ with basis P_1, P_2, P_3, P_4 of order $\frac{p+1}{2}, \frac{p+1}{2}, 2, 2$.

Image of doubling is

$$[2]J_\alpha = a \cdot [2]P_1 + b \cdot [2]P_2 \quad \text{with} \quad a, b \in \{1, \ldots, \frac{p+1}{4}\}$$

Decomposition into 16 cosets is given by

$$a \cdot P_1 + b \cdot P_2 + c \cdot P_3 + d \cdot P_4 + [2]J_\alpha \quad \text{with} \quad a, b, c, d \in \{0,1\}$$

gives group structure $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \cong J_\alpha[2]$.

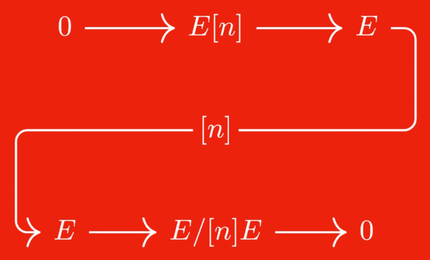
Points $R \in \mathrm{im}\, E_\alpha$ with full 2-torsion are the cosets with $c = d = 0$.

Advanced tricks: can identify such points by *sub-profile*, don't need full profile $t_2(R)$.
(abstract interpretation: there is an isogeny φ with $t_\varphi(R)$ non-trivial ⇔ $R \in \mathrm{im}\, E_\alpha$ with full 2-torsion)

practice

Want to compute profiles, e.g. 2-Tate pairings, on Kummer K_α

3



Pairings on Kummers

1. Fun facts for elliptic curve friends
2. Decompose cokernel using pairings
3. Higher genus fun facts for Jacobian friends

genus 2 example

Let E_α be a supersingular curve as before over $\mathbb{F}_{p^2}$, and J_α be its genus-2 friend over $\mathbb{F}_p$. Then $J_\alpha \cong \mathbb{Z}_{\frac{p+1}{2}} \times \mathbb{Z}_{\frac{p+1}{2}} \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

problem

The image of E_α is the part $\mathbb{Z}_{\frac{p+1}{2}} \times \mathbb{Z}_{\frac{p+1}{2}}$.

For basis P_1, P_2, P_3, P_4 of J_α, we want $R \in \mathrm{im}(E_\alpha) = \langle P_1, P_2 \rangle$ with full 2-torsion

how? →

profiles

In genus 1: find $R \in E \backslash [2]E$ ⇒ non-triv profile

In genus 2: $R \in J_\alpha \backslash [2]J_\alpha$ might not have full 2-torsion!

how? →

instead

Compute profiles $t_2(P_1)$ and $t_2(P_2)$, and find R with such a profile

Not only R has full 2-torsion, but shows that $R \in \mathrm{im}\, E_\alpha$

decomposition

Have $J_\alpha(\mathbb{F}_p) \cong \mathbb{Z}_{\frac{p+1}{2}} \times \mathbb{Z}_{\frac{p+1}{2}} \times \mathbb{Z}_2 \times \mathbb{Z}_2$ with basis P_1, P_2, P_3, P_4 of order $\frac{p+1}{2}, \frac{p+1}{2}, 2, 2$.

Image of doubling is

$$[2]J_\alpha = a \cdot [2]P_1 + b \cdot [2]P_2 \quad \text{with} \quad a, b \in \{1, \ldots, \frac{p+1}{4}\}$$

Decomposition into 16 cosets is given by

$$a \cdot P_1 + b \cdot P_2 + c \cdot P_3 + d \cdot P_4 + [2]J_\alpha \quad \text{with} \quad a, b, c, d \in \{0,1\}$$

gives group structure $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \cong J_\alpha[2]$.

Points $R \in \mathrm{im}\, E_\alpha$ with full 2-torsion are the cosets with $c = d = 0$.

Advanced tricks: can identify such points by *sub-profile*, don't need full profile $t_2(R)$.
(abstract interpretation: there is an isogeny φ with $t_\varphi(R)$ non-trivial ⇔ $R \in \mathrm{im}\, E_\alpha$ with full 2-torsion)

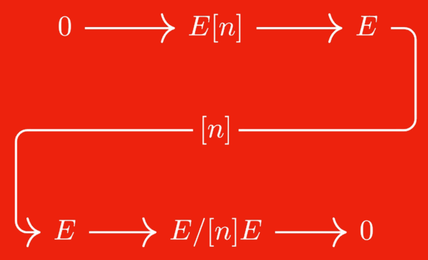
practice

Want to compute profiles, e.g. 2-Tate pairings, on Kummer K_α

Three approaches:

1. Use theta functions to express pairing in terms of coord. $(X_1 : X_2 : X_3 : X_4) \in K_\alpha$

3



Pairings on Kummers

1. Fun facts for elliptic curve friends
2. Decompose cokernel using pairings
3. Higher genus fun facts for Jacobian friends

genus 2 example

Let E_α be a supersingular curve as before over $\mathbb{F}_{p^2}$, and J_α be its genus-2 friend over $\mathbb{F}_p$. Then $J_\alpha \cong \mathbb{Z}_{\frac{p+1}{2}} \times \mathbb{Z}_{\frac{p+1}{2}} \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

problem

The image of E_α is the part $\mathbb{Z}_{\frac{p+1}{2}} \times \mathbb{Z}_{\frac{p+1}{2}}$.

For basis P_1, P_2, P_3, P_4 of J_α, we want $R \in \mathrm{im}(E_\alpha) = \langle P_1, P_2 \rangle$ with full 2-torsion

how? →

profiles

In genus 1: find $R \in E \backslash [2]E$ ⇒ non-triv profile

In genus 2: $R \in J_\alpha \backslash [2]J_\alpha$ might not have full 2-torsion!

how? →

instead

Compute profiles $t_2(P_1)$ and $t_2(P_2)$, and find R with such a profile

Not only R has full 2-torsion, but shows that $R \in \mathrm{im}\, E_\alpha$

decomposition

Have $J_\alpha(\mathbb{F}_p) \cong \mathbb{Z}_{\frac{p+1}{2}} \times \mathbb{Z}_{\frac{p+1}{2}} \times \mathbb{Z}_2 \times \mathbb{Z}_2$ with basis P_1, P_2, P_3, P_4 of order $\frac{p+1}{2}, \frac{p+1}{2}, 2, 2$.

Image of doubling is

$$[2]J_\alpha = a \cdot [2]P_1 + b \cdot [2]P_2 \quad \text{with} \quad a, b \in \{1, \ldots, \frac{p+1}{4}\}$$

Decomposition into 16 cosets is given by

$$a \cdot P_1 + b \cdot P_2 + c \cdot P_3 + d \cdot P_4 + [2]J_\alpha \quad \text{with} \quad a, b, c, d \in \{0,1\}$$

gives group structure $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \cong J_\alpha[2]$.

Points $R \in \mathrm{im}\, E_\alpha$ with full 2-torsion are the cosets with $c = d = 0$.

Advanced tricks: can identify such points by *sub-profile*, don't need full profile $t_2(R)$.
(abstract interpretation: there is an isogeny φ with $t_\varphi(R)$ non-trivial ⇔ $R \in \mathrm{im}\, E_\alpha$ with full 2-torsion)

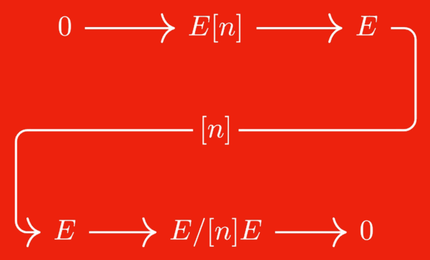
practice

Want to compute profiles, e.g. 2-Tate pairings, on Kummer K_α

Three approaches:

1. Use theta functions to express pairing in terms of coord. $(X_1 : X_2 : X_3 : X_4) \in K_\alpha$
2. Use elegant monodromy approach of Robert (2024)!

3



Pairings on Kummers

1. Fun facts for elliptic curve friends
2. Decompose cokernel using pairings
3. Higher genus fun facts for Jacobian friends

genus 2 example

Let E_α be a supersingular curve as before over $\mathbb{F}_{p^2}$, and J_α be its genus-2 friend over $\mathbb{F}_p$. Then $J_\alpha \cong \mathbb{Z}_{\frac{p+1}{2}} \times \mathbb{Z}_{\frac{p+1}{2}} \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

problem

The image of E_α is the part $\mathbb{Z}_{\frac{p+1}{2}} \times \mathbb{Z}_{\frac{p+1}{2}}$.

For basis P_1, P_2, P_3, P_4 of J_α, we want $R \in \mathrm{im}(E_\alpha) = \langle P_1, P_2 \rangle$ with full 2-torsion

how? →

profiles

In genus 1: find $R \in E \backslash [2]E$ ⇒ non-triv profile

In genus 2: $R \in J_\alpha \backslash [2]J_\alpha$ might not have full 2-torsion!

how? →

instead

Compute profiles $t_2(P_1)$ and $t_2(P_2)$, and find R with such a profile

Not only R has full 2-torsion, but shows that $R \in \mathrm{im}\, E_\alpha$

decomposition

Have $J_\alpha(\mathbb{F}_p) \cong \mathbb{Z}_{\frac{p+1}{2}} \times \mathbb{Z}_{\frac{p+1}{2}} \times \mathbb{Z}_2 \times \mathbb{Z}_2$ with basis P_1, P_2, P_3, P_4 of order $\frac{p+1}{2}, \frac{p+1}{2}, 2, 2$.

Image of doubling is

$$[2]J_\alpha = a \cdot [2]P_1 + b \cdot [2]P_2 \quad \text{with} \quad a, b \in \{1, \ldots, \frac{p+1}{4}\}$$

Decomposition into 16 cosets is given by

$$a \cdot P_1 + b \cdot P_2 + c \cdot P_3 + d \cdot P_4 + [2]J_\alpha \quad \text{with} \quad a, b, c, d \in \{0,1\}$$

gives group structure $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \cong J_\alpha[2]$.

Points $R \in \mathrm{im}\, E_\alpha$ with full 2-torsion are the cosets with $c = d = 0$.

Advanced tricks: can identify such points by *sub-profile*, don't need full profile $t_2(R)$.
(abstract interpretation: there is an isogeny φ with $t_\varphi(R)$ non-trivial ⇔ $R \in \mathrm{im}\, E_\alpha$ with full 2-torsion)

practice

Want to compute profiles, e.g. 2-Tate pairings, on Kummer K_α

Three approaches:

1. Use theta functions to express pairing in terms of coord. $(X_1 : X_2 : X_3 : X_4) \in K_\alpha$
2. Use elegant monodromy approach of Robert (2024)!
3. Develop more efficient methods for partial map $K_\alpha \to J_\alpha$ which allows very efficient profiling 😎😎😎

Concluding

1

In general, can do many things on the Kummer that we can do on ell curve.

Allows for isogeny-based crypto on the Kummer over $\mathbb{F}_p$!

Concluding

1

In general, can do many things on the Kummer that we can do on ell curve.

Allows for isogeny-based crypto on the Kummer over $\mathbb{F}_p$!

2

Doing SQIsign uncompressed is easy given the tools “out there”.

Is it faster using optimised parallelised low-level aright.?

Concluding

1

In general, can do many things on the Kummer that we can do on ell curve.

Allows for isogeny-based crypto on the Kummer over $\mathbb{F}_p$!

2

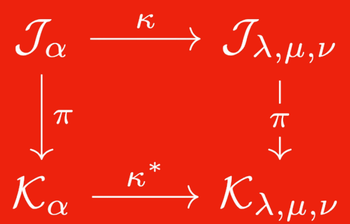
Doing SQIsign uncompressed is easy given the tools “out there”.

Is it faster using optimised parallelised low-level aright.?

3

Doing compressed SQIsign requires fun but complex techniques

Pairings are great to decompose cokernels!
Applies for efficient sampling.

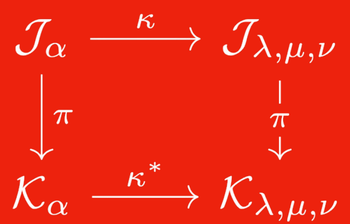


Kummers in Cryptography

Costello's SIDH on Kummer

Any elliptic curve $E_\alpha/\mathbb{F}_{p^2}$ has a $(2,2)$-isogenous Kummer friend $K_\alpha/\mathbb{F}_p$

- The curve E_α has three 2-isogenies, defined either by $P_0, P_\alpha, P_{1/\alpha}$
- The Kummer K_α has corresponding $(2,2)$-isogenies
- By magic, these $(2,2)$'s can be described by single points $P'_0, P'_\alpha, P'_{1/\alpha}$ instead of subgroups!
- Thus, given a point of order 2^n on $K_{\alpha'}$ we can do a $(2^n,2^n)$-isogeny on the Kummers



Kummers in Cryptography

Costello's SIDH on Kummer

Any elliptic curve $E_\alpha/\mathbb{F}_{p^2}$ has a $(2,2)$-isogenous Kummer friend $K_\alpha/\mathbb{F}_p$

- The curve E_α has three 2-isogenies, defined either by $P_0, P_\alpha, P_{1/\alpha}$
- The Kummer K_α has corresponding $(2,2)$-isogenies
- By magic, these $(2,2)$'s can be described by single points $P'_0, P'_\alpha, P'_{1/\alpha}$ instead of subgroups!
- Thus, given a point of order 2^n on $K_{\alpha'}$ we can do a $(2^n,2^n)$-isogeny on the Kummers

Scholten

Each elliptic curve E_α over $\mathbb{F}_{p^2}$ has a (2,2)-isogenous Kummer K_α over $\mathbb{F}_p$ whenever $\alpha = \alpha_0 + \alpha_1 i$ has $\alpha_0, \alpha_1 \neq 0$.

K_α is derived through a curve $C_{\lambda,\mu,\nu}$ with $\lambda, \mu, \nu \in \mathbb{F}_p$ and $\lambda \cdot \mu = \nu$.

Categorically, we map **objects**
$E_\alpha \mapsto K_\alpha$ by $\alpha \mapsto (\lambda, \mu, \nu)$

$$\begin{array}{ccc} \mathcal{J}_\alpha & \xrightarrow{\kappa} & \mathcal{J}_{\lambda,\mu,\nu} \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ \mathcal{K}_\alpha & \xrightarrow{\kappa^*} & \mathcal{K}_{\lambda,\mu,\nu} \end{array}$$

Kummers in Cryptography

Costello's SIDH on Kummer

Any elliptic curve $E_\alpha/\mathbb{F}_{p^2}$ has a (2,2)-isogenous Kummer friend $K_\alpha/\mathbb{F}_p$

- The curve E_α has three 2-isogenies, defined either by $P_0, P_\alpha, P_{1/\alpha}$
- The Kummer K_α has corresponding (2,2)-isogenies
- By magic, these (2,2)'s can be described by single points $P'_0, P'_\alpha, P'_{1/\alpha}$ instead of subgroups!
- Thus, given a point of order 2^n on $K_{\alpha'}$ we can do a $(2^n,2^n)$-isogeny on the Kummers

Scholten

Each elliptic curve E_α over $\mathbb{F}_{p^2}$ has a (2,2)-isogenous Kummer K_α over $\mathbb{F}_p$ whenever $\alpha = \alpha_0 + \alpha_1 i$ has $\alpha_0, \alpha_1 \neq 0$.

K_α is derived through a curve $C_{\lambda,\mu,\nu}$ with $\lambda, \mu, \nu \in \mathbb{F}_p$ and $\lambda \cdot \mu = \nu$.

Categorically, we map **objects**
$E_\alpha \mapsto K_\alpha$ by $\alpha \mapsto (\lambda, \mu, \nu)$

Costello

These elliptic curves E_α naturally have 2-isogenies, given by $E_\alpha[2]$.

Similarly, Kummer surface K_α has associated (2,2)-isogenies, that are identified by point $P \in K_\alpha[2]$.

Categorically, maps **morphisms**
$E_\alpha \xrightarrow{\varphi} E'_\alpha$ to $K_\alpha \xrightarrow{\xi} K'_\alpha$

$$\begin{array}{ccc} \mathcal{J}_\alpha & \xrightarrow{\kappa} & \mathcal{J}_{\lambda,\mu,\nu} \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ \mathcal{K}_\alpha & \xrightarrow{\kappa^*} & \mathcal{K}_{\lambda,\mu,\nu} \end{array}$$

Kummers in Cryptography

Costello's SIDH on Kummer

Any elliptic curve $E_\alpha/\mathbb{F}_{p^2}$ has a (2,2)-isogenous Kummer friend $K_\alpha/\mathbb{F}_p$

- The curve E_α has three 2-isogenies, defined either by $P_0, P_\alpha, P_{1/\alpha}$
- The Kummer K_α has corresponding (2,2)-isogenies
- By magic, these (2,2)'s can be described by single points $P'_0, P'_\alpha, P'_{1/\alpha}$ instead of subgroups!
- Thus, given a point of order 2^n on $K_{\alpha'}$ we can do a $(2^n,2^n)$-isogeny on the Kummers

Scholten

Each elliptic curve E_α over $\mathbb{F}_{p^2}$ has a (2,2)-isogenous Kummer K_α over $\mathbb{F}_p$ whenever $\alpha = \alpha_0 + \alpha_1 i$ has $\alpha_0, \alpha_1 \neq 0$.

K_α is derived through a curve $C_{\lambda,\mu,\nu}$ with $\lambda, \mu, \nu \in \mathbb{F}_p$ and $\lambda \cdot \mu = \nu$.

Categorically, we map **objects**

$E_\alpha \mapsto K_\alpha$ by $\alpha \mapsto (\lambda, \mu, \nu)$

Costello

These elliptic curves E_α naturally have 2-isogenies, given by $E_\alpha[2]$.

Similarly, Kummer surface K_α has associated (2,2)-isogenies, that are identified by point $P \in K_\alpha[2]$.

Categorically, maps **morphisms**

$E_\alpha \xrightarrow{\varphi} E'_\alpha$ to $K_\alpha \xrightarrow{\xi} K'_\alpha$

Corte-Real Santos & R.

Given $\lambda, \mu, \nu \in \mathbb{F}_p$ with $\lambda \cdot \mu = \nu$, the Kummer surface K over $\mathbb{F}_p$ derived from $C_{\lambda,\mu,\nu}$ has a (2,2)-isogenous elliptic curve friend E_α over $\mathbb{F}_{p^2}$.

The 2-isogeny graph of elliptic curves over $\mathbb{F}_{p^2}$ **reappears** as a subgraph of (2,2)-isogeny graph!