Let us walk on the 3-isogeny graph: efficient, fast, and simple

CHES 2025

Jesús-Javier Chi-Domínguez [1], Eduardo Ochoa-Jimenez [1], Ricardo-Neftalí Pontaza-Rodas[1]

[1] Cryptography Research Center, Technology Innovation Institute, Abu Dhabi, UAE

{jesus.dominguez,eduardo.ochoa,ricardo.pontaza}@tii.ae

September 17, 2025

Technology
Innovation
Institute

1. Preliminaries
2. Contributions
3. On the application to QFESTA
4. On the application to dCTIDH
5. Additional remarks

Preliminaries

Along the talk, we consider

- Prime numbers p such that $p \equiv 3 \mod 4$.
- Supersingular elliptic curves $\mathcal{E}$ with $\#\mathcal{E}(\mathbb{F}_{p^2}) = (p \pm 1)^2$ points where $\mathbb{F}_{p^2} = \mathbb{F}_p[i]/(i^2 + 1)$.
- Unless we specify a different model, we center on elliptic curves in Montgomery form (i.e, $\mathcal{E} : y^2 = x^3 + Ax^2 + x$ for some $A \in \mathbb{F}_{p^2}$).
- Small ℓ-isogenies ϕ with cyclic kernels of size $\ell \in \{2, 3\}$.
- Length-n chains of ℓ-isogenies with non-backtracking (i.e., ϕ_{i+1} different from $\hat{\phi}_i$)

$$\mathcal{E}_0 := \mathcal{E} \xrightarrow[\phi_1]{\ell\text{-isogeny}} \mathcal{E}_1 \xrightarrow[\phi_2]{\ell\text{-isogeny}} \mathcal{E}_2 \xrightarrow[\phi_3]{\ell\text{-isogeny}} \cdots \xrightarrow[\phi_n]{\ell\text{-isogeny}} \mathcal{E}' := \mathcal{E}_n$$

Preliminaries

Along the talk, we consider

- Prime numbers p such that $p \equiv 3 \mod 4$.
- Supersingular elliptic curves $\mathcal{E}$ with $\#\mathcal{E}(\mathbb{F}_{p^2}) = (p \pm 1)^2$ points where $\mathbb{F}_{p^2} = \mathbb{F}_p[i]/(i^2 + 1)$.
- Unless we specify a different model, we center on elliptic curves in Montgomery form (i.e, $\mathcal{E}: y^2 = x^3 + Ax^2 + x$ for some $A \in \mathbb{F}_{p^2}$).
- Small ℓ-isogenies ϕ with cyclic kernels of size $\ell \in \{2, 3\}$.
- Length-n chains of ℓ-isogenies with non-backtracking (i.e., ϕ_{i+1} different from $\hat{\phi}_i$)

$$\mathcal{E}_0 := \mathcal{E} \xrightarrow[\phi_1]{\ell\text{-isogeny}} \mathcal{E}_1 \xrightarrow[\phi_2]{\ell\text{-isogeny}} \mathcal{E}_2 \xrightarrow[\phi_3]{\ell\text{-isogeny}} \cdots \xrightarrow[\phi_n]{\ell\text{-isogeny}} \mathcal{E}' := \mathcal{E}_n$$

Preliminaries

Along the talk, we consider

- Prime numbers p such that $p \equiv 3 \mod 4$.
- Supersingular elliptic curves $\mathcal{E}$ with $\#\mathcal{E}(\mathbb{F}_{p^2}) = (p \pm 1)^2$ points where $\mathbb{F}_{p^2} = \mathbb{F}_p[i]/(i^2+1)$.
- Unless we specify a different model, we center on elliptic curves in Montgomery form (i.e, $\mathcal{E} : y^2 = x^3 + Ax^2 + x$ for some $A \in \mathbb{F}_{p^2}$).
- Small ℓ-isogenies ϕ with cyclic kernels of size $\ell \in \{2, 3\}$.
- Length-n chains of ℓ-isogenies with non-backtracking (i.e., ϕ_{i+1} different from $\hat{\phi}_i$)

$$\mathcal{E}_0 := \mathcal{E} \xrightarrow[\phi_1]{\ell\text{-isogeny}} \mathcal{E}_1 \xrightarrow[\phi_2]{\ell\text{-isogeny}} \mathcal{E}_2 \xrightarrow[\phi_3]{\ell\text{-isogeny}} \cdots \xrightarrow[\phi_n]{\ell\text{-isogeny}} \mathcal{E}' := \mathcal{E}_n$$

Preliminaries

Along the talk, we consider

- Prime numbers p such that $p \equiv 3 \mod 4$.
- Supersingular elliptic curves $\mathcal{E}$ with $\#\mathcal{E}(\mathbb{F}_{p^2}) = (p \pm 1)^2$ points where $\mathbb{F}_{p^2} = \mathbb{F}_p[i]/(i^2 + 1)$.
- Unless we specify a different model, we center on elliptic curves in Montgomery form (i.e, $\mathcal{E} : y^2 = x^3 + Ax^2 + x$ for some $A \in \mathbb{F}_{p^2}$).
- Small ℓ-isogenies ϕ with cyclic kernels of size $\ell \in \{2, 3\}$.
- Length-n chains of ℓ-isogenies with non-backtracking (i.e., ϕ_{i+1} different from $\hat{\phi}_i$)

$$\mathcal{E}_0 := \mathcal{E} \xrightarrow[\phi_1]{\ell\text{-isogeny}} \mathcal{E}_1 \xrightarrow[\phi_2]{\ell\text{-isogeny}} \mathcal{E}_2 \xrightarrow[\phi_3]{\ell\text{-isogeny}} \cdots \xrightarrow[\phi_n]{\ell\text{-isogeny}} \mathcal{E}' := \mathcal{E}_n$$

Preliminaries

Along the talk, we consider

- Prime numbers p such that $p \equiv 3 \bmod 4$.
- Supersingular elliptic curves $\mathcal{E}$ with $\#\mathcal{E}(\mathbb{F}_{p^2}) = (p \pm 1)^2$ points where $\mathbb{F}_{p^2} = \mathbb{F}_p[i]/(i^2+1)$.
- Unless we specify a different model, we center on elliptic curves in Montgomery form (i.e, $\mathcal{E}: y^2 = x^3 + Ax^2 + x$ for some $A \in \mathbb{F}_{p^2}$).
- Small ℓ-isogenies ϕ with cyclic kernels of size $\ell \in \{2, 3\}$.
- Length-n chains of ℓ-isogenies with non-backtracking (i.e., ϕ_{i+1} different from $\hat{\phi}_i$)

$$\mathcal{E}_0 := \mathcal{E} \xrightarrow[\phi_1]{\ell\text{-isogeny}} \mathcal{E}_1 \xrightarrow[\phi_2]{\ell\text{-isogeny}} \mathcal{E}_2 \xrightarrow[\phi_3]{\ell\text{-isogeny}} \cdots \xrightarrow[\phi_n]{\ell\text{-isogeny}} \mathcal{E}' := \mathcal{E}_n$$

Preliminaries

Along the talk, we consider

- Prime numbers p such that $p \equiv 3 \mod 4$.
- Supersingular elliptic curves $\mathcal{E}$ with $\#\mathcal{E}(\mathbb{F}_{p^2}) = (p \pm 1)^2$ points where $\mathbb{F}_{p^2} = \mathbb{F}_p[i]/(i^2 + 1)$.
- Unless we specify a different model, we center on elliptic curves in Montgomery form (i.e, $\mathcal{E} : y^2 = x^3 + Ax^2 + x$ for some $A \in \mathbb{F}_{p^2}$).
- Small ℓ-isogenies ϕ with cyclic kernels of size $\ell \in \{2, 3\}$.
- Length-n chains of ℓ-isogenies with non-backtracking (i.e., ϕ_{i+1} different from $\hat{\phi}_i$)

$$\mathcal{E}_{-1} \xrightarrow[\phi_0]{\ell\text{-isogeny}} \mathcal{E}_0 := \mathcal{E} \xrightarrow[\phi_1]{\ell\text{-isogeny}} \mathcal{E}_1 \xrightarrow[\phi_2]{\ell\text{-isogeny}} \mathcal{E}_2 \xrightarrow[\phi_3]{\ell\text{-isogeny}} \cdots \xrightarrow[\phi_n]{\ell\text{-isogeny}} \mathcal{E}' := \mathcal{E}_n$$

Each ℓ-isogeny path connecting $\mathcal{E}_0$ and $\mathcal{E}_n$ can be encoded by a length-n list of integers in $[1, \ell - 1]$ when given $\mathcal{E}_{-1}$.

Preliminaries

Along the talk, we consider

- Prime numbers p such that $p \equiv 3 \bmod 4$.
- Supersingular elliptic curves $\mathcal{E}$ with $\#\mathcal{E}(\mathbb{F}_{p^2}) = (p \pm 1)^2$ points where $\mathbb{F}_{p^2} = \mathbb{F}_p[i]/(i^2 + 1)$.
- Unless we specify a different model, we center on elliptic curves in Montgomery form (i.e, $\mathcal{E}: y^2 = x^3 + Ax^2 + x$ for some $A \in \mathbb{F}_{p^2}$).
- Small ℓ-isogenies ϕ with cyclic kernels of size $\ell \in \{2, 3\}$.
- Length-n chains of ℓ-isogenies with non-backtracking (i.e., ϕ_{i+1} different from $\hat{\phi}_i$)

$$\begin{tikzcd}
\mathcal{E}_{-1} \arrow[r, "\ell\text{-isogeny}", "\phi_0"'] & \mathcal{E}_0 := \mathcal{E} \arrow[r, "\ell\text{-isogeny}", "\phi_1"'] & \mathcal{E}_1 \arrow[r, "\ell\text{-isogeny}", "\phi_2"'] & \mathcal{E}_2 \arrow[r, "\ell\text{-isogeny}", "\phi_3"'] & \cdots \arrow[r, "\ell\text{-isogeny}", "\phi_n"'] & \mathcal{E}' := \mathcal{E}_n
\end{tikzcd}$$

Each ℓ-isogeny path connecting $\mathcal{E}_0$ and $\mathcal{E}_n$ can be encoded by a length-n list of integers in $[1, \ell - 1]$ when given $\mathcal{E}_{-1}$.

Charles-Goren-Lauter hash function

The Charles-Goren-Lauter hash function [3] determined by $\mathcal{E}_0$ and $\mathcal{E}_{-1}$ is defined as

$$\begin{aligned} \mathrm{CGLHash}_{\ell} \colon \{1, \ldots, \ell - 1\}^* &\to \mathbb{F}_{p^2} \\ \mathrm{path} &\mapsto j(\mathcal{E}_n) \end{aligned} \tag{1}$$

where $n = \#\mathrm{path}$ and $\mathcal{E}_n$ is the end curve of the length-n ℓ-isogeny chain determined by path.

1 Preliminaries

2 **Contributions**

3 On the application to QFESTA

4 On the application to dCTIDH

5 Additional remarks

Contributions (over $\mathbb{F}_{p^2}$)

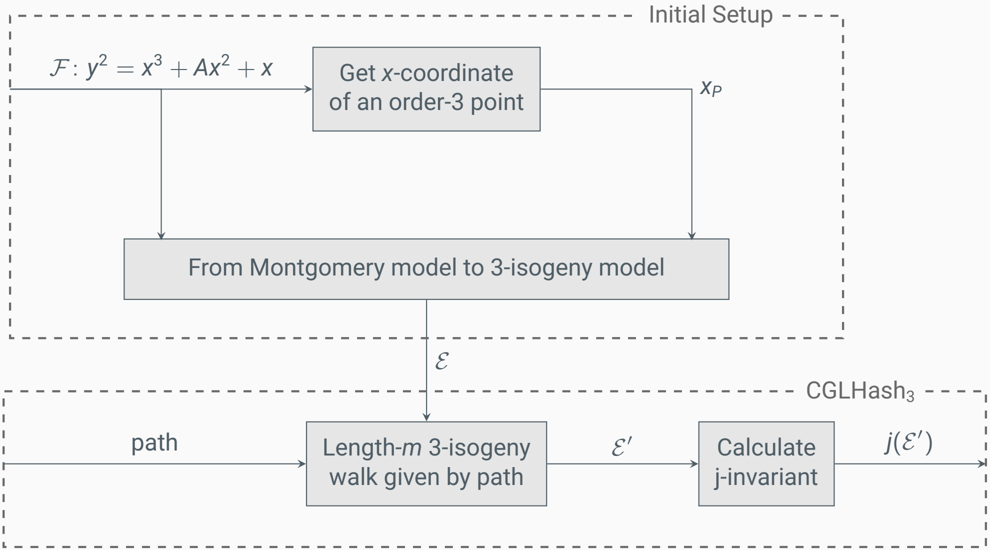
Initial Setup
$\mathcal{F}: y^2 = x^3 + Ax^2 + x$
Get x-coordinate of an order-3 point
x_P
From Montgomery model to 3-isogeny model
$\mathcal{E}$
CGLHash$_3$
path
Length-m 3-isogeny walk given by path
$\mathcal{E}'$
Calculate j-invariant
$j(\mathcal{E}')$

Figure: The superingular elliptic curves $\mathcal{E}$ and $\mathcal{E}'$ are defined over $\mathbb{F}_{p^2}$ and given in the curve model from [2].

Contributions (over $\mathbb{F}_p$)

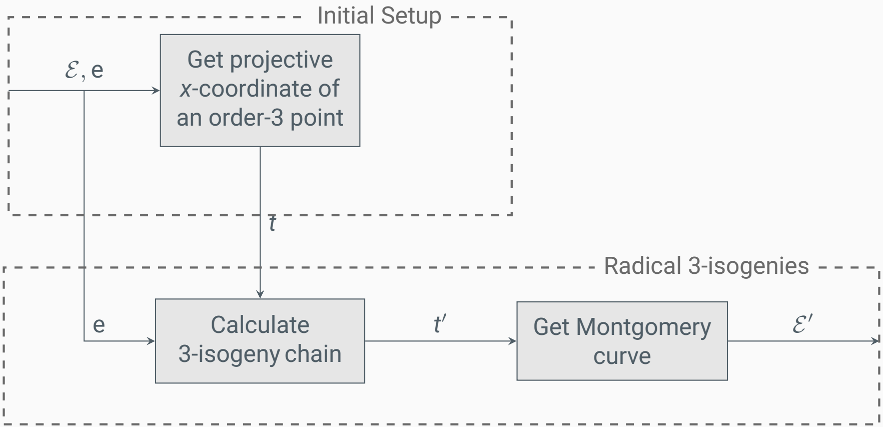

Figure: The superingular elliptic curves $\mathcal{E}$ and $\mathcal{E}'$ are defined over $\mathbb{F}_p$ and given in Montgomery curve form. The block computations describe an efficient projective version of the radical 3-isogeny formulas of [6]

1 Preliminaries

2 Contributions

3 **On the application to QFESTA**

4 On the application to dCTIDH

5 Additional remarks

On the application to QFESTA

QFESTA parameter set	Original	Proposed
QFESTA-128	$p398 = 2^{3\cdot 130}\cdot 3\cdot 55 - 1$	$p381 = 2^{3\cdot 124}\cdot 437 - 1$
QFESTA-192	$p592 = 2^{3\cdot 194}\cdot 3\cdot 307 - 1$	$p575 = 2^{3\cdot 189}\cdot 139 - 1$
QFESTA-256	$p783 = 2^{3\cdot 258}\cdot 3\cdot 137 - 1$	$p765 = 2^{3\cdot 252}\cdot 257 - 1$
Primes bit-length for small $\delta \ll 64$ and an integer t	$(64t + \delta)$	$(64t - \delta)$

- The security analysis of [5] highlights a time complexity for breaking QFESTA of at least $\tilde{O}(2^a)$ where $p = 2^{3a}\cdot 3\cdot f - 1$.
- Our results allow primes not restricted to the form $p = 2^{3a}\cdot 3\cdot f - 1$. They allow a more efficient arithmetic implementation in terms of bit operations since they have one less 64-bits word.
- If we look for smaller $(64t - \delta)$-bits primes of the form $p = 2^{3a}\cdot 3\cdot f - 1$, we end up with parameters with a lower security level than our proposals (i.e., much smaller values of a).
- Our experiments illustrate an improvement between 26.41% and 35.60% in savings for 3-isogeny chain required in QFESTA.

On the application to QFESTA

QFESTA parameter set	Original	Proposed
QFESTA-128	$p398 = 2^{3\cdot 130} \cdot 3 \cdot 55 - 1$	$p381 = 2^{3\cdot 124} \cdot 437 - 1$
QFESTA-192	$p592 = 2^{3\cdot 194} \cdot 3 \cdot 307 - 1$	$p575 = 2^{3\cdot 189} \cdot 139 - 1$
QFESTA-256	$p783 = 2^{3\cdot 258} \cdot 3 \cdot 137 - 1$	$p765 = 2^{3\cdot 252} \cdot 257 - 1$
Primes bit-length for small $\delta \ll 64$ and an integer t	$(64t + \delta)$	$(64t - \delta)$

- The security analysis of [5] highlights a time complexity for breaking QFESTA of at least $\tilde{O}(2^a)$ where $p = 2^{3a} \cdot 3 \cdot f - 1$.
- Our results allow primes not restricted to the form $p = 2^{3a} \cdot 3 \cdot f - 1$. They allow a more efficient arithmetic implementation in terms of bit operations since they have one less 64-bits word.
- If we look for smaller $(64t - \delta)$-bits primes of the form $p = 2^{3a} \cdot 3 \cdot f - 1$, we end up with parameters with a lower security level than our proposals (i.e., much smaller values of a).
- Our experiments illustrate an improvement between 26.41% and 35.60% in savings for 3-isogeny chain required in QFESTA.

On the application to QFESTA

QFESTA parameter set	Original	Proposed
QFESTA-128	$p398 = 2^{3\cdot 130}\cdot 3\cdot 55 - 1$	$p381 = 2^{3\cdot 124}\cdot 437 - 1$
QFESTA-192	$p592 = 2^{3\cdot 194}\cdot 3\cdot 307 - 1$	$p575 = 2^{3\cdot 189}\cdot 139 - 1$
QFESTA-256	$p783 = 2^{3\cdot 258}\cdot 3\cdot 137 - 1$	$p765 = 2^{3\cdot 252}\cdot 257 - 1$
Primes bit-length for small $\delta \ll 64$ and an integer t	$(64t + \delta)$	$(64t - \delta)$

- The security analysis of [5] highlights a time complexity for breaking QFESTA of at least $\tilde{O}(2^a)$ where $p = 2^{3a}\cdot 3\cdot f - 1$.
- Our results allow primes not restricted to the form $p = 2^{3a}\cdot 3\cdot f - 1$. They allow a more efficient arithmetic implementation in terms of bit operations since they have one less 64-bits word.
- If we look for smaller $(64t - \delta)$-bits primes of the form $p = 2^{3a}\cdot 3\cdot f - 1$, we end up with parameters with a lower security level than our proposals (i.e., much smaller values of a).
- Our experiments illustrate an improvement between 26.41% and 35.60% in savings for 3-isogeny chain required in QFESTA.

On the application to QFESTA

QFESTA parameter set	Original	Proposed
QFESTA-128	$p398 = 2^{3\cdot 130} \cdot 3 \cdot 55 - 1$	$p381 = 2^{3\cdot 124} \cdot 437 - 1$
QFESTA-192	$p592 = 2^{3\cdot 194} \cdot 3 \cdot 307 - 1$	$p575 = 2^{3\cdot 189} \cdot 139 - 1$
QFESTA-256	$p783 = 2^{3\cdot 258} \cdot 3 \cdot 137 - 1$	$p765 = 2^{3\cdot 252} \cdot 257 - 1$
Primes bit-length for small $\delta \ll 64$ and an integer t	$(64t + \delta)$	$(64t - \delta)$

- The security analysis of [5] highlights a time complexity for breaking QFESTA of at least $\tilde{O}(2^a)$ where $p = 2^{3a} \cdot 3 \cdot f - 1$.
- Our results allow primes not restricted to the form $p = 2^{3a} \cdot 3 \cdot f - 1$. They allow a more efficient arithmetic implementation in terms of bit operations since they have one less 64-bits word.
- If we look for smaller $(64t - \delta)$-bits primes of the form $p = 2^{3a} \cdot 3 \cdot f - 1$, we end up with parameters with a lower security level than our proposals (i.e., much smaller values of a).
- Our experiments illustrate an improvement between 26.41% and 35.60% in savings for 3-isogeny chain required in QFESTA.

On the application to QFESTA

QFESTA parameter set	Original	Proposed
QFESTA-128	$p398 = 2^{3\cdot 130} \cdot 3 \cdot 55 - 1$	$p381 = 2^{3\cdot 124} \cdot 437 - 1$
QFESTA-192	$p592 = 2^{3\cdot 194} \cdot 3 \cdot 307 - 1$	$p575 = 2^{3\cdot 189} \cdot 139 - 1$
QFESTA-256	$p783 = 2^{3\cdot 258} \cdot 3 \cdot 137 - 1$	$p765 = 2^{3\cdot 252} \cdot 257 - 1$
Primes bit-length for small $\delta \ll 64$ and an integer t	$(64t + \delta)$	$(64t - \delta)$

- The security analysis of [5] highlights a time complexity for breaking QFESTA of at least $\tilde{O}(2^{a})$ where $p = 2^{3a} \cdot 3 \cdot f - 1$.
- Our results allow primes not restricted to the form $p = 2^{3a} \cdot 3 \cdot f - 1$. They allow a more efficient arithmetic implementation in terms of bit operations since they have one less 64-bits word.
- If we look for smaller $(64t - \delta)$-bits primes of the form $p = 2^{3a} \cdot 3 \cdot f - 1$, we end up with parameters with a lower security level than our proposals (i.e., much smaller values of a).
- Our experiments illustrate an improvement between 26.41% and 35.60% in savings for 3-isogeny chain required in QFESTA.

1 Preliminaries

2 Contributions

3 On the application to QFESTA

4 On the application to dCTIDH

5 Additional remarks

On the application to dCTIDH

We emphasize that

- The original dCTIDH work [1] focuses on key derivation and therefore assumes knowledge of a pair of full torsion points, while our results focus on ephemeral key generation scenario.
- Our experiments illustrate a speedup of $\approx$2x on average, while in the best case scenario we obtain close to 4x, for the dCTIDH key generation.
- The speedups in ephemeral key generation are primarily from the omission of the smallest ℓ's along with our optimized technique of finding a point of the correct order.
- The main advantage of our proposal is that it allows us to integrate it straightforwardly into the dCTIDH protocol without changing the prime, that is, without looking for optimal dCTIDH parameters, which are challenging to find, as addressed in [1].

On the application to dCTIDH

We emphasize that

- The original dCTIDH work [1] focuses on key derivation and therefore assumes knowledge of a pair of full torsion points, while our results focus on ephemeral key generation scenario.
- Our experiments illustrate a speedup of ≈2x on average, while in the best case scenario we obtain close to 4x, for the dCTIDH key generation.
- The speedups in ephemeral key generation are primarily from the omission of the smallest ℓ's along with our optimized technique of finding a point of the correct order.
- The main advantage of our proposal is that it allows us to integrate it straightforwardly into the dCTIDH protocol without changing the prime, that is, without looking for optimal dCTIDH parameters, which are challenging to find, as addressed in [1].

On the application to dCTIDH

We emphasize that

- The original dCTIDH work [1] focuses on key derivation and therefore assumes knowledge of a pair of full torsion points, while our results focus on ephemeral key generation scenario.
- Our experiments illustrate a speedup of $\approx$2x on average, while in the best case scenario we obtain close to 4x, for the dCTIDH key generation.
- The speedups in ephemeral key generation are primarily from the omission of the smallest ℓ's along with our optimized technique of finding a point of the correct order.
- The main advantage of our proposal is that it allows us to integrate it straightforwardly into the dCTIDH protocol without changing the prime, that is, without looking for optimal dCTIDH parameters, which are challenging to find, as addressed in [1].

On the application to dCTIDH

We emphasize that

- The original dCTIDH work [1] focuses on key derivation and therefore assumes knowledge of a pair of full torsion points, while our results focus on ephemeral key generation scenario.
- Our experiments illustrate a speedup of $\approx$2x on average, while in the best case scenario we obtain close to 4x, for the dCTIDH key generation.
- The speedups in ephemeral key generation are primarily from the omission of the smallest ℓ's along with our optimized technique of finding a point of the correct order.
- The main advantage of our proposal is that it allows us to integrate it straightforwardly into the dCTIDH protocol without changing the prime, that is, without looking for optimal dCTIDH parameters, which are challenging to find, as addressed in [1].

1 Preliminaries

2 Contributions

3 On the application to QFESTA

4 On the application to dCTIDH

5 Additional remarks

Additional remarks

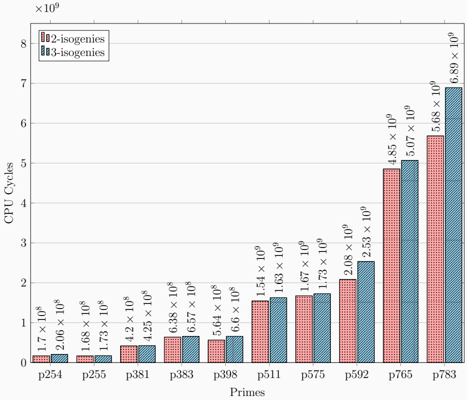

Figure: Benchmarks for the 2-isogenies vs. 3-isogenies walks, measured in CPU cycles.

Open questions for future research:

- Can we speed up the cube-root calculation over $\mathbb{F}_{p^2}$? This would imply that faster radical 3-isogenies chains (potentially faster than 2-isogeny chains!)
- Can radical 3-isogeny chains improve the VDF proposed by Chávez-Saab, Rodríguez-Henríquez, and Tibouchi [4]? It could be the case since we have shorter isogeny chains!
- Can we extend our results to the radical 5-isogeny scenario? A deterministic algorithm for calculating order-5 points (over arbitrary curves) reduce to finding roots of a degree-6 polynomial!

Additional remarks

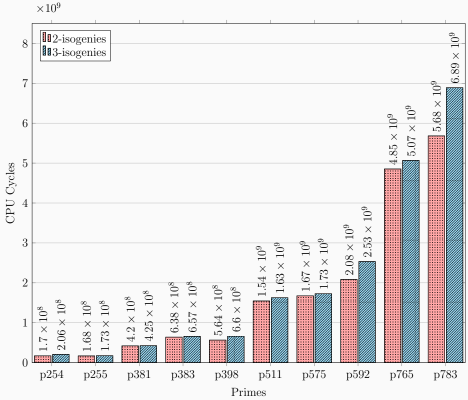

Figure: Benchmarks for the 2-isogenies vs. 3-isogenies walks, measured in CPU cycles.

Open questions for future research:

- Can we speed up the cube-root calculation over $\mathbb{F}_{p^2}$? This would imply that faster radical 3-isogenies chains (potentially faster than 2-isogeny chains!)
- Can radical 3-isogeny chains improve the VDF proposed by Chávez-Saab, Rodríguez-Henríquez, and Tibouchi [4]? It could be the case since we have shorter isogeny chains!
- Can we extend our results to the radical 5-isogeny scenario? A deterministic algorithm for calculating order-5 points (over arbitrary curves) reduce to finding roots of a degree-6 polynomial!

Additional remarks

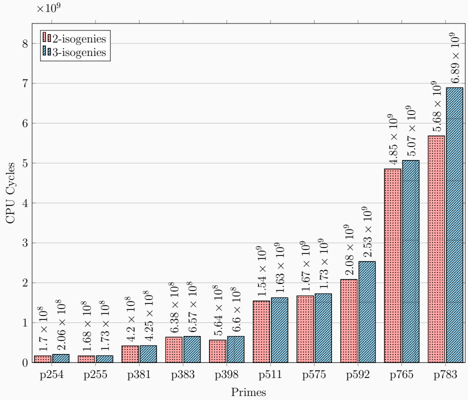

Figure: Benchmarks for the 2-isogenies vs. 3-isogenies walks, measured in CPU cycles.

Open questions for future research:

- Can we speed up the cube-root calculation over $\mathbb{F}_{p^2}$? This would imply that faster radical 3-isogenies chains (potentially faster than 2-isogeny chains!)
- Can radical 3-isogeny chains improve the VDF proposed by Chávez-Saab, Rodríguez-Henríquez, and Tibouchi [4]? It could be the case since we have shorter isogeny chains!
- Can we extend our results to the radical 5-isogeny scenario? A deterministic algorithm for calculating order-5 points (over arbitrary curves) reduce to finding roots of a degree-6 polynomial!

Questions?

We thank Andreas Hellenbrand for the useful comments on the dCTIDH experiments.

Thanks for attending!

References I

[1] Fabio Campos, Andreas Hellenbrand, Michael Meyer, and Krijn Reijnders.
dCTIDH: Fast &; Deterministic CTIDH.
IACR Transactions on Cryptographic Hardware and Embedded Systems, 2025(3):516–541, Jun. 2025.

[2] Wouter Castryck, Thomas Decru, and Frederik Vercauteren.
Radical isogenies.
In Shiho Moriai and Huaxiong Wang, editors, *ASIACRYPT 2020, Part II*, volume 12492 of *LNCS*, pages 493–519. Springer, Cham, December 2020.

[3] Denis Xavier Charles, Kristin E. Lauter, and Eyal Z. Goren.
Cryptographic hash functions from expander graphs.
Journal of Cryptology, 22(1):93–113, January 2009.

[4] Jorge Chávez-Saab, Francisco Rodríguez-Henríquez, and Mehdi Tibouchi.
Verifiable isogeny walks: Towards an isogeny-based postquantum VDF.
In Riham AlTawy and Andreas Hülsing, editors, *SAC 2021*, volume 13203 of *LNCS*, pages 441–460. Springer, Cham, September / October 2022.

[5] Kohei Nakagawa and Hiroshi Onuki.
QFESTA: Efficient algorithms and parameters for FESTA using quaternion algebras.
In Leonid Reyzin and Douglas Stebila, editors, *CRYPTO 2024, Part V*, volume 14924 of *LNCS*, pages 75–106. Springer, Cham, August 2024.

References II

[6] Hiroshi Onuki and Tomoki Moriya.
Radical isogenies on montgomery curves.
In Goichiro Hanaoka, Junji Shikata, and Yohei Watanabe, editors, *PKC 2022, Part I*, volume 13177 of *LNCS*, pages 473–497. Springer, Cham, March 2022.