Radical Isogenies on Montgomery Curves

Hiroshi Onuki, Tomoki Moriya

The University of Tokyo, Japan

Supported by the Ministry of Internal Affairs and Communications, Japan (JPJ000254) and JSPS KAKENHI Grant Numbers JP21K17739, JP21J10711.

Overview

Isogeny-based cryptography

- a candidate for **post-quantum cryptography**,
- **small** keys and ciphertext,
- **slow** because of isogeny computation.

Radical isogenies

- formulas for computing **repeating isongenies of the same degree**,
- proposed by [CDV2020] (Castryck, Decru, and Vercauteren @Asiacrypt 2020),
- The original formulas are constructed on **Tate normal forms**.

This work

- constructs radical isogenies of degree 3, 4 on **Montgomery curves**,
- **reduce the cost** of transforms between curves in some protocols,
- **prove a conjecture** left open by [CDV2020].

Elliptic curves

Definition 1

An **elliptic curve** is a smooth algebraic curve of genus one.

- An elliptic curve E has an **abelian group structure**, i.e., we can define $P+Q$ for $P, Q \in E$.
- There are **many forms** of elliptic curves.
- In isogeny-based cryptography, we often use **Montgomery curves**

$$y^2 = x^3 + Ax^2 + x,$$

because of efficient scalar multiplications and isogeny formulas.

Isogenies (1/2)

Definition 2

An **isogeny** is a nonzero rational homomorphism between elliptic curves.

Let $\varphi : E \to E'$ be an isogeny.

- We can define the **degree** of φ, denoted by $\deg \varphi$.
- There is the **dual isogeny** $\hat{\varphi} : E' \to E$ $(\deg \hat{\varphi} = \deg \varphi)$.

Example (degree 2)

$$E_1 : y^2 = x^3 + 6x^2 + x,\ \ E_2 : y^2 = x^3 - 12x^2 + 32x,$$

$$E_1 \to E_2,\ \ (x, y) \mapsto \left(\frac{y^2}{x^2}, \frac{y(x^2 - 1)}{x^2} \right).$$

Isogenies (2/2)

E: an elliptic curve over K, N: an integer coprime to $\mathrm{char}(K)$

one to one correspondence

$$\begin{array}{ccc} \{\text{subgroups of } E \text{ of order } N\} & \overset{1:1}{\longleftrightarrow} & \{\text{isogenies of degree } N \text{ from } E\} \\ G & \longmapsto & \varphi_G : E \to E/G \\ & & \text{s.t. } \ker \varphi_G = G \end{array}$$

- This work considers the case that G is **cyclic**.
  I.e., we consider a subgroup of the form $\langle P \rangle$.
- $(E; P, Q \in E) \mapsto (\varphi_{\langle P \rangle}(Q), E/\langle P \rangle$ can be **efficiently computed**.
  (**Vélu's formula**)
- $(E, E/\langle P \rangle) \mapsto P$ is consider to be **hard**.
  (the security of isogeny-based cryptography)

CSIDH and CSURF

CSIDH

- isogeny-based key-exchange,
- by Castryck, Lange, Martindale, Panny, and Renes @Asiacrypt 2018,
- uses elliptic curves $/\mathbb{F}_p$ and isogenies $/\mathbb{F}_p$ with $p \equiv 3 \pmod 8$,
- uses only isogenies of **odd degrees**.

CSURF

- variant of CSIDH by Castryck and Decru @PQCrypto 2020,
- uses $p \equiv 7 \mod 8$,
- also uses isogenies of **degree 2 and 4**.

E: an elliptic curve over K,
N: an integer coprime to $\mathrm{char}(K)$,
P: a point on E of order N.

A **radical isogeny** is a formula of a map

$$\begin{array}{ccc} \text{(elliptic curve, order-}N\text{ point)} & & \text{(elliptic curve, order-}N\text{ point)} \\ (E, P \in E) & \longmapsto & (E/\langle P\rangle, P' \in E/\langle P\rangle), \end{array}$$

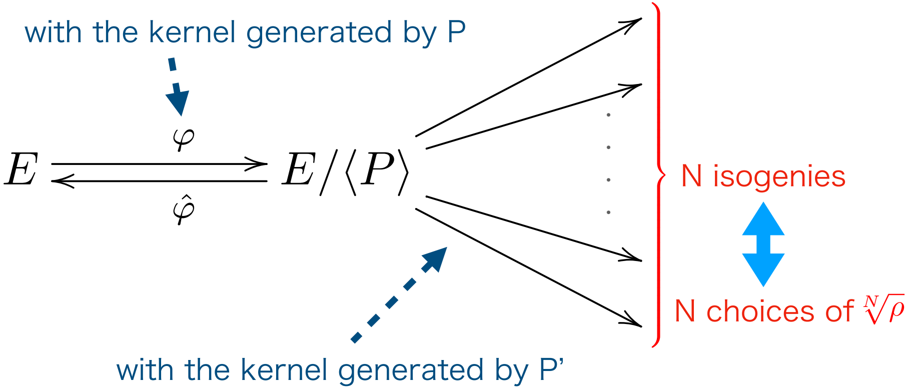
where $\langle \hat{\varphi}(P')\rangle = \langle P\rangle$.

Thoery of radical isogenies

One can chose a form of $E/\langle P\rangle$ such that

$$E/\langle P\rangle \text{ and } P' \text{ are defined over } K(\sqrt[N]{\rho}),$$

where ρ is the Tate pairing $\tau_N(P, -P)$.


with the kernel generated by P
$E \underset{\hat{\varphi}}{\overset{\varphi}{\rightleftarrows}} E/\langle P \rangle$
N isogenies
N choices of $\sqrt[N]{\rho}$
with the kernel generated by P'

Radical Isongenies (3/6)

[CDV2020] uses forms of elliptic curves such that P and P' are $(0, 0)$.

$N = 3$

$$E : y^2 + a_1 xy + a_3 y = x^3.$$

$N \geq 4$

Tate normal form

$$E : y^2 + (1 - c)xy - by = x^3 - bx^2$$

(b, c satisfy a relation depending on N).

Radical Isongenies (4/6)

$\mathbf{N = 3}$

$E : y^2 + a_1xy + a_3y = x^3$, $P = (0,0)$,

$E/\langle P\rangle : y^2 + a_1'xy + a_3'y = x^3$, $P' = (0,0)$,

$$a_1' = -6\alpha + a_1,\ a_3' = 3a_1\alpha^2 - a_1^2\alpha + 9a_3,$$

α is a cube root of $-a_3$.

$\mathbf{N = 4}$

$E : y^2 + xy - by = x^3 - bx^2$, $P = (0,0)$,

$E/\langle P\rangle : y^2 + xy - b'y = x^3 - b'x^2$, $P' = (0,0)$,

$$b' = \frac{\alpha(4\alpha^2 + 1)}{(2\alpha + 1)^4},$$

α is a fourth root of $-b$.

Iteration of radical isogenies of degree $N = 3$:

$$E \xrightarrow{\langle(0,0)\rangle} E' \xrightarrow{\langle(0,0)\rangle} E'' \xrightarrow{\langle(0,0)\rangle}$$

$$(a_1, a_3) \qquad (a_1', a_3') \qquad (a_1'', a_3'')$$

$$a_1' = -6\alpha + a_1 \qquad a_1'' = -6\alpha' + a_1'$$

$$a_3' = 3a_1\alpha^2 - a_1^2\alpha + 9a_3 \qquad a_3'' = 3a_1'{\alpha'}^2 - {a_1'}^2\alpha' + 9a_3'$$

No computation for the kernels of intermediate isogenies.
$\Rightarrow$ **accelerating isogenies of small degrees** in CSIDH and CSURF.
(especially in **CSURF**. $\because$ one can use $N = 4$.)

Q. How to choose a radical $\alpha = \sqrt[3]{-a_3}$?

A. Choose $\alpha \in \mathbb{F}_p$ in CSIDH and CSURF.

$\because$ There is the unique N-th root in $\mathbb{F}_p$ if $\#\mathbb{F}_p^\times = p - 1$ is coprime to N.

Radical Isogenies (6/6)

Radical isogenies in CSURF

- One needs to **transform to a Montgomery curve**
  $\because$ generating the first kernel and computing higher degree isogenies.

- In the case $N = 4$, there are two fourth roots in $\mathbb{F}_p$.
  $\Rightarrow$ The choice is conjectured but **not proven**.

This work

- constructs radical isogenies of degree 3 and 4 on Montgomery curves.

- proves the conjecture on $N = 4$.

Montgomery Curves

Montgomery Curves

A **Montgomery curve** is an elliptic curve defined by

$$y^3 = x^3 + Ax^2 + x, \quad A^2 \neq 4.$$

We call A the **Montgomery coefficient**.

- The order of the point $(0, 0)$ is 2.
- $[2](1, -) = [2](-1, -) = (0, 0)$.
- $C_E^{(4)} \coloneqq \langle (1, -) \rangle$.
- If $(t, -)$ is a point of order 3 then

$$A = \frac{-3t^4 - 6t^2 + 1}{4t^3}.$$

I.e., t determines the Montgomery coefficient.

Our Contribution 1-1: A Formula of Degree 3

A pair $(E, (t, -))$ of a Montgomery curve and a point of order 3 is represented by t.

$\Rightarrow$ There exists a radical isogeny: $t \mapsto t'$.

Theorem 1

$(E, (t, -))$: a pair of a Montgomery curve and a point order 3,

$\varphi : E \to E/\langle (t, -) \rangle$: an isogeny with kernel $\langle (t, -) \rangle$.

$(t', -)$: a point on $E/\langle (t, -) \rangle$ of order 3 such that $\langle \hat{\varphi}((t', -)) \rangle = \langle (t, -) \rangle$.

Then

$$t' = 3t\alpha^2 + (3t^2 - 1)\alpha + 3t^3 - 2t,$$

where α is a **cube root** of $t(t^2 - 1)$.

Our Contribution 1-2: A Formula of Degree 4

A pair $(E, C_E^{(4)})$ of a Montgomery curve and a point of order 4 is represented by A.

$\Rightarrow$ There exists a radical isogeny: $A \mapsto A'$.

Theorem 2

E : a Montgomery curve with coefficient A,

$\varphi : E \to E'$: an isogeny of kernel $C_E^{(4)}$ such that $\hat{\varphi}(C_{E'}^{(4)}) = C_E^{(4)}$,

A' : the Montgomery coefficient of E', $a := 4(A+2)$, $a' := 4(A'+2)$.
Then

$$a' = \frac{(\alpha+2)^4}{\alpha(\alpha^2+4)}.$$

where α is a **fourth root** of a.

Comparison (1/2)

[CDV2020]:

$$
\begin{tikzcd}
E_T \arrow[r] \arrow[rrrr, phantom, bend left, "\overbrace{\hspace{6cm}}^{\text{radical isogenies}}"] & E_T^{(1)} \arrow[r] & \cdots \arrow[r] & & E_T^{(n)} \arrow[d, "\text{transform}"] \\
E_M \arrow[u, "\text{transform}"] & & & & E_M^{(n)}
\end{tikzcd}
$$

This work:

$$
\begin{tikzcd}
E_M \arrow[loop left, "\text{to radical representation}"'] \arrow[r] \arrow[rrrr, phantom, bend left, "\overbrace{\hspace{6cm}}^{\text{radical isogenies}}"] & E_M^{(1)} \arrow[r] & \cdots \arrow[r] & & E_M^{(n)} \arrow[loop right, "\text{recover coefficient}"]
\end{tikzcd}
$$

Comparison (2/2)

Number of operations in $\mathbb{F}_p$ in CSURF

	Degree 3		Degree 4	
	[CDV2020]	**Our formula**	[CDV2020]	**Our formula**
Isogeny	$\mathbf{E} + 3\mathbf{M} + 12\mathbf{A}$	$\mathbf{E} + 5\mathbf{M} + 12\mathbf{A}$	$\mathbf{E} + 3\mathbf{M} + 5\mathbf{A} + \mathbf{I}$	$\mathbf{E} + 3\mathbf{M} + 4\mathbf{A} + \mathbf{I}$
To radial form	$> \mathbf{E}$	0	$2\mathbf{A} + \mathbf{I}$	$3\mathbf{A}$
From radical form	$> 3\mathbf{E}$	$3\mathbf{M} + 9\mathbf{A} + \mathbf{I}$	$2\mathbf{A} + \mathbf{I}$	$\mathbf{M} + 3\mathbf{A}$

E: exponentiation, **M**: multiplication, **A**: addition, **I**: inversion.

Radicals are computed by exponentiation. $\mathbf{E} \approx 1.5 \log p \mathbf{M}$.

Our Contribution 2: Fourth Root in $\mathbb{F}_p$ (1/2)

Theorem 3

Let p be a prime satisfying $p \equiv 7 \pmod 8$. Consider a radical isogeny of degree 4 on Montgomery curves:

$$a \mapsto a' = \frac{(\alpha + 2)^4}{\alpha(\alpha^2 + 4)}.$$

We can compute **the isogeny used in CSURF** by taking

$$\alpha = (-a)^{(p+1)/8}.$$

Our Contribution 2: Fourth Root in $\mathbb{F}_p$ (2/2)

Corollary 1 (Conjecture by [CDV2020])

Let p be a prime satisfying $p \equiv 7 \pmod 8$. Consider a radical isogeny of degree 4 on Tate normal forms:

$$b \mapsto b' = \frac{\alpha(4\alpha^2+1)}{(2\alpha+1)^4}.$$

We can compute **the isogeny used in CSURF** by taking

$$\alpha = b^{(p+1)/8}.$$

Conclusion

Our contribution:

- We constructed radical isogenies of degree 3 and 4 on Montgomery curves.
- Our formulas slightly improve the efficiency of CSURF using radical isogenies.
- We proved a conjecture left as open by [CDV2020].

Future work:

- Other applications; e.g., random walks in isogeny graphs