Finanziato dall'Unione europea NextGenerationEU

Ministero dell'Università e della Ricerca

Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA

SERICS SECURITY AND RIGHTS IN THE CYBERSPACE

CrypTO CONFERENCE

Politecnico di Torino 1859

Telsy A TIM ENTERPRISE BRAND

DISMA

Representing isogenies via (classical, canonical, Atkin...) modular polynomials

Joint work with Thomas den Hollander, Marc Houben,
Sören Kleine, Daniel Slamanig, Sebastian A. Spindler

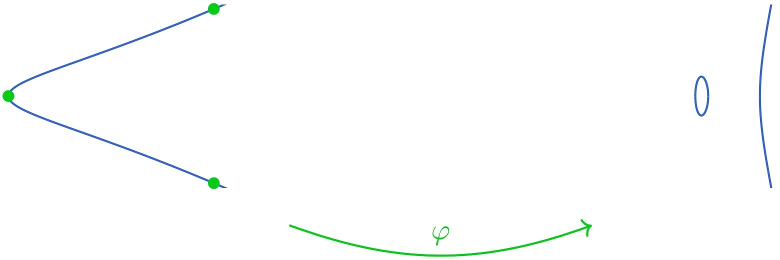
Marzio Mula • May 23, 2025

Research Institute
Cyber Defence
Universität der Bundeswehr München

An isogeny is a map between elliptic curves.

$E : y^2 = x^3 + 13x - 34$

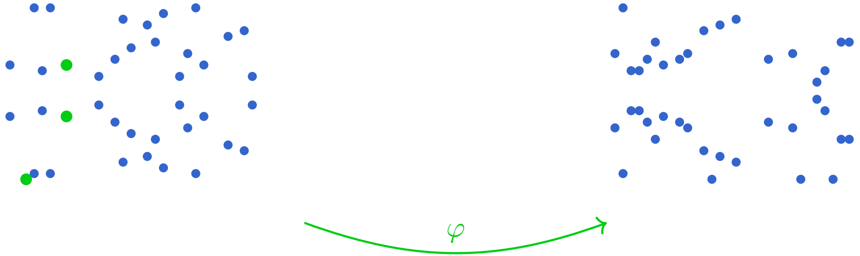
$E' : y^2 = x^3 - 7x - 6$



An isogeny is a map between elliptic curves.

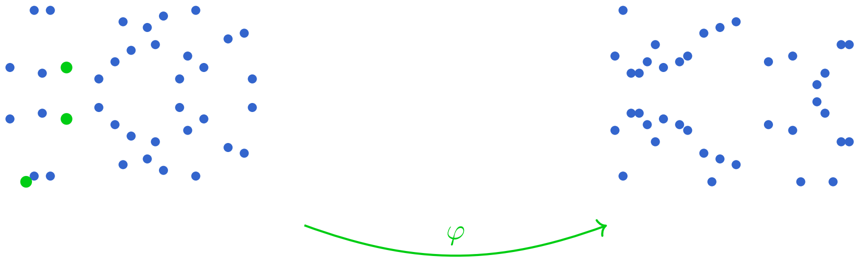
$E : y^2 = x^3 + 13x - 34$

$E' : y^2 = x^3 - 7x - 6$



An isogeny is a map between elliptic curves.

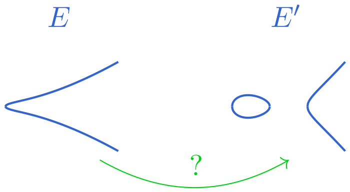
$E : y^2 = x^3 + 13x - 34$ $\qquad$ $E' : y^2 = x^3 - 7x - 6$



The **degree** of a (separable) isogeny is the cardinality of its kernel.

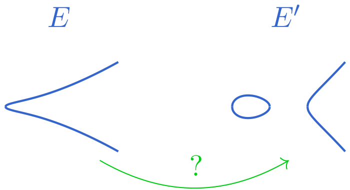
$$p = \text{a prime of cryptographic size}$$
$$E, E' = \text{supersingular elliptic curves over } \mathbb{F}_{p^2}$$

Problem (IsogenyPath): Given E and E', find an isogeny $\varphi\colon E \to E'$.



$$p = \text{a prime of cryptographic size}$$
$$E, E' = \text{supersingular elliptic curves over } \mathbb{F}_{p^2}$$

Problem (ISOGENYPATH): Given E and E', find an isogeny $\varphi\colon E \to E'$.

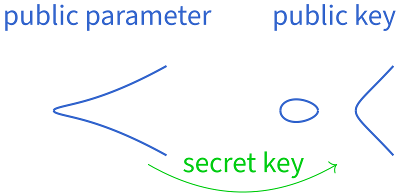


ISOGENYPATH is considered hard even for quantum computers.

A HARD MATHEMATICAL PROBLEM

$$p = \text{a prime of cryptographic size}$$
$$E, E' = \text{supersingular elliptic curves over } \mathbb{F}_{p^2}$$

Problem (ISOGENYPATH): Given E and E', find an isogeny $\varphi\colon E \to E'$.



ISOGENYPATH is considered hard even for quantum computers.

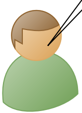
$$\Downarrow$$

Can be used for **post-quantum cryptography**!

- Key exchanges (CSIDH, SCALLOP, SCALLOP HD...)
- Signatures (SQIsign, PRISM)

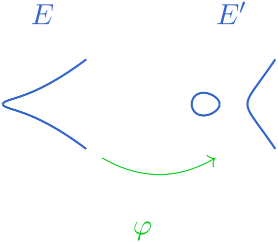
Proving knowledge of an isogeny

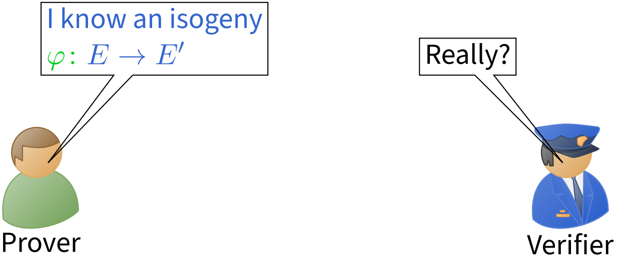
I know an isogeny
$\varphi\colon E \to E'$

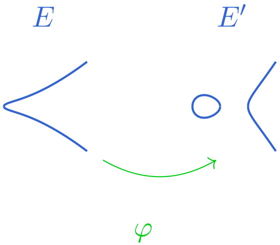


Prover

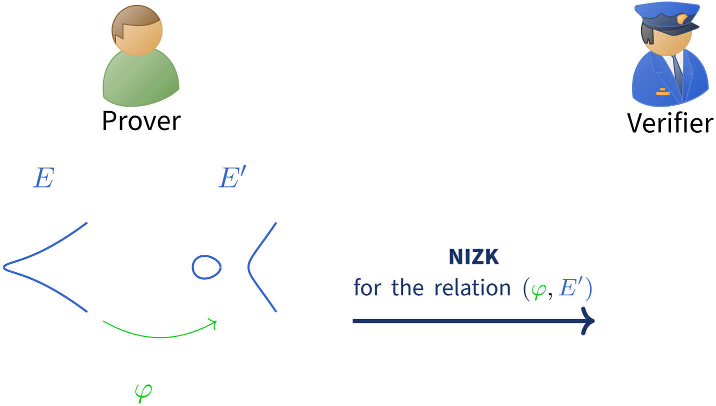
Verifier



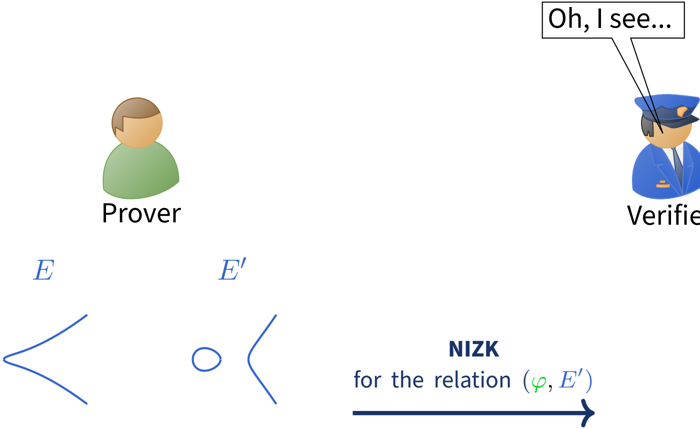

I know an isogeny
$\varphi\colon E \to E'$
Really?
Prover
Verifier


E
E'
φ

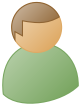
Proving knowledge of an isogeny



Proving knowledge of an isogeny



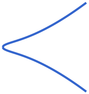
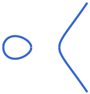
NIZK (Non-interactive zero-knowledge proof): proving knowledge of the witness corresponding to a given statement...



Prover

Verifier

E $\qquad\qquad$ E'

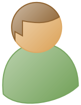
 

NIZK

for the relation (φ, E')

NIZK (Non-interactive zero-knowledge proof): proving knowledge of the witness corresponding to a given statement...

...without revealing the witness



Prover

Verifier

NIZK

for the relation (φ, E') $\longrightarrow$

NIZK (Non-interactive zero-knowledge proof): proving knowledge of the witness corresponding to a given statement...

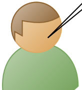
...without interacting with the verifier

Rank-1 Constraint Systems (R1CS)

A class of relations (statement, witness) that are ‘easy’ to prove:

I know a vector $(w_1, \ldots, w_n)$ such that

$$\begin{pmatrix} & & \\ & A & \\ & & \end{pmatrix} \begin{pmatrix} 1 \\ w_1 \\ w_2 \\ \vdots \\ w_n \end{pmatrix} \cdot \begin{pmatrix} & & \\ & B & \\ & & \end{pmatrix} \begin{pmatrix} 1 \\ w_1 \\ w_2 \\ \vdots \\ w_n \end{pmatrix} = \begin{pmatrix} & & \\ & C & \\ & & \end{pmatrix} \begin{pmatrix} 1 \\ w_1 \\ w_2 \\ \vdots \\ w_n \end{pmatrix}$$

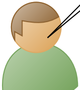


Rank-1 Constraint Systems (R1CS)

A class of relations (statement, witness) that are ‘easy’ to prove:

I know a vector $(w_1, \ldots, w_n)$ such that

$$\begin{pmatrix} \quad A \quad \end{pmatrix}\begin{pmatrix} 1 \\ w_1 \\ w_2 \\ \vdots \\ w_n \end{pmatrix} \cdot \begin{pmatrix} \quad B \quad \end{pmatrix}\begin{pmatrix} 1 \\ w_1 \\ w_2 \\ \vdots \\ w_n \end{pmatrix} = \begin{pmatrix} \quad C \quad \end{pmatrix}\begin{pmatrix} 1 \\ w_1 \\ w_2 \\ \vdots \\ w_n \end{pmatrix}$$



Idea (Cong, Lai, Levin): translate the isogeny relation into an R1CS

The isogeny relation

$$E, E' = \text{Elliptic curves over } \mathbb{F}_q$$
$$\varphi\colon E \to E' = \text{Isogeny of degree } d$$

I know φ

The isogeny relation

$$E, E' = \text{Elliptic curves over } \mathbb{F}_q$$
$$\varphi\colon E \to E' = \text{Isogeny of degree } d$$

I know φ

=

I know an *efficient representation* of φ

The isogeny relation

$$E, E' = \text{Elliptic curves over } \mathbb{F}_q$$
$$\varphi\colon E \to E' = \text{Isogeny of degree } d$$

I know φ

=

I know an *efficient representation* of φ

=

I know an algorithm that, on input $P \in E(\mathbb{F}_q)$, outputs $\varphi(P)$ in time $O(\log q \log d)$

THE ISOGENY RELATION

$$E, E' = \text{Elliptic curves over } \mathbb{F}_q$$
$$\varphi\colon E \to E' = \text{Isogeny of degree } d$$

I know φ

=

I know an *efficient representation* of φ

=

I know an algorithm that, on input $P \in E(\mathbb{F}_q)$, outputs $\varphi(P)$ in time $O(\log q \log d)$

THEOREM (ROBERT)

Every isogeny admits an efficient representation.

$$E, E' = \text{Elliptic curves over } \mathbb{F}_q$$
$$\varphi\colon E \to E' = \text{Isogeny of degree } d$$

I know φ

=

I know an *efficient representation* of φ

=

I know an algorithm that, on input $P \in E(\mathbb{F}_q)$, outputs $\varphi(P)$ in time $O(\log q \log d)$

THEOREM (ROBERT)

Every isogeny admits an efficient representation.

Our work: we consider the case $d = \ell^n$ and E, E' supersingular.

Ways to represent an ℓ^n-isogeny

- the rational functions defining φ

- (Generators of) the kernel of φ

- Factor φ as a chain of ℓ-isogenies $\varphi_n \circ \cdots \circ \varphi_1$

- The j-invariants of the codomains of $\varphi_n, \ldots, \varphi_1$

Ways to represent an ℓ^n-isogeny

Example: over $\mathbb{F}_{107}$, the 3^3-isogeny

$$\underbrace{(y^2 = x^3 + x)}_{E} \xrightarrow{\varphi} \underbrace{(y^2 = x^3 + 55x + 89}_{E'}$$

- the rational functions defining φ

- (Generators of) the kernel of φ

- Factor φ as a chain of ℓ-isogenies $\varphi_n \circ \cdots \circ \varphi_1$

- The j-invariants of the codomains of $\varphi_n, \ldots, \varphi_1$

Ways to represent an ℓ^n-isogeny

Example: over $\mathbb{F}_{107}$, the 3^3-isogeny

$$\underbrace{(y^2 = x^3 + x)}_{E} \xrightarrow{\varphi} \underbrace{(y^2 = x^3 + 55x + 89)}_{E'}$$

- the rational functions defining φ

$$\varphi\colon (x, y) \mapsto \left(\frac{x^{27} + 104x^{26} + \dots}{x^{26} + 104x^{25} + \dots}, \frac{x^{39}y + 49x^{38}y + \dots}{x^{39} + 49x^{38} + \dots} \right)$$

- (Generators of) the kernel of φ

- Factor φ as a chain of ℓ-isogenies $\varphi_n \circ \cdots \circ \varphi_1$

- The j-invariants of the codomains of $\varphi_n, \dots, \varphi_1$

Ways to represent an ℓ^n-isogeny

Example: over $\mathbb{F}_{107}$, the 3^3-isogeny

$$\underbrace{(y^2 = x^3 + x)}_{E} \xrightarrow{\varphi} \underbrace{(y^2 = x^3 + 55x + 89}_{E'}$$

- the rational functions defining φ

$$\varphi\colon (x,y) \mapsto \left(\frac{x^{27} + 104x^{26} + \dots}{x^{26} + 104x^{25} + \dots}, \frac{x^{39}y + 49x^{38}y + \dots}{x^{39} + 49x^{38} + \dots} \right)$$

- (Generators of) the kernel of φ

$$\ker\varphi = \{\text{roots of } x^{26} + 104x^{25} + \dots\} = \langle (3,43) \rangle$$

- Factor φ as a chain of ℓ-isogenies $\varphi_n \circ \cdots \circ \varphi_1$

- The j-invariants of the codomains of $\varphi_n, \dots, \varphi_1$

Ways to represent an ℓ^n-isogeny

Example: over $\mathbb{F}_{107}$, the 3^3-isogeny

$$\underbrace{(y^2 = x^3 + x)}_{E} \xrightarrow{\varphi} \underbrace{(y^2 = x^3 + 55x + 89}_{E'}$$

- the rational functions defining φ

$$\varphi\colon (x,y) \mapsto \left(\frac{x^{27} + 104x^{26} + \dots}{x^{26} + 104x^{25} + \dots}, \frac{x^{39}y + 49x^{38}y + \dots}{x^{39} + 49x^{38} + \dots} \right)$$

- (Generators of) the kernel of φ

$$\ker\varphi = \{\text{roots of } x^{26} + 104x^{25} + \dots\} = \langle (3, 43) \rangle$$

- Factor φ as a chain of ℓ-isogenies $\varphi_n \circ \cdots \circ \varphi_1$

$$E \xrightarrow{\varphi_1} (y^2 = x^3 + 89x + 89) \xrightarrow{\varphi_2} (y^2 = x^3 + 86x + 23) \xrightarrow{\varphi_3} E'$$

- The j-invariants of the codomains of $\varphi_n, \dots, \varphi_1$

Example: over $\mathbb{F}_{107}$, the 3^3-isogeny

$$\underbrace{(y^2 = x^3 + x)}_{E} \xrightarrow{\varphi} \underbrace{(y^2 = x^3 + 55x + 89}_{E'}$$

- the rational functions defining φ

$$\varphi\colon (x, y) \mapsto \left(\frac{x^{27} + 104x^{26} + \dots}{x^{26} + 104x^{25} + \dots}, \frac{x^{39}y + 49x^{38}y + \dots}{x^{39} + 49x^{38} + \dots} \right)$$

- (Generators of) the kernel of φ

$$\ker \varphi = \{\text{roots of } x^{26} + 104x^{25} + \dots\} = \langle (3, 43) \rangle$$

- Factor φ as a chain of ℓ-isogenies $\varphi_n \circ \dots \circ \varphi_1$

$$E \xrightarrow{\varphi_1} (y^2 = x^3 + 89x + 89) \xrightarrow{\varphi_2} (y^2 = x^3 + 86x + 23) \xrightarrow{\varphi_3} E'$$

- The j-invariants of the codomains of $\varphi_n, \dots, \varphi_1$

$$16 \xrightarrow{\varphi_1} 47 \xrightarrow{\varphi_2} 81 \xrightarrow{\varphi_3} 94$$

Ways to represent an ℓ^n-isogeny

Example: over $\mathbb{F}_{107}$, the 3^3-isogeny

$$\underbrace{(y^2 = x^3 + x)}_{E} \xrightarrow{\varphi} \underbrace{(y^2 = x^3 + 55x + 89)}_{E'}$$

- the rational functions defining φ

$$\varphi\colon (x,y) \mapsto \left(\frac{x^{27} + 104x^{26} + \dots}{x^{26} + 104x^{25} + \dots}, \frac{x^{39}y + 49x^{38}y + \dots}{x^{39} + 49x^{38} + \dots} \right)$$

- (Generators of) the kernel of φ

$$\ker \varphi = \{\text{roots of } x^{26} + 104x^{25} + \dots\} = \langle (3, 43) \rangle$$

- Factor φ as a chain of ℓ-isogenies $\varphi_n \circ \dots \circ \varphi_1$

$$E \xrightarrow{\varphi_1} (y^2 = x^3 + 89x + 89) \xrightarrow{\varphi_2} (y^2 = x^3 + 86x + 23) \xrightarrow{\varphi_3} E'$$

- The j-invariants of the codomains of $\varphi_n, \dots, \varphi_1$

$$16 \xrightarrow{\varphi_1} 47 \xrightarrow{\varphi_2} 81 \xrightarrow{\varphi_3} 94$$

Bottom line

The prover can represent his witness ℓ^n-isogeny as a chain of j-invariants

$$j_0 = j(E) \xrightarrow{\varphi_1} j_1 \xrightarrow{\varphi_2} j_2 \xrightarrow{\varphi_3} \dots \xrightarrow{\varphi_n} j_n = j(E')$$

Bottom line

The prover can represent his witness ℓ^n-isogeny as a chain of j-invariants

$$j_0 = j(E) \xrightarrow{\varphi_1} j_1 \xrightarrow{\varphi_2} j_2 \xrightarrow{\varphi_3} \dots \xrightarrow{\varphi_n} j_n = j(E')$$

Goal: plugging $j_0, j_1, \dots, j_n$ in an R1CS

$$\left(\underset{?}{\mathsf{A}}\right)\begin{pmatrix} 1 \\ w_1 \\ \vdots \\ w_n \end{pmatrix} \cdot \left(\underset{?}{\mathsf{B}}\right)\begin{pmatrix} 1 \\ w_1 \\ \vdots \\ w_n \end{pmatrix} = \left(\underset{?}{\mathsf{C}}\right)\begin{pmatrix} 1 \\ w_1 \\ \vdots \\ w_n \end{pmatrix}$$

Bottom line

The prover can represent his witness ℓ^n-isogeny as a chain of j-invariants

$$j_0 = j(E) \xrightarrow{\varphi_1} j_1 \xrightarrow{\varphi_2} j_2 \xrightarrow{\varphi_3} \dots \xrightarrow{\varphi_n} j_n = j(E')$$

Goal: plugging $j_0, j_1, \dots, j_n$ in an R1CS

$$\left(\underset{?}{\mathsf{A}} \right) \begin{pmatrix} 1 \\ w_1 \\ \vdots \\ w_n \end{pmatrix} \cdot \left(\underset{?}{\mathsf{B}} \right) \begin{pmatrix} 1 \\ w_1 \\ \vdots \\ w_n \end{pmatrix} = \left(\underset{?}{\mathsf{C}} \right) \begin{pmatrix} 1 \\ w_1 \\ \vdots \\ w_n \end{pmatrix}$$

To do so, we need equations involving $j_0, j_1, \dots, j_n$:

- Cong, Lai, Levin: classical modular polynomials.
- Our work: other modular polynomials.

Classical modular polynomial for $\ell = 2$

$$\Phi_2(X,Y) = X^3 + Y^3 - \underbrace{162000}_{c_2}(X^2+Y^2) + \underbrace{1488}_{c_4} XY(X+Y) +$$
$$-X^2Y^2 + \underbrace{8748000000}_{c_1}(X+Y) + \underbrace{40773375}_{c_3} XY \underbrace{-157464000000000}_{c_0}$$

Theorem

There is a 2-isogeny $j_i \to j_{i+1} \quad \iff \quad \Phi_2(j_i, j_{i+1}) = 0$

Classical modular polynomial for $\ell = 2$

$$\Phi_2(X,Y) = X^3 + Y^3 - \underbrace{162000}_{c_2}(X^2+Y^2) + \underbrace{1488}_{c_4} XY(X+Y) +$$
$$-X^2Y^2 + \underbrace{8748000000}_{c_1}(X+Y) + \underbrace{40773375}_{c_3} XY \underbrace{-157464000000000}_{c_0}$$

Theorem

There is a 2-isogeny $j_i \to j_{i+1} \quad \Longleftrightarrow \quad \Phi_2(j_i, j_{i+1}) = 0$

Therefore, for a 2^n-isogeny...

$$j_0 = j(E) \xrightarrow{\varphi_1} j_1 \xrightarrow{\varphi_2} j_2 \xrightarrow{\varphi_3} \cdots \xrightarrow{\varphi_n} j_n = j(E')$$

Classical modular polynomial for $\ell = 2$

$$\Phi_2(X,Y) = X^3 + Y^3 - \underbrace{162000}_{c_2}(X^2+Y^2) + \underbrace{1488}_{c_4} XY(X+Y) +$$
$$-X^2Y^2 + \underbrace{8748000000}_{c_1}(X+Y) + \underbrace{40773375}_{c_3} XY \underbrace{-157464000000000}_{c_0}$$

Theorem

There is a 2-isogeny $j_i \to j_{i+1}$ $\iff$ $\Phi_2(j_i, j_{i+1}) = 0$

Therefore, for a 2^n-isogeny...

$$j_0 = j(E) \xrightarrow{\varphi_1} j_1 \xrightarrow{\varphi_2} j_2 \xrightarrow{\varphi_3} \cdots \xrightarrow{\varphi_n} j_n = j(E')$$

$\Phi_2(j_0, j_1) = 0$

Classical modular polynomial for $\ell = 2$

$$\Phi_2(X,Y) = X^3 + Y^3 - \underbrace{162000}_{c_2}(X^2+Y^2) + \underbrace{1488}_{c_4} XY(X+Y) +$$
$$-X^2Y^2 + \underbrace{8748000000}_{c_1}(X+Y) + \underbrace{40773375}_{c_3} XY \underbrace{-157464000000000}_{c_0}$$

Theorem

There is a 2-isogeny $j_i \to j_{i+1} \iff \Phi_2(j_i, j_{i+1}) = 0$

Therefore, for a 2^n-isogeny...

$$j_0 = j(E) \xrightarrow{\varphi_1} j_1 \xrightarrow{\varphi_2} j_2 \xrightarrow{\varphi_3} \cdots \xrightarrow{\varphi_n} j_n = j(E')$$

$$\Phi_2(j_1, j_2) = 0$$

Classical modular polynomial for $\ell = 2$

$$\Phi_2(X,Y) = X^3 + Y^3 - \underbrace{162000}_{c_2}(X^2+Y^2) + \underbrace{1488}_{c_4} XY(X+Y) +$$
$$-X^2Y^2 + \underbrace{8748000000}_{c_1}(X+Y) + \underbrace{40773375}_{c_3} XY \underbrace{-157464000000000}_{c_0}$$

Theorem

There is a 2*-isogeny* $j_i \to j_{i+1} \iff \Phi_2(j_i, j_{i+1}) = 0$

Therefore, for a 2^n-isogeny...

$$j_0 = j(E) \xrightarrow{\varphi_1} j_1 \xrightarrow{\varphi_2} j_2 \xrightarrow{\varphi_3} \cdots \xrightarrow{\varphi_n} j_n = j(E')$$

$$\Phi_2(j_2, \dots) = 0$$

CLASSICAL MODULAR POLYNOMIAL FOR $\ell = 2$

$$\Phi_2(X,Y) = X^3 + Y^3 - \underbrace{162000}_{c_2}(X^2+Y^2) + \underbrace{1488}_{c_4}XY(X+Y) +$$
$$-X^2Y^2 + \underbrace{8748000000}_{c_1}(X+Y) + \underbrace{40773375}_{c_3}XY \underbrace{-157464000000000}_{c_0}$$

THEOREM

There is a 2-isogeny $j_i \to j_{i+1} \iff \Phi_2(j_i, j_{i+1}) = 0$

Therefore, for a 2^n-isogeny...

$$j_0 = j(E) \xrightarrow{\varphi_1} j_1 \xrightarrow{\varphi_2} j_2 \xrightarrow{\varphi_3} \cdots \xrightarrow{\varphi_n} j_n = j(E')$$

$$\Phi_2(j_{n-1}, j_n) = 0$$

Classical modular polynomial for any ℓ

$$\Phi_\ell(X,Y) = X^{\ell+1} + Y^{\ell+1} + \text{polynomial symmetric in } X \text{ and } Y$$
$$\text{with very large integer coefficients}$$

Theorem

There is an ℓ-isogeny $j_i \to j_{i+1}$ $\iff$ $\Phi_\ell(j_i, j_{i+1}) = 0$

Therefore, for an ℓ^n-isogeny...

$$j_0 = j(E) \xrightarrow{\varphi_1} j_1 \xrightarrow{\varphi_2} j_2 \xrightarrow{\varphi_3} \cdots \xrightarrow{\varphi_n} j_n = j(E')$$

$$\Phi_\ell(j_{n-1}, j_n) = 0$$

$$(\mathsf{A})\begin{pmatrix}1\\ w_1\\ \vdots\\ w_n\end{pmatrix}\cdot(\mathsf{B})\begin{pmatrix}1\\ w_1\\ \vdots\\ w_n\end{pmatrix}= \\ =(\mathsf{C})\begin{pmatrix}1\\ w_1\\ \vdots\\ w_n\end{pmatrix}$$

Cong, Lai, Levin: R1CS via classical modular polynomial

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ j_i \\ j_{i+1} \\ j_i^2 \\ j_{i+1}^2 \\ j_i^3 \\ j_{i+1}^3 \\ j_i j_{i+1} \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & c_4 & c_4 & 0 & 0 & 0 & 0 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ j_i \\ j_{i+1} \\ j_i^2 \\ j_{i+1}^2 \\ j_i^3 \\ j_{i+1}^3 \\ j_i j_{i+1} \end{pmatrix} =$$

$$= \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ c_0 & c_1 & c_1 & c_2 & c_2 & 1 & 1 & c_3 \end{pmatrix} \begin{pmatrix} 1 \\ j_i \\ j_{i+1} \\ j_i^2 \\ j_{i+1}^2 \\ j_i^3 \\ j_{i+1}^3 \\ j_i j_{i+1} \end{pmatrix}$$

...for each i in $\{0, \ldots, n-1\}$

OUR WORK: FROM CLASSICAL TO CANONICAL MODULAR POLYNOMIALS

For $\ell \in \{2, 3, 5, 7, 13\}$, we consider the *canonical polynomials* constructed by Müller

$$\Phi_2^c(f,j) = f^3 + 48f^2 + 768f + 4096 - f \cdot j$$

$$\Phi_3^c(f,j) = f^4 + 36f^3 + 270f^2 + 756f + 729 - f \cdot j$$

$$\Phi_5^c(f,j) = f^6 + 30f^5 + 315f^4 + 1300f^3 + 1575f^2 + 750f + \\ + 125 - f \cdot j$$

$$\Phi_7^c(f,j) = f^8 + 28f^7 + 322f^6 + 1904f^5 + 5915f^4 + 8624f^3 + \\ + 4018f^2 + 748f + 49 - f \cdot j$$

$$\Phi_{13}^c(f,j) = f^{14} + 26f^{13} + 325f^{12} + 2548f^{11} + 13832f^{10} + \\ + 54340f^9 + 157118f^8 + 333580f^7 + 509366f^6 + \\ + 534820f^5 + 354536f^4 + 124852f^3 + 15145f^2 + \\ + 746f + 13 - f \cdot j$$

For $\boldsymbol{\ell} \in \{\mathbf{2, 3, 5, 7, 13}\}$, we consider the *canonical polynomials* constructed by Müller

$$\Phi_3^c(f, j) = f^4 + 36f^3 + 270f^2 + 756f + 729 - f \cdot j$$

For comparison, the 3rd classical modular polynomial is

$$\begin{aligned}\Phi_3(X, Y) = -X^3Y^3 + X^4 + Y^4 + 2232(X^3Y^2 + X^2Y^3)\\ - 1069956(X^3Y + XY^3) + 36864000(X^3 + Y^3)\\ + 2587918086X^2Y^2 + 8900222976000(X^2Y + XY^2)\\ + 452984832000000(X^2 + Y^2) - 770845966336000000XY\\ + 1855425871872000000000(X + Y)\end{aligned}$$

Our work: from classical to canonical modular polynomials

For $\boldsymbol{\ell \in \{2, 3, 5, 7, 13\}}$, we consider the *canonical polynomials* constructed by Müller

$$\Phi_3^c(f, j) = f^4 + 36f^3 + 270f^2 + 756f + 729 - f \cdot j$$

For comparison, the 3rd classical modular polynomial is

$$\begin{aligned}
\Phi_3(X, Y) = -X^3Y^3 + X^4 + Y^4 + 2232(X^3Y^2 + X^2Y^3) \\
- 1069956(X^3Y + XY^3) + 36864000(X^3 + Y^3) \\
+ 2587918086X^2Y^2 + 8900222976000(X^2Y + XY^2) \\
+ 452984832000000(X^2 + Y^2) - 770845966336000000XY \\
+ 1855425871872000000000(X + Y)
\end{aligned}$$

Sparser polynomials $\longrightarrow$ Sparser A, B, C $\longrightarrow$ Faster prover time

Sparser polynomials $\longrightarrow$ Less rows in A, B, C $\longrightarrow$ Smaller proof size and prover/verifier time

Our main results on canonical modular polynomials

- How does Φ_ℓ^c encode isogenies?

Theorem

Let $\boldsymbol{\ell \in \{2, 3, 5, 7, 13\}}$ *and* $s = \frac{12}{\gcd(12,\ell-1)}$.

There is an ℓ-isogeny $j_i \to j_{i+1}$

$$\Updownarrow$$

There exists $f_i \in \overline{\mathbb{F}_p}^\times$ *s.t.* $\begin{cases} \Phi_\ell^c(f_i, j_i) = 0 \\ \Phi_\ell^c(\ell^s/f_i, j_{i+1}) = 0 \end{cases}$

OUR MAIN RESULTS ON CANONICAL MODULAR POLYNOMIALS

- How does Φ_ℓ^c encode isogenies?

THEOREM

Let $\boldsymbol{\ell \in \{2, 3, 5, 7, 13\}}$ *and* $s = \frac{12}{\gcd(12, \ell-1)}$.

There is an ℓ*-isogeny* $j_i \to j_{i+1}$

$$\Updownarrow$$

There exists $f_i \in \overline{\mathbb{F}_p}^\times$ *s.t.* $\begin{cases} \Phi_\ell^c(f_i, j_i) = 0 \\ \Phi_\ell^c(\ell^s/f_i, j_{i+1}) = 0 \end{cases}$

$$j_0 = j(E) \xrightarrow{\varphi_1} j_1 \xrightarrow{\varphi_2} j_2 \xrightarrow{\varphi_3} \cdots \xrightarrow{\varphi_n} j_n = j(E')$$

$$\begin{cases} \Phi_\ell^c(f_0, j_0) = 0 \\ \Phi_\ell^c(\ell^s/f_0, j_1) = 0 \end{cases}$$

Our main results on canonical modular polynomials

- How does Φ_ℓ^c encode isogenies?

Theorem

Let $\ell \in \{\mathbf{2}, \mathbf{3}, \mathbf{5}, \mathbf{7}, \mathbf{13}\}$ *and* $s = \frac{12}{\gcd(12,\ell-1)}$.

There is an ℓ*-isogeny* $j_i \to j_{i+1}$

$$\Updownarrow$$

There exists $f_i \in \overline{\mathbb{F}_p}^\times$ *s.t.* $\begin{cases} \Phi_\ell^c(f_i, j_i) = 0 \\ \Phi_\ell^c(\ell^s/f_i, j_{i+1}) = 0 \end{cases}$

$$j_0 = j(E) \xrightarrow{\varphi_1} j_1 \xrightarrow{\varphi_2} j_2 \xrightarrow{\varphi_3} \cdots \xrightarrow{\varphi_n} j_n = j(E')$$

$$\begin{cases} \Phi_\ell^c(f_1, j_1) = 0 \\ \Phi_\ell^c(\ell^s/f_1, j_2) = 0 \end{cases}$$

Our main results on canonical modular polynomials

- How does Φ_ℓ^c encode isogenies?

Theorem

Let $\boldsymbol{\ell \in \{2, 3, 5, 7, 13\}}$ *and* $s = \frac{12}{\gcd(12, \ell - 1)}$.

There is an ℓ*-isogeny* $j_i \to j_{i+1}$

$$\Updownarrow$$

There exists $f_i \in \overline{\mathbb{F}_p}^\times$ *s.t.* $\begin{cases} \Phi_\ell^c(f_i, j_i) = 0 \\ \Phi_\ell^c(\ell^s / f_i, j_{i+1}) = 0 \end{cases}$

$$j_0 = j(E) \xrightarrow{\varphi_1} j_1 \xrightarrow{\varphi_2} j_2 \xrightarrow{\varphi_3} \cdots \xrightarrow{\varphi_n} j_n = j(E')$$

$$\begin{cases} \Phi_\ell^c(f_2, j_2) = 0 \\ \Phi_\ell^c(\ell^s / f_2, \dots) = 0 \end{cases}$$

Our main results on canonical modular polynomials

- How does Φ_ℓ^c encode isogenies?

Theorem

Let $\ell \in \{\mathbf{2}, \mathbf{3}, \mathbf{5}, \mathbf{7}, \mathbf{13}\}$ *and* $s = \frac{12}{\gcd(12, \ell-1)}$.

There is an ℓ*-isogeny* $j_i \to j_{i+1}$

$$\Updownarrow$$

There exists $f_i \in \overline{\mathbb{F}_p}^\times$ *s.t.* $\begin{cases} \Phi_\ell^c(f_i, j_i) = 0 \\ \Phi_\ell^c(\ell^s/f_i, j_{i+1}) = 0 \end{cases}$

$$j_0 = j(E) \xrightarrow{\varphi_1} j_1 \xrightarrow{\varphi_2} j_2 \xrightarrow{\varphi_3} \cdots \xrightarrow{\varphi_n} j_n = j(E')$$

$$\begin{cases} \Phi_\ell^c(f_{n-1}, j_{n-1}) = 0 \\ \Phi_\ell^c(\ell^s/f_{n-1}, j_n) = 0 \end{cases}$$

OUR MAIN RESULTS ON CANONICAL MODULAR POLYNOMIALS

- How does Φ_ℓ^c encode isogenies?

THEOREM

Let $\boldsymbol{\ell} \in \{\mathbf{2, 3, 5, 7, 13}\}$ *and* $s = \frac{12}{\gcd(12, \ell-1)}$.

There is an ℓ-isogeny $j_i \to j_{i+1}$

$$\Updownarrow$$

There exists $f_i \in \overline{\mathbb{F}_p}^\times$ *s.t.* $\begin{cases} \Phi_\ell^c(f_i, j_i) = 0 \\ \Phi_\ell^c(\ell^s/f_i, j_{i+1}) = 0 \end{cases}$

- Where does f_i live?

THEOREM

Let $\boldsymbol{\ell} \in \{\mathbf{2, 3, 5, 7, 13}\}$*. If* j_i *is supersingular, then* $\Phi_\ell^c(f, j_i)$ *splits over* $\mathbb{F}_{p^2}$*.*

R1CS: CLASSICAL VS CANONICAL

Cong, Lai, Levin: $\ell = 2$ with classical modular polynomials

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ j_i \\ j_{i+1} \\ j_i^2 \\ j_{i+1}^2 \\ j_i^3 \\ j_{i+1}^3 \\ j_i j_{i+1} \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & c_4 & c_4 & 0 & 0 & 0 & 0 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ j_i \\ j_{i+1} \\ j_i^2 \\ j_{i+1}^2 \\ j_i^3 \\ j_{i+1}^3 \\ j_i j_{i+1} \end{pmatrix} =$$

$$= \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ c_0 & c_1 & c_1 & c_2 & c_2 & 1 & 1 & c_3 \end{pmatrix} \begin{pmatrix} 1 \\ j_i \\ j_{i+1} \\ j_i^2 \\ j_{i+1}^2 \\ j_i^3 \\ j_{i+1}^3 \\ j_i j_{i+1} \end{pmatrix}$$

...for each i in $\{0, \ldots, n-1\}$

Our work: $\ell = 2$ with canonical modular polynomials

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ f_i \\ f_i^2 \\ j_i - c'_1 \\ j_{i+1} - c'_1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & c'_2 & c'_3 & -1 & 0 \\ 0 & c''_3 & 0 & 0 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ f_i \\ f_i^2 \\ j_i - c'_1 \\ j_{i+1} - c'_1 \end{pmatrix} =$$

$$= \begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ -c'_0 & 0 & 0 & 0 & 0 \\ -c''_0 & -c''_1 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ f_i \\ f_i^2 \\ j_i - c'_1 \\ j_{i+1} - c'_1 \end{pmatrix}$$

...for each i in $\{0, \ldots, n-1\}$
(and c'_k, c''_k obtained from the coefficients of $\Phi_2^c(f, X)$)

For $\ell \in \{\mathbf{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 41, 47, 59, 71}\}$, we consider the Atkin modular polynomials:

$$\begin{aligned}\Phi_2^{\mathsf{A}}(f,j) &= j^2 - j(f^2 + f - 7256) + f^3 + 744f^2 + 184512f + \\ &+ 15252992 \\ \Phi_3^{\mathsf{A}}(f,j) &= j^2 - j(f^3 - 2348f - 24528) + f^4 + 744f^3 + \\ &+ 193752f^2 + 19712160f + 538141968\end{aligned}$$

$$\vdots$$

$$\Phi_\ell^{\mathsf{A}}(f,j) = j^2 - j \cdot \left(f^\ell + \sum_{i=0}^{\ell-1} a_{\ell,i} f^i\right) + f^{\ell+1} + \sum_{i=0}^{\ell} b_{\ell,i} f^i$$

Our work (in progress): Atkin modular polynomials

For $\ell \in \{\mathbf{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 41, 47, 59, 71}\}$, we consider the Atkin modular polynomials:

$$\begin{aligned}\Phi_2^{\mathsf{A}}(f,j) &= j^2 - j(f^2 + f - 7256) + f^3 + 744f^2 + 184512f + \\ &+ 15252992 \\ \Phi_3^{\mathsf{A}}(f,j) &= j^2 - j(f^3 - 2348f - 24528) + f^4 + 744f^3 + \\ &+ 193752f^2 + 19712160f + 538141968 \\ &\vdots \\ \Phi_\ell^{\mathsf{A}}(f,j) &= j^2 - j \cdot \left(f^\ell + \sum_{i=0}^{\ell-1} a_{\ell,i} f^i \right) + f^{\ell+1} + \sum_{i=0}^{\ell} b_{\ell,i} f^i\end{aligned}$$

We also consider the difference quotient polynomial

$$\delta_\ell(f, j_0, j_1) = \frac{\Phi_\ell^{\mathsf{A}}(f, j_1) - \Phi_\ell^{\mathsf{A}}(f, j_0)}{j_1 - j_0} = j_0 + j_1 - \left(f^\ell + \sum_{i=0}^{\ell-1} a_{\ell,i} f^i \right)$$

- How does Φ_ℓ^A encode isogenies?

Theorem

Let $\ell \in \{\mathbf{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 41, 47, 59, 71}\}$.

There is an ℓ*-isogeny* $j_i \to j_{i+1}$

$$\Updownarrow$$

There exists $f_i \in \overline{\mathbb{F}_p}^\times$ *s.t.* $\begin{cases} \Phi_\ell^A(f_i, j_i) = 0 \\ \delta_\ell(f_i, j_i, j_{i+1}) = 0 \end{cases}$

Our results on Atkin modular polynomials

- How does Φ_ℓ^A encode isogenies?

Theorem

Let $\ell \in \{\mathbf{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 41, 47, 59, 71}\}$.

There is an ℓ*-isogeny* $j_i \to j_{i+1}$

$$\Updownarrow$$

There exists $f_i \in \overline{\mathbb{F}_p}^\times$ *s.t.* $\begin{cases} \Phi_\ell^A(f_i, j_i) = 0 \\ \delta_\ell(f_i, j_i, j_{i+1}) = 0 \end{cases}$

$$j_0 = j(E) \xrightarrow{\varphi_1} j_1 \xrightarrow{\varphi_2} j_2 \xrightarrow{\varphi_3} \cdots \xrightarrow{\varphi_n} j_n = j(E')$$

$$\begin{cases} \Phi_\ell^A(f_0, j_0) = 0 \\ \delta_\ell(f_0, j_0, j_1) = 0 \end{cases}$$

Our results on Atkin modular polynomials

- How does Φ_ℓ^A encode isogenies?

Theorem

Let $\ell \in \{\mathbf{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 41, 47, 59, 71}\}$.

There is an ℓ*-isogeny* $j_i \to j_{i+1}$

$$\Updownarrow$$

There exists $f_i \in \overline{\mathbb{F}_p}^\times$ *s.t.* $\begin{cases} \Phi_\ell^A(f_i, j_i) = 0 \\ \delta_\ell(f_i, j_i, j_{i+1}) = 0 \end{cases}$

$$j_0 = j(E) \xrightarrow{\varphi_1} j_1 \xrightarrow{\varphi_2} j_2 \xrightarrow{\varphi_3} \cdots \xrightarrow{\varphi_n} j_n = j(E')$$

$$\begin{cases} \Phi_\ell^A(f_1, j_1) = 0 \\ \delta_\ell(f_1, j_1, j_2) = 0 \end{cases}$$

Our results on Atkin modular polynomials

- How does Φ_ℓ^A encode isogenies?

Theorem

Let $\ell \in \{\mathbf{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 41, 47, 59, 71}\}$.

There is an ℓ-isogeny $j_i \to j_{i+1}$

$$\Updownarrow$$

There exists $f_i \in \overline{\mathbb{F}_p}^\times$ s.t. $\begin{cases} \Phi_\ell^A(f_i, j_i) = 0 \\ \delta_\ell(f_i, j_i, j_{i+1}) = 0 \end{cases}$

$$j_0 = j(E) \xrightarrow{\varphi_1} j_1 \xrightarrow{\varphi_2} j_2 \xrightarrow{\varphi_3} \cdots \xrightarrow{\varphi_n} j_n = j(E')$$

$$\begin{cases} \Phi_\ell^A(f_2, j_2) = 0 \\ \delta_\ell(f_2, j_2, \dots) = 0 \end{cases}$$

Our results on Atkin modular polynomials

- How does Φ_ℓ^A encode isogenies?

Theorem

Let $\boldsymbol{\ell \in \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 41, 47, 59, 71\}}$.

There is an ℓ*-isogeny* $j_i \to j_{i+1}$

$$\Updownarrow$$

There exists $f_i \in \overline{\mathbb{F}_p}^\times$ *s.t.* $\begin{cases} \Phi_\ell^A(f_i, j_i) = 0 \\ \delta_\ell(f_i, j_i, j_{i+1}) = 0 \end{cases}$

$$j_0 = j(E) \xrightarrow{\varphi_1} j_1 \xrightarrow{\varphi_2} j_2 \xrightarrow{\varphi_3} \cdots \xrightarrow{\varphi_n} j_n = j(E')$$

$$\begin{cases} \Phi_\ell^A(f_{n-1}, j_{n-1}) = 0 \\ \delta_\ell(f_{n-1}, j_{n-1}, j_n) = 0 \end{cases}$$

Our results on Atkin modular polynomials

- How does Φ_ℓ^A encode isogenies?

Theorem

Let $\ell \in \{\mathbf{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 41, 47, 59, 71}\}$.

There is an ℓ*-isogeny* $j_i \to j_{i+1}$

$$\Updownarrow$$

There exists $f_i \in \overline{\mathbb{F}_p}^\times$ *s.t.* $\begin{cases} \Phi_\ell^A(f_i, j_i) = 0 \\ \delta_\ell(f_i, j_i, j_{i+1}) = 0 \end{cases}$

- Where does f_i live?

Conjecture: If j_i is supersingular, then $\Phi_\ell^A(f, j_i)$ splits over $\mathbb{F}_{p^2}$

Modular curves: the elephant in the room

$$\{\text{Elliptic curves}\}/\simeq \;\longleftrightarrow\; X(1)$$

$$\{\ell\text{-isogenies}\}/\sim \;\longleftrightarrow\; X_0(\ell)$$

Modular curves: the elephant in the room

$$\begin{tikzcd}
\{\text{Elliptic curves}\}/\simeq \arrow[r, leftrightarrow] & X(1) \\
\{\ell\text{-isogenies}\}/\sim \arrow[r, leftrightarrow] \arrow[u, twoheadrightarrow] & X_0(\ell) \arrow[u, twoheadrightarrow]
\end{tikzcd}$$

$$\{\text{Elliptic curves}\}/\simeq \;\longleftrightarrow\; X(1)$$

$$\begin{array}{ccc}
\begin{array}{c}\{\{\varphi,\hat{\varphi}\}\mid \\ \varphi \text{ is an } \ell\text{-isogeny}\}/\sim\end{array} & \longleftrightarrow & X_0^+(\ell) \\
\big\uparrow\!\!\!\uparrow & & \big\uparrow\!\!\!\uparrow \\
\{\ell\text{-isogenies}\}/\sim & \longleftrightarrow & X_0(\ell)
\end{array}$$

Modular curves: the elephant in the room

$$\{\text{Elliptic curves}\}/\simeq \;\longleftrightarrow\; X(1)$$

Classical mod. poly

$$\begin{array}{ccc}
\begin{array}{c}\{\{\varphi,\hat{\varphi}\} \mid \\ \varphi \text{ is an } \ell\text{-isogeny}\}/\sim\end{array} & \longleftrightarrow & X_0^+(\ell) \\
\Big\uparrow & & \Big\uparrow \\
\{\ell\text{-isogenies}\}/\sim & \longleftrightarrow & X_0(\ell)
\end{array}$$

Modular curves: the elephant in the room

$$\{\text{Elliptic curves}\}/\simeq \longleftrightarrow X(1)$$ **Classical** mod. poly

$$\begin{tikzcd}
\begin{array}{c}\{\{\varphi,\hat{\varphi}\} \mid \\ \varphi \text{ is an } \ell\text{-isogeny}\}/\sim\end{array} \arrow[r, leftrightarrow] & X_0^+(\ell) \\
\{\ell\text{-isogenies}\}/\sim \arrow[r, leftrightarrow] \arrow[u, twoheadrightarrow] & X_0(\ell) \arrow[u, twoheadrightarrow]
\end{tikzcd}$$

Canonical mod. poly

Modular curves: the elephant in the room

$$\{\text{Elliptic curves}\}/\simeq \;\longleftrightarrow\; X(1)$$

Classical mod. poly

$$\begin{tikzcd}
\{\{\varphi, \hat{\varphi}\} \mid \varphi \text{ is an } \ell\text{-isogeny}\}/\sim \arrow[r, leftrightarrow] & X_0^+(\ell) \\
\{\ell\text{-isogenies}\}/\sim \arrow[r, leftrightarrow] \arrow[u, two heads] & X_0(\ell) \arrow[u, two heads]
\end{tikzcd}$$

Atkin mod. poly

Canonical mod. poly

$$\begin{tikzcd}
\{\text{Elliptic curves}\}/\simeq \arrow[r, leftrightarrow] & X(1) & \text{Classical mod. poly} \\
\{\{\varphi,\hat{\varphi}\} \mid \varphi \text{ is an } \ell\text{-isogeny}\}/\sim \arrow[r, leftrightarrow] & X_0^+(\ell) & \text{Atkin mod. poly} \\
\{\ell\text{-isogenies}\}/\sim \arrow[r, leftrightarrow] \arrow[u, twoheadrightarrow] & X_0(\ell) \arrow[u, twoheadrightarrow] & \text{Canonical mod. poly}
\end{tikzcd}$$

Our results apply exactly when $X_0(\ell)$ (resp. $X_0^+(\ell)$) has genus 0.


Thank you for your attention!

Essential bibliography

[CLL23] K. Cong, Y.-F. Lai, and S. Levin. “Efficient Isogeny Proofs Using Generic Techniques”. In: *Applied Cryptography and Network Security*. Cham: Springer Nature Switzerland, 2023, pp. 248–275.

[Hol+] T. den Hollander et al. *More Efficient Isogeny Proofs of Knowledge via Canonical Modular Polynomials*. To appear at CRYPTO 2025. URL: https://eprint.iacr.org/2024/1738.

[Mü95] V. Müller. “Ein Algorithmus zur Bestimmung der Punktanzahl elliptischer Kurven über endlichen Körpern der Charakteristik größer drei”. PhD thesis. Universität des Saarlandes, 1995.

[Rob] D. Robert. *On the efficient representation of isogenies (a survey)*. URL: https://eprint.iacr.org/2024/1071.

ℓ	Rows		Variables		Non-zero entries	
	CLL	Ours	CLL	Ours	CLL	Ours
2	$4\lambda + 2$	3λ	$4\lambda + 3$	$3\lambda + 1$	$21\lambda + 6$	13λ
3		2.524λ		$2.524\lambda + 1$		11.357λ
5		2.584λ		$2.584\lambda + 1$		12.059λ
7		2.493λ		$2.493\lambda + 1$		12.467λ
13		2.702λ		$2.702\lambda + 1$		15.133λ

Table: Parameters of the R1CS for an ℓ-smooth isogeny of degree $\geq 2^\lambda$

Ways to represent an ℓ^n-isogeny – Example over $\mathbb{F}_{41^2}$

- the rational functions defining φ

- (Generators of) the kernel of φ + Vélu's formulae

- Factor φ as a chain of ℓ-isogenies $\varphi_n \circ \cdots \circ \varphi_1$

- The j-invariants of the codomains of $\varphi_n, \ldots, \varphi_1$

Ways to represent an ℓ^n-isogeny – Example over $\mathbb{F}_{41^2}$

Example: over $\mathbb{F}_{41^2}$, the 5^3-isogeny

$$\underbrace{(y^2 = x^3 + 1)}_{E} \xrightarrow{\varphi} \underbrace{(y^2 = x^3 + (16a + 10)x + (3a + 34))}_{E'}$$

with $(a - 22)^2 \equiv 27 \bmod 41$

- the rational functions defining φ
- (Generators of) the kernel of φ + Vélu's formulae
- Factor φ as a chain of ℓ-isogenies $\varphi_n \circ \cdots \circ \varphi_1$
- The j-invariants of the codomains of $\varphi_n, \ldots, \varphi_1$

Ways to represent an ℓ^n-isogeny – Example over $\mathbb{F}_{41^2}$

Example: over $\mathbb{F}_{41^2}$, the 5^3-isogeny

$$\underbrace{(y^2 = x^3 + 1)}_{E} \xrightarrow{\varphi} \underbrace{(y^2 = x^3 + (16a+10)x + (3a+34))}_{E'}$$

with $(a-22)^2 \equiv 27 \bmod 41$

- the rational functions defining φ

$$\varphi\colon (x,y) \mapsto \left(\frac{4x^{125} + (7a+7)\,x^{124} + \ldots}{10x^{124} + (38a+38)\,x^{123} + \ldots}, \frac{21x^{186}y + \ldots}{31x^{186} + \ldots} \right)$$

- (Generators of) the kernel of φ + Vélu's formulae
- Factor φ as a chain of ℓ-isogenies $\varphi_n \circ \cdots \circ \varphi_1$
- The j-invariants of the codomains of $\varphi_n, \ldots, \varphi_1$

Ways to represent an ℓ^n-isogeny – Example over $\mathbb{F}_{41^2}$

Example: over $\mathbb{F}_{41^2}$, the 5^3-isogeny

$$\underbrace{(y^2 = x^3 + 1)}_{E} \xrightarrow{\varphi} \underbrace{(y^2 = x^3 + (16a + 10)x + (3a + 34))}_{E'}$$

with $(a-22)^2 \equiv 27 \bmod 41$

- the rational functions defining φ

$$\varphi\colon (x,y) \mapsto \left(\frac{4x^{125} + (7a+7)\,x^{124} + \dots}{10x^{124} + (38a+38)\,x^{123} + \dots}, \frac{21x^{186}y + \dots}{31x^{186} + \dots} \right)$$

- (Generators of) the kernel of φ + Vélu's formulae

$$\ker\varphi = \{\text{roots of } x^{62} + (6a+6)\,x^{61} + \dots\} \subseteq \mathbb{F}_{41^{50}}$$

- Factor φ as a chain of ℓ-isogenies $\varphi_n \circ \dots \circ \varphi_1$

- The j-invariants of the codomains of $\varphi_n, \dots, \varphi_1$

Example: over $\mathbb{F}_{41^2}$, the 5^3-isogeny

$$\underbrace{(y^2 = x^3 + 1)}_{E} \xrightarrow{\varphi} \underbrace{(y^2 = x^3 + (16a + 10)x + (3a + 34))}_{E'}$$

with $(a - 22)^2 \equiv 27 \bmod 41$

- the rational functions defining φ

$$\varphi\colon (x, y) \mapsto \left(\frac{4x^{125} + (7a + 7)\,x^{124} + \dots}{10x^{124} + (38a + 38)\,x^{123} + \dots}, \frac{21x^{186}y + \dots}{31x^{186} + \dots} \right)$$

- (Generators of) the kernel of φ + Vélu's formulae

$$\ker\varphi = \{\text{roots of } x^{62} + (6a + 6)\,x^{61} + \dots\} \subseteq \mathbb{F}_{41^{50}}$$

- Factor φ as a chain of ℓ-isogenies $\varphi_n \circ \cdots \circ \varphi_1$

$$E \xrightarrow{\varphi_1} (y^2 = x^3 + (21a + 23)x + 1)$$

$$\xrightarrow{\varphi_2} (y^2 = x^3 + (34a + 11)x + (21a + 33)) \xrightarrow{\varphi_3} E'$$

- The j-invariants of the codomains of $\varphi_n, \dots, \varphi_1$

Ways to represent an ℓ^n-isogeny – Example over $\mathbb{F}_{41^2}$

Example: over $\mathbb{F}_{41^2}$, the 5^3-isogeny

$$\underbrace{(y^2 = x^3 + 1)}_{E} \xrightarrow{\varphi} \underbrace{(y^2 = x^3 + (16a+10)x + (3a+34))}_{E'}$$

with $(a-22)^2 \equiv 27 \bmod 41$

- the rational functions defining φ

$$\varphi\colon (x,y) \mapsto \left(\frac{4x^{125} + (7a+7)\,x^{124} + \dots}{10x^{124} + (38a+38)\,x^{123} + \dots}, \frac{21x^{186}y + \dots}{31x^{186} + \dots} \right)$$

- (Generators of) the kernel of φ + Vélu's formulae

$$\ker\varphi = \{\text{roots of } x^{62} + (6a+6)\,x^{61} + \dots\} \subseteq \mathbb{F}_{41^{50}}$$

- Factor φ as a chain of ℓ-isogenies $\varphi_n \circ \cdots \circ \varphi_1$

$$E \xrightarrow{\varphi_1} (y^2 = x^3 + (21a+23)x + 1)$$

$$\xrightarrow{\varphi_2} (y^2 = x^3 + (34a+11)x + (21a+33)) \xrightarrow{\varphi_3} E'$$

- The j-invariants of the codomains of $\varphi_n, \dots, \varphi_1$

$$0 \xrightarrow{\varphi_1} 28 \xrightarrow{\varphi_2} 3 \xrightarrow{\varphi_3} 32$$

Ways to represent an ℓ^n-isogeny – Example over $\mathbb{F}_{41^2}$

Example: over $\mathbb{F}_{41^2}$, the 5^3-isogeny

$$\underbrace{(y^2 = x^3 + 1)}_{E} \xrightarrow{\varphi} \underbrace{(y^2 = x^3 + (16a+10)x + (3a+34))}_{E'}$$

with $(a-22)^2 \equiv 27 \bmod 41$

- the rational functions defining φ

$$\varphi\colon (x,y) \mapsto \left(\frac{4x^{125} + (7a+7)\,x^{124} + \dots}{10x^{124} + (38a+38)\,x^{123} + \dots}, \frac{21x^{186}y + \dots}{31x^{186} + \dots} \right)$$

- (Generators of) the kernel of φ + Vélu's formulae

$$\ker\varphi = \{\text{roots of } x^{62} + (6a+6)\,x^{61} + \dots\} \subseteq \mathbb{F}_{41^{50}}$$

- Factor φ as a chain of ℓ-isogenies $\varphi_n \circ \cdots \circ \varphi_1$

$$E \xrightarrow{\varphi_1} (y^2 = x^3 + (21a+23)x + 1)$$

$$\xrightarrow{\varphi_2} (y^2 = x^3 + (34a+11)x + (21a+33)) \xrightarrow{\varphi_3} E'$$

- The j-invariants of the codomains of $\varphi_n, \dots, \varphi_1$

$$0 \xrightarrow{\varphi_1} 28 \xrightarrow{\varphi_2} 3 \xrightarrow{\varphi_3} 32$$