PRISMO

A Quaternion Signature for Supersingular Isogeny Group Actions

Tako Boris Fouotsa, EPFL

Swiss Crypto Day 2025 - Halloween Edition

31st October 2025

Outline

Motivation

Supersingular isogenies and endomorphisms

PRISM*

PRISMO*

Motivation

Sigma protocols

$$\mathcal{L} = \{\ (x, w)\ \} \qquad \text{arising from a hard relation}$$

Prover(x, w)		**Verifier**(x)
$(\mathsf{com}, \mathsf{P}_{\mathsf{state}}) \leftarrow \mathcal{P}_1(x, w)$	$\xrightarrow{\quad\mathsf{com}\quad}$	
	$\xleftarrow{\quad\mathsf{ch}\quad}$	$\mathsf{ch} \leftarrow\!\!\$\ \mathcal{C}$
$\mathsf{rsp} \leftarrow \mathcal{P}_2(\mathsf{P}_{\mathsf{state}}, \mathsf{ch})$	$\xrightarrow{\quad\mathsf{rsp}\quad}$	
		$\mathcal{V}(x, \mathsf{com}, \mathsf{ch}, \mathsf{rsp}) = \text{Accept/Reject}$

Sigma protocols

Prover(x, w)		**Verifier**(x)
$(\mathsf{com}, \mathsf{P}_{\mathsf{state}}) \leftarrow \mathcal{P}_1(x, w)$	$\xrightarrow{\quad\mathsf{com}\quad}$	
	$\xleftarrow{\quad\mathsf{ch}\quad}$	$\mathsf{ch} \leftarrow\!\!\$\ \mathcal{C}$
$\mathsf{rsp} \leftarrow \mathcal{P}_2(\mathsf{P}_{\mathsf{state}}, \mathsf{ch})$	$\xrightarrow{\quad\mathsf{rsp}\quad}$	
		$\mathcal{V}(x, \mathsf{com}, \mathsf{ch}, \mathsf{rsp}) = \text{Accept/Reject}$

Completeness: V accepts when P knows a witness and they follow the protocol.
Special Soundness: $w \leftarrow \mathsf{extract}(x, (com, ch, rsp), (com, ch', rsp')),\ ch \neq ch'$.
Special HVZK: given ch, $(com, ch, rsp) \leftarrow \mathsf{simulate}(x, ch)$ that is valid.

Sigma protocols (2)

A dishonest P can always fool V with probability at least $1/\#\mathcal{C}$.

- $\#\mathcal{C} = O(\mathsf{poly}(\lambda))$ (2 for example), $1/\#\mathcal{C}$ is not negligible, not great!
  - Solution: repeat the sigma protocol several times.
  - Consequence: huge efficiency/size overhead.
  - ⋆ The case for CSI-FiSh (isogeny group action signature).
- $\#\mathcal{C} = O(\mathsf{exp}(\lambda))$, $1/\#\mathcal{C}$ is negligible, great!
  - ⋆ The case for SQIsign and PRISM

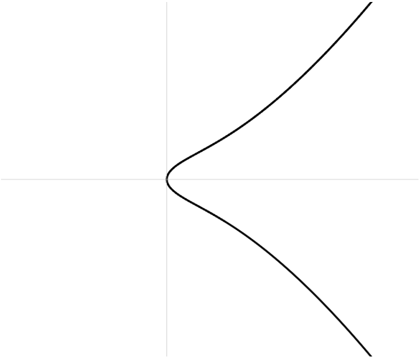
Question: Can we adapt PRISM to the isogeny group action setting?

λ is the security parameter; PRISM is a hash and sign signature instead.

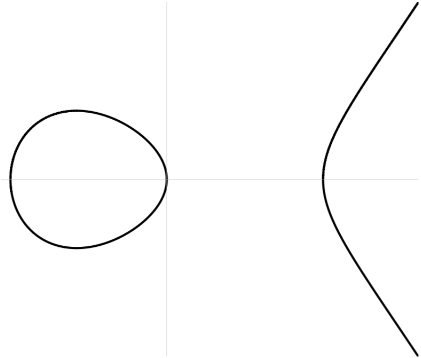
Supersingular isogenies and endomorphisms

Elliptic curves

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

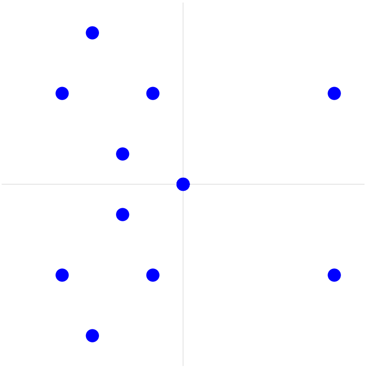


$$E' \ : \ y^2 = x^3 - 4x$$

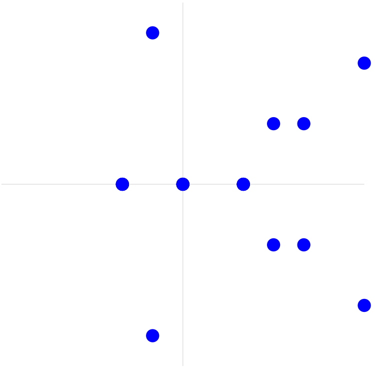


Elliptic curves

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

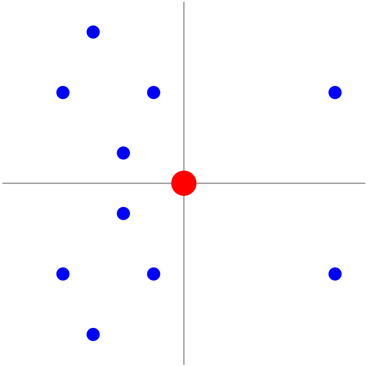


$$E' \ : \ y^2 = x^3 - 4x$$

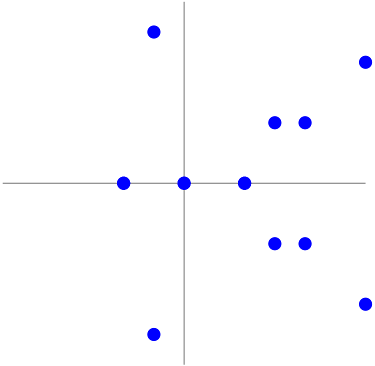


Isogenies

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



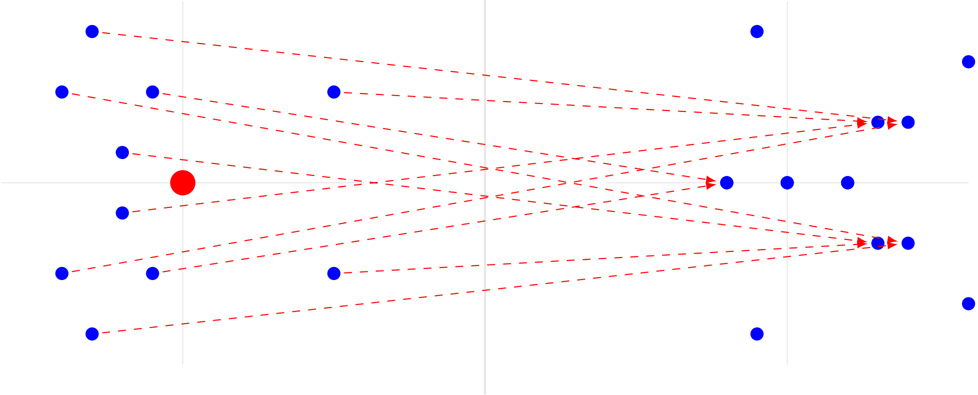
$E' \ : \ y^2 = x^3 - 4x$



Credits: Luca De Feo

Isogenies

$E \ : \ y^2 = x^3 + x$ $\qquad$ $E' \ : \ y^2 = x^3 - 4x$



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

- Kernel generator in red.
- The degree of the isogeny is 2.

Isogeny computation

Degree ℓ isogeny where $\ell > 2$ is a prime, Impractical for large primes.

$$\phi(P) = \left(\frac{x^{\ell} + ...}{(x^{(\ell-1)/2} + ...)^2}, y \cdot \frac{x^{\ell} + ...}{(x^{(\ell-1)/2} + ...)^3} \right)$$

Degree ℓ^n isogeny

$$\phi(P) = \left(\frac{x^{\ell} + ...}{(x^{(\ell-1)/2} + ...)^2}, y \cdot \frac{x^{\ell} + ...}{(x^{(\ell-1)/2} + ...)^3} \right) \circ \cdots \circ \left(\frac{x^{\ell} + ...}{(x^{(\ell-1)/2} + ...)^2}, y \cdot \frac{x^{\ell} + ...}{(x^{(\ell-1)/2} + ...)^3} \right)$$

Isogeny computation

Degree ℓ isogeny where $\ell > 2$ is a prime, Impractical for large primes.

$$\phi(P) = \left(\frac{x^\ell + \ldots}{(x^{(\ell-1)/2} + \ldots)^2}, y \cdot \frac{x^\ell + \ldots}{(x^{(\ell-1)/2} + \ldots)^3} \right)$$

Degree ℓ^n isogeny

$$\phi(P) = \left(\frac{x^\ell + \ldots}{(x^{(\ell-1)/2} + \ldots)^2}, y \cdot \frac{x^\ell + \ldots}{(x^{(\ell-1)/2} + \ldots)^3} \right) \circ \cdots \circ \left(\frac{x^\ell + \ldots}{(x^{(\ell-1)/2} + \ldots)^2}, y \cdot \frac{x^\ell + \ldots}{(x^{(\ell-1)/2} + \ldots)^3} \right)$$

Isogeny computation

Degree ℓ isogeny where $\ell > 2$ is a prime, Impractical for large primes.

$$\phi(P) = \left(\frac{x^\ell + \dots}{(x^{(\ell-1)/2} + \dots)^2}, y \cdot \frac{x^\ell + \dots}{(x^{(\ell-1)/2} + \dots)^3} \right)$$

Degree ℓ^n isogeny

$$\phi(P) = \left(\frac{x^\ell + \dots}{(x^{(\ell-1)/2} + \dots)^2}, y \cdot \frac{x^\ell + \dots}{(x^{(\ell-1)/2} + \dots)^3} \right) \circ \dots \circ \left(\frac{x^\ell + \dots}{(x^{(\ell-1)/2} + \dots)^2}, y \cdot \frac{x^\ell + \dots}{(x^{(\ell-1)/2} + \dots)^3} \right)$$

Ordinary/supersingular curves

For n coprime to the field characteristic

$$E[n] = \langle P, Q \rangle \simeq \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}.$$

Ordinary curves

- $E[p] = \langle P \rangle \simeq \mathbb{Z}/p\mathbb{Z}$
- $\mathrm{End}(E)$ has rank 2, is commutative

Supersingular curves:

- $E[p] = \{\infty\}$
- $\mathrm{End}(E)$ has rank 4, is not commutative

Ordinary/supersingular curves

For n coprime to the field characteristic

$$E[n] = \langle P, Q \rangle \simeq \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}.$$

Ordinary curves

- $E[p] = \langle P \rangle \simeq \mathbb{Z}/p\mathbb{Z}$
- $\mathrm{End}(E)$ has rank 2, is commutative

Supersingular curves:

- $E[p] = \{\infty\}$
- $\mathrm{End}(E)$ has rank 4, is not commutative
- Allow more efficient protocols

Prime degree isogeny problem

Prime degree isogeny problem

Given a random supersingular elliptic curve E and a large prime q, compute an isogeny $\phi : E \to E'$ of degree q.

Easy when one knows one the following:

- the endomorphism ring $\mathrm{End}(E)$ of E [something called Deuring correspondence]
- a non scalar endomorphism $\theta \in \mathrm{End}(E)$ which fixes a group $\langle P \rangle$ of order q

We can hence use $\mathrm{End}(E)$ as a trapdoor. In fact, computing $\mathrm{End}(E)$ is hard.

PRISM*

PRISM* Signature

$$\begin{tikzcd}[column sep=huge] & & E' \\ E_0 \arrow[r, "\tau"] & E \arrow[ur, "\sigma"] & \end{tikzcd}$$

$\mathrm{End}(E_0)$ $\qquad\qquad$ $\mathrm{End}(E)$

PRISM* Signature

$$\begin{tikzcd}
 & & E' \\
E_0 \arrow[r, "\tau"] & E \arrow[ur, "\sigma"] & \\
\mathrm{End}(E_0) & \mathrm{End}(E) &
\end{tikzcd}$$

PRISM* Signature

$$
\begin{tikzcd}
 & & E' \\
E_0 \arrow[r, "\tau"] & E \arrow[ur, "\sigma"] & \\
\mathrm{End}(E_0) & \mathrm{End}(E) &
\end{tikzcd}
$$

PRISM* Signature

$$E_0 \xrightarrow{\tau} E \xrightarrow{\sigma} E'$$

$\mathrm{End}(E_0)$ $\mathrm{End}(E)$

Signer(E, End(E), m)

Verifier (E)

PRISM* Signature

$$E_0 \xrightarrow{\tau} E \xrightarrow{\sigma} E'$$

$$\mathrm{End}(E_0) \qquad\qquad \mathrm{End}(E)$$

Signer(E, End(E), m)

Verifier (E)

$q \leftarrow \mathsf{H}_{\mathsf{Prime}_a}(E||\mathsf{m})$
$\sigma \leftarrow \mathsf{GenIsogeny}(E, \mathrm{End}(E), q)$

PRISM* Signature

$$E_0 \xrightarrow{\tau} E \xrightarrow{\sigma} E'$$

$\mathrm{End}(E_0)$ $\mathrm{End}(E)$

Signer$(E, \mathrm{End}(E), \mathsf{m})$

Verifier (E, m, σ)

$q \leftarrow \mathsf{H}_{\mathsf{Prime}_a}(E||\mathsf{m})$
$\sigma \leftarrow \mathsf{GenIsogeny}(E, \mathrm{End}(E), q)$

$\xrightarrow{(\mathsf{m},\ \sigma)}$

PRISM* Signature

$$\begin{tikzcd} & & E' \\ E_0 \arrow[r, "\tau"] & E \arrow[ur, "\sigma"] & \end{tikzcd}$$

$\mathrm{End}(E_0)$ $\qquad\qquad$ $\mathrm{End}(E)$

Signer$(E,\ \mathrm{End}(E),\ \mathsf{m})$

$q \leftarrow \mathsf{H}_{\mathsf{Prime}_{\mathsf{a}}}(E||\mathsf{m})$
$\sigma \leftarrow \mathsf{GenIsogeny}(E, \mathrm{End}(E), q)$

$\xrightarrow{(\mathsf{m},\ \sigma)}$

Verifier $(E,\ \mathsf{m},\ \sigma)$

$q \leftarrow \mathsf{H}_{\mathsf{Prime}_{\mathsf{a}}}(E||\mathsf{m})$
Is $\sigma : E \to E'$ of degree q?

Hard problem underlying the security of PRISM*

PrimeIsogenyOracle: takes as inputs a supersingular elliptic curve E defined over $\mathbb{F}_{p^2}$ and a prime q of length a, and returns a uniformly random isogeny of degree q from E.

One more prime degree isogeny problem

Given a random supersingular elliptic curve E and a PrimeIsogenyOracle, *output an isogeny of degree q' where q' is a prime of length a different from all the primes q formerly queried to* PrimeIsogenyOracle.

PRISMO*

Supersingular isogeny group actions

$$\pi : E \to E^{(p)}; \qquad (x, y) \mapsto (x^p, y^p)$$

If E is defined over $\mathbb{F}_p$, then $\pi \in \mathrm{End}(E)$.

$\mathbb{F}_p$-rational isogenies* arise from the action of some abelian group denoted by $\mathrm{cl}(\mathbb{Z}[\pi])$ on the set of supersingular elliptic curves defined over $\mathbb{F}_p$.

This action is a (rich) cryptography group action, and it allows to design various cryptographic protocols. Nevertheless:

- it requires larger primes compared to the generic supersingular setting,
- all existing signatures (CSI-FiSh and friends) use parallel repetitions.

PRISM is not secure when $E/\mathbb{F}_p$

This is because we know $\pi \in \mathrm{End}(E)$ which is not a scalar endomorphism.

With $\pi \in \mathrm{End}(E)$ we can efficiently compute an isogeny of degree q where there exist a point P such that $\pi(\langle P \rangle) = \langle P \rangle$.

Odd primes q for which such a point exists are exactly the split (in $\mathbb{Z}[\pi]$) primes.

For inert primes q, no such point exists, hence the knowledge of π is useless to adversaries.

PRISMO: variant of PRISM where $E/\mathbb{F}_p$ and the primes q are inert in $\mathbb{Z}[\pi]$.

PRISMO* Signature (E is defined over $\mathbb{F}_p$)

$$\begin{tikzcd}
 & & & E' \\
\begin{array}{c} E_0, \pi \\ \mathrm{End}(E_0) \end{array} \arrow[rr, "\tau_{\mathfrak{a}}"] & & \begin{array}{c} E, \pi \\ \mathrm{End}(E) \end{array} \arrow[ur, "\sigma"] &
\end{tikzcd}$$

PRISMO* Signature (E is defined over $\mathbb{F}_p$)

$$E_0, \pi \xrightarrow{\tau_{\mathfrak{a}}} E, \pi \xrightarrow{\sigma} E'$$

$$\mathrm{End}(E_0) \qquad\qquad\qquad \mathrm{End}(E)$$

PRISMO* Signature (E is defined over $\mathbb{F}_p$)

$$\begin{tikzcd} & & E' \\ E_0, \pi \arrow[r, "\tau_{\mathfrak{a}}"] & E, \pi \arrow[ur, "\sigma"] & \\ \mathrm{End}(E_0) & \mathrm{End}(E) & \end{tikzcd}$$

Signer(E, $\mathrm{End}(E)$, m)

Verifier (E)

PRISMO* Signature (E is defined over $\mathbb{F}_p$)

$$\begin{array}{c} E_0, \pi \\ \mathrm{End}(E_0) \end{array} \xrightarrow{\tau_{\mathfrak{a}}} \begin{array}{c} E, \pi \\ \mathrm{End}(E) \end{array} \xrightarrow{\sigma} E'$$

Signer(E, $\mathrm{End}(E)$, m)

Verifier (E)

$$q \leftarrow \mathsf{H}_{\mathsf{InsertPrime}_{\mathsf{a}}}(E||\mathsf{m})$$
$$\sigma \leftarrow \mathsf{GenIsogeny}(E, \mathrm{End}(E), q)$$

PRISMO* Signature (E is defined over $\mathbb{F}_p$)

$$\begin{array}{c} E_0, \pi \\ \mathrm{End}(E_0) \end{array} \xrightarrow{\tau_{\mathfrak{a}}} \begin{array}{c} E, \pi \\ \mathrm{End}(E) \end{array} \xrightarrow{\sigma} E'$$

Signer(E, $\mathrm{End}(E)$, m)

$q \leftarrow \mathsf{H}_{\mathsf{InsertPrime}_{\mathsf{a}}}(E||\mathsf{m})$

$\sigma \leftarrow \mathsf{GenIsogeny}(E, \mathrm{End}(E), q)$

$\xrightarrow{(\mathsf{m},\ \sigma)}$

Verifier (E, m, σ)

PRISMO* Signature (E is defined over $\mathbb{F}_p$)

$$E_0, \pi \xrightarrow{\tau_{\mathfrak{a}}} E, \pi \xrightarrow{\sigma} E'$$

$\mathrm{End}(E_0)$ $\qquad$ $\mathrm{End}(E)$

Signer(E, $\mathrm{End}(E)$, m) $\qquad$ Verifier (E, m, σ)

$q \leftarrow \mathsf{H}_{\mathsf{InsertPrime}_{\mathsf{a}}}(E||\mathsf{m})$

$\sigma \leftarrow \mathsf{GenIsogeny}(E, \mathrm{End}(E), q)$

$\xrightarrow{(\mathsf{m},\ \sigma)}$

$q \leftarrow \mathsf{H}_{\mathsf{InertPrime}_{\mathsf{a}}}(E||\mathsf{m})$

Is $\sigma : E \to E'$ of degree q?

Hard problem underlying the security of PRISMO*

$\mathsf{PrimeIsogenyOracle}_{\mathcal{O}}$: takes as inputs a supersingular elliptic curve E defined over $\mathbb{F}_p$ and an inert[1] prime q of length a, and returns a uniformly random isogeny of degree q from E.

One more inert prime degree isogeny problem

Given a random supersingular elliptic curve E defined over $\mathbb{F}_p$ and a $\mathsf{PrimeIsogenyOracle}_{\mathcal{O}}$, *output an isogeny of degree q' where q' is an inert prime of length a different from all the primes q formerly queried to* $\mathsf{PrimeIsogenyOracle}_{\mathcal{O}}$.

[1] inert in $\mathbb{Z}[\pi]$.

Results

PRISMO is more efficient and more compact compared to CSI-FiSh:

- 80x faster for signing
- 1457x faster for verification
- 29x more compact (signature size)

for NIST level I[2].

[2] Supersingular isogeny group action with a 2000 bits prime.

Thanks for still being awake!

ePrint