$\sqrt[R]{adical}$ Isogenies

Wouter Castryck, *Thomas Decru* & Fréderik Vercauteren
COSIC, ESAT, KU Leuven

Asiacrypt 2020

Isogeny-based cryptography

- Let $E/\mathbb{F}_q$ be an elliptic curve over $\mathbb{F}_q$ with $q = p^n$, e.g.

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

- Isogeny $\varphi : E \to E'$ is non-constant morphism with $\varphi(0_E) = 0_{E'}$ and is also a group homomorphism
- Degree of φ is degree as morphism
- Isogenies of smooth degree are easy to compute
- Cyclic separable isogenies can be identified by a point that generates the kernel
- General hard problem: given E and E', find an isogeny $\varphi : E \to E'$

CSIDH

- CSIDH: supersingular curves over $\mathbb{F}_p$ with $p = 4\ell_1\ell_2\cdots\ell_r - 1$ and $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$
- Allows easy computations of isogenies of degree $\ell_1, \ldots, \ell_r$:
  - Isogenies corresponding to action of $\mathfrak{l} = (\ell, \pi - 1)$ in the class group
  - Isogenies corresponding to action of $\mathfrak{l}^{-1} = (\ell, \pi + 1)$ in the class group
- For CSIDH-512:
  - $r = 74$, and we compute up to 5 isogenies for each of the 74 distinct prime degrees ranging from 3 to 587
  - this corresponds to action of

$$(3, \pi - 1)^{e_1}(5, \pi - 1)^{e_2}\cdots(587, \pi - 1)^{e_{74}}$$

with $e_i \in [-5; 5]$

Computing isogenies

Trivial approach:

- Vélu's formulae require point P in kernel, i.e. a rational ℓ-torsion point
- Generate random point $Q \in E(\mathbb{F}_p)$ and set $P = [(p+1)/\ell]Q$
- $P \neq 0_E$, then it has order ℓ, otherwise start over (with probability $1/\ell$)

Computing isogenies

Trivial approach:

- Vélu's formulae require point P in kernel, i.e. a rational ℓ-torsion point
- Generate random point $Q \in E(\mathbb{F}_p)$ and set $P = [(p+1)/\ell]Q$
- $P \neq 0_E$, then it has order ℓ, otherwise start over (with probability $1/\ell$)

Better approach: push point through isogenies

- Generate a point R_0 of order dividing $\ell_1 \ell_2 \cdots \ell_r$
- In step i, multiply R_{i-1} by smaller cofactor to get point P_i of order ℓ_i
- Compute isogeny using Vélu, but also image R_i of R_{i-1} under isogeny with order $\ell_{i+1} \cdots \ell_r$

Computing chains of isogenies

- Point P_i can still be 0_{E_i} with probability $1/\ell_i$

- Alternative approach: compute chain of N-isogenies (N any of the primes)
- Given E/K and $P \in E(K)$ of order N derive expressions for
  - $E' = E/\langle P \rangle$ (given by Vélu)
  - $P' \in E$ such that

$$E \to E' \to E'/\langle P' \rangle$$

  is **cyclic** isogeny of degree N^2

- P' is in general not defined over K, but can be used to apply Vélu again
- Cyclic so no walking backwards; so can repeat for degree N^k

Radical isogenies: 3 step approach

1. Find general curve model with distinguished point of order N
   - Solution: Tate normal form and Vélu's formulae give equation for E'

Radical isogenies: 3 step approach

1. Find general curve model with distinguished point of order N
   - Solution: Tate normal form and Vélu's formulae give equation for E'
2. Determine field of definition of a good P'
   - Solution: Tate pairing value defining simple radical extension

Radical isogenies: 3 step approach

1. Find general curve model with distinguished point of order N
   - Solution: Tate normal form and Vélu's formulae give equation for E'
2. Determine field of definition of a good P'
   - Solution: Tate pairing value defining simple radical extension
3. Determine coordinates of P'
   - Solution: division polynomials

Step 1: Tate normal form

Lemma

Let E be an elliptic curve over K and let $P \in E(K)$ be a point of order $N \geq 4$, then (E, P) is isomorphic to a unique pair of the form

$$E : y^2 + (1 - c)xy - by = x^3 - bx^2, \qquad P = (0, 0)$$

with $b, c \in K$ and $\Delta \neq 0$

Step 1: Tate normal form

Lemma

Let E be an elliptic curve over K and let $P \in E(K)$ be a point of order $N \geq 4$, then (E, P) is isomorphic to a unique pair of the form

$$E : y^2 + (1-c)xy - by = x^3 - bx^2, \qquad P = (0,0)$$

with $b, c \in K$ and $\Delta \neq 0$

- Derive relation $F_N(b,c) = 0$ such that P has exact order N
  - easy by expressing $\ldots, -2P, -P, 2P, 3P, \ldots$ in function of b, c

Step 1: example for $N = 5$

- Curve $E : y^2 + (1-c)xy - by = x^3 - bx^2$, point $P = (0, 0)$
- Relation: $F_5(b, c) = c - b = 0$
- Applying Vélu to $\langle P \rangle$ gives isogeny φ and

$$E' : y^2 + (1-b)xy - by = x^3 - bx^2 - 5b(b^2 + 2b - 1)x - b(b^4 + 10b^3 - 5b^2 + 15b - 1)$$

- Next up: find point of order 5 on E'

Step 2: Tate pairing and simple radical extension

- Tate pairing
  - bilinear map

$$t_N : E(K)[N] \times E(K)/NE(K) \to K^*/(K^*)^N : (P_1, P_2) \mapsto t_N(P_1, P_2)$$

  - easy to compute ($\sim$ scalar multiplication)

Step 2: Tate pairing and simple radical extension

- Tate pairing
  - bilinear map

$$t_N : E(K)[N] \times E(K)/NE(K) \to K^*/(K^*)^N : (P_1, P_2) \mapsto t_N(P_1, P_2)$$

  - easy to compute ($\sim$ scalar multiplication)
- A field extension $K \subset L$ is simple radical of degree $N \geq 2$ if there exists an $\alpha \in L$ such that
  - $L = K(\alpha)$
  - $\alpha^N \in K$
  - $x^N - \alpha^N \in K[x]$ is irreducible

Radical isogenies: main theorem

Theorem

Let $N \geq 4$ and consider the universal Tate normal curve

$$E : y^2 + (1-c)xy - by = x^3 - bx^2, \qquad P = (0,0)$$

over the field

$$\mathbb{Q}_N(b,c) := \mathrm{Frac}\frac{\mathbb{Q}[b,c]}{(F_N(b,c))}.$$

Let $P' \in E' = E/\langle P \rangle$, such that $E \to E'/\langle P' \rangle$ has degree N^2. Then

$$\mathbb{Q}_N(b,c)(P') = \mathbb{Q}_N(b,c)\left(\sqrt[N]{t_N(P,-P)}\right)$$

is a simple radical extension of degree N for a well-chosen Nth root of $t_N(P,-P)$.

Radical isogenies: main theorem

Theorem

Let $N \geq 4$ and consider the universal Tate normal curve

$$E : y^2 + (1-c)xy - by = x^3 - bx^2, \qquad P = (0,0)$$

over the field

$$\mathbb{Q}_N(b,c) := \mathrm{Frac}\frac{\mathbb{Q}[b,c]}{(F_N(b,c))}.$$

Let $P' \in E' = E/\langle P \rangle$, such that $E \to E'/\langle P' \rangle$ has degree N^2. Then

$$\mathbb{Q}_N(b,c)(P') = \mathbb{Q}_N(b,c)\left(\sqrt[N]{t_N(P,-P)}\right)$$

is a simple radical extension of degree N for a well-chosen Nth root of $t_N(P,-P)$.

- For $N = 5$, $t_5(P,-P) = b$ so P' is defined over $\mathbb{Q}_N(b,c)(\sqrt[5]{b})$

Step 3: division polynomials

- N-division polynomial $\Psi_{E',N}$:
  - recursively defined
  - easy to compute
  - $P' \in E'[N]$ iff $\Psi_{E',N}(P') = 0$
- Find root of $\Psi_{E',N} = 0$ over $\mathbb{Q}_N(b, c)\left(\sqrt[N]{t_N(P, -P)}\right)$ to find P'!

Example for $N = 5$

Factor 5-division polynomial over $\mathbb{Q}_N(b, c) = \mathbb{Q}_N(b)$

$$\begin{aligned}\Psi_{E',5}(x) = 5 \cdot (&x^2 + (b^2 - b + 1)x + (b^4 + 3b^3 - 26b^2 - 8b + 1)/5) \\ &\cdot (x^5 + 10bx^4 - 5b(b^2 + b - 11)x^3 - 5b(17b^3 + 24b^2 + 46b - 7)x^2 \\ &\quad - 5b(b^5 + 62b^4 + 154b^3 - 65b^2 + 19b - 2)x \\ &\quad - b(b^7 - 19b^6 + 777b^5 - 757b^4 + 755b^3 + 2b^2 + 17b - 1)) \\ &\cdot (x^5 - 15bx^4 - 5b(11b^2 - 9b - 1)x^3 - 5b^2(7b^3 + 13b^2 - 13b + 20)x^2 \\ &\quad - 5b^2(2b^5 + 5b^4 + 6b^3 + 196b^2 - 99b + 1)x \\ &\quad - b^2(b^7 + 7b^6 - 62b^5 + 605b^4 - 127b^3 + 1177b^2 + 14b + 1))\end{aligned}$$

Example for $N = 5$

- Let $\alpha = \sqrt[5]{b}$, then first quintic factor admits the root

$$x_0' = 5\alpha^4 + (b-3)\alpha^3 + (b+2)\alpha^2 + (2b-1)\alpha - 2b$$

- All other roots obtained by scaling α with powers of ζ_5
- Corresponding y_0' is

$$y_0' = 5\alpha^4 + (b-3)\alpha^3 + (b^2-10b+1)\alpha^2 + (13b-b^2)\alpha - b^2 - 11b$$

Example for $N = 5$

- Let $\alpha = \sqrt[5]{b}$, then first quintic factor admits the root

$$x_0' = 5\alpha^4 + (b-3)\alpha^3 + (b+2)\alpha^2 + (2b-1)\alpha - 2b$$

- All other roots obtained by scaling α with powers of ζ_5
- Corresponding y_0' is

$$y_0' = 5\alpha^4 + (b-3)\alpha^3 + (b^2-10b+1)\alpha^2 + (13b-b^2)\alpha - b^2 - 11b$$

- Translating P' to $(0,0)$, we obtain the isomorphic form

$$E' : y^2 + (1-b')xy - b'y = x^3 - b'x^2,$$

where

$$b' = \alpha \frac{\alpha^4 + 3\alpha^3 + 4\alpha^2 + 2\alpha + 1}{\alpha^4 - 2\alpha^3 + 4\alpha^2 - 3\alpha + 1}$$

Application 1: chains of isogenies

- If $\gcd(N, q-1) = 1$, then unique N-th root of any element in $\mathbb{F}_q$

	Sampling N-torsion	Isogenous curve Vélu	Image of a point	Modular polynomial	Radical isogeny
3-isogeny	50,449,710	38,513	18,860	9,939,840	1,071,612
4-isogeny*	63,693,051	45,093	45,004	29,628,400	1,101,677
5-isogeny	41,519,930	140,968	33,453	19,943,602	1,086,011
7-isogeny	39,049,435	247,526	47,734	34,049,452	1,192,454
9-isogeny	47,994,892	319,695	70,899	76,299,055	1,304,341
11-isogeny	36,755,529	448,043	75,995	76,435,364	3,161,470
13-isogeny	36,252,253	548,833	90,168	147,552,105	3,626,544

Application 2: CSIDH / CSURF

- Let $\mathbb{F}_p$ be the CSURF-512 prime

$$p = 2^3 \cdot 3 \cdot \underbrace{(3 \cdot \ldots \cdot 389)}_{\substack{74 \text{ consecutive primes,} \\ \text{skip 347 and 359}}} - 1 \approx 2^{512}$$

- Use skew box of exponents instead of $[-5; 5]$

$$I = [-202; 202] \times [-170; 170] \times [-95; 95] \times [-91; 91] \times [-33; 33] \times$$
$$[-29; 29] \times [-6; 6]^{20} \times [-5; 5]^{14} \times [-4; 4]^{10} \times [-3; 3]^{10} \times [-2; 2]^8 \times [-1; 1]^7$$

  to represent the action of classes of ideals of the form

$$\left(2, \frac{\sqrt{-p} - 1}{2}\right)^{e_1} (3, \sqrt{-p} - 1)^{e_2} (5, \sqrt{-p} - 1)^{e_3} \cdots (389, \sqrt{-p} - 1)^{e_{75}}$$

- Using radical isogenies up to degree 13 gives overall speed-up of 19%

Conclusion & open problems

- Radical isogenies efficient method to compute long chains of small degree isogenies, e.g. $\ell \leq 13$
- Can use very skew exponent box in CSIDH / CSURF with speed-up of 19%
- Open problems:
  - Better method to compute coordinates of P' instead of finding roots of division polynomial?
  - Formulae are not unique: how to find most efficient expressions?
  - Impact on constant time implementation?
  - For large degree isogenies have $\sqrt{\ell}$-techniques by Bernstein, De Feo, Leroux and Smith. What to do for medium sized primes?