Supersingular Curves with Small Non-integer Endomorphisms

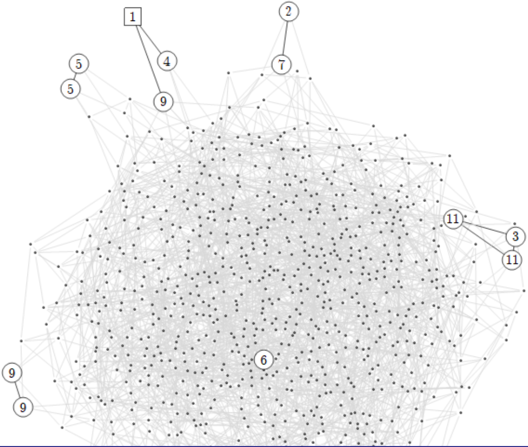
Jonathan Love[1] Dan Boneh[2]

[1]Department of Mathematics, Stanford University
https://stanford.edu/~jonlove

[2]Department of Computer Science, Stanford University
https://stanford.edu/~dabo

Algorithmic Number Theory Symposium, June 2020

Preview



Main Goal

Describe a manageable subclass of supersingular curves and analyze its structure.

Outline

Outline

Elliptic Curves

Throughout:

- $p \geq 5$ is a prime,

Elliptic Curves

Throughout:

- $p \geq 5$ is a prime,
- F is a finite field of characteristic p,
- E and E' are elliptic curves defined over F.

Isogenies

Isogeny $\phi : E \to E'$: a non-constant map of algebraic varieties (i.e. given by rational functions in x and y) that sends O to O. We will assume isogenies are defined over $\overline{F}$.

Isogenies

Isogeny $\phi : E \to E'$: a non-constant map of algebraic varieties (i.e. given by rational functions in x and y) that sends O to O. We will assume isogenies are defined over $\overline{F}$.

An isogeny $E \to E'$ induces a homomorphism $E\left(\overline{F}\right) \to E'\left(\overline{F}\right)$.

Isogenies

Isogeny $\phi : E \to E'$: a non-constant map of algebraic varieties (i.e. given by rational functions in x and y) that sends O to O. We will assume isogenies are defined over $\overline{F}$.

An isogeny $E \to E'$ induces a homomorphism $E\left(\overline{F}\right) \to E'\left(\overline{F}\right)$.

Degree of ϕ: degree as a map of varieties. This equals the size of the kernel of $\phi : E\left(\overline{F}\right) \to E'\left(\overline{F}\right)$ when ϕ is separable.

Isogenies

Isogeny $\phi : E \to E'$: a non-constant map of algebraic varieties (i.e. given by rational functions in x and y) that sends O to O. We will assume isogenies are defined over $\overline{F}$.

An isogeny $E \to E'$ induces a homomorphism $E\left(\overline{F}\right) \to E'\left(\overline{F}\right)$.

Degree of ϕ: degree as a map of varieties. This equals the size of the kernel of $\phi : E\left(\overline{F}\right) \to E'\left(\overline{F}\right)$ when ϕ is separable.

Example

If $E : y^2 = x^3 + x$ and $E' : y^2 = x^3 - 4x$, then

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

is an isogeny of degree 2 from E to E', with kernel $\{(0,0), O\}$.

Endomorphisms

Endomorphism of E: an isogeny $E \to E$. The constant map $P \mapsto O$ is also considered to be an endomorphism.

Endomorphisms

Endomorphism of E: an isogeny $E \to E$. The constant map $P \mapsto O$ is also considered to be an endomorphism.

Example

For any $n \in \mathbb{Z}$, the map $P \mapsto nP$ is an endomorphism of degree n^2.

Endomorphisms

Endomorphism of E: an isogeny $E \to E$. The constant map $P \mapsto O$ is also considered to be an endomorphism.

Example

For any $n \in \mathbb{Z}$, the map $P \mapsto nP$ is an endomorphism of degree n^2.

Example

If $E : y^2 = x^3 + x$, then

$$(x, y) \mapsto (-x, iy)$$

is a non-integer endomorphism of degree 1.

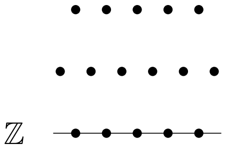
Endomorphism Ring

Endomorphism Ring of E, $\mathrm{End}(E)$: the set of endomorphisms of E under pointwise addition and composition.

Endomorphism Ring

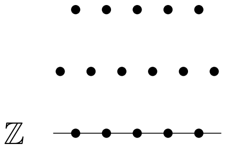
Endomorphism Ring of E, $\mathrm{End}(E)$: the set of endomorphisms of E under pointwise addition and composition.

E is ordinary
if $\mathrm{End}(E)$ is 2-dimensional
(order in some $\mathbb{Q}(\sqrt{D})$)

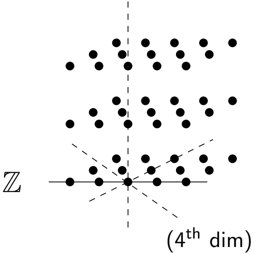


Endomorphism Ring of E, $\mathrm{End}(E)$: the set of endomorphisms of E under pointwise addition and composition.

E is ordinary
if $\mathrm{End}(E)$ is 2-dimensional
(order in some $\mathbb{Q}(\sqrt{D})$)



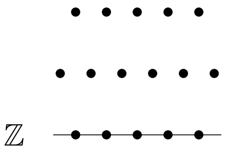
E is supersingular
if $\mathrm{End}(E)$ is 4-dimensional
(order in a quaternion algebra)



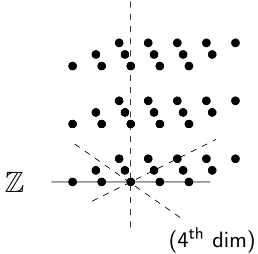
Endomorphism Ring

Endomorphism Ring of E, $\mathrm{End}(E)$: the set of endomorphisms of E under pointwise addition and composition.

E is ordinary
if $\mathrm{End}(E)$ is 2-dimensional
(order in some $\mathbb{Q}(\sqrt{D})$)



E is supersingular
if $\mathrm{End}(E)$ is 4-dimensional
(order in a quaternion algebra)



In both cases, degree = norm.

Outline

ℓ-isogeny graphs

Let $\ell \neq p$ be a prime, and define a graph as follows:

- Vertices: elliptic curves over F (up to isomorphism)
- Edges: isogenies of degree ℓ

ℓ-isogeny graphs

Let $\ell \neq p$ be a prime, and define a graph as follows:

- Vertices: elliptic curves over F (up to isomorphism)
- Edges: isogenies of degree ℓ

Example: elliptic curves over $\mathbb{F}_{p^2}$ with $p = 401$, $\ell = 3$.

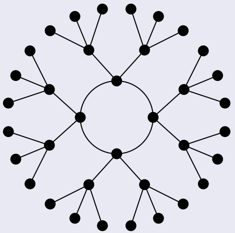
ℓ-isogeny graphs

Let $\ell \neq p$ be a prime, and define a graph as follows:

- Vertices: elliptic curves over F (up to isomorphism)
- Edges: isogenies of degree ℓ

Example: elliptic curves over $\mathbb{F}_{p^2}$ with $p = 401$, $\ell = 3$.

An ordinary component:



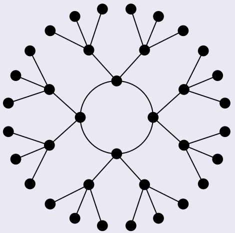
ℓ-isogeny graphs

Let $\ell \neq p$ be a prime, and define a graph as follows:

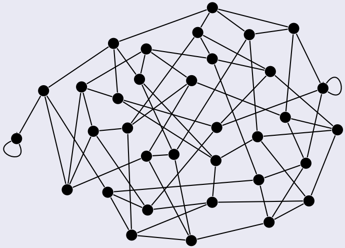
- Vertices: elliptic curves over F (up to isomorphism)
- Edges: isogenies of degree ℓ

Example: elliptic curves over $\mathbb{F}_{p^2}$ with $p = 401$, $\ell = 3$.

An ordinary component:



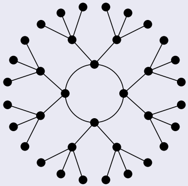
The supersingular component:



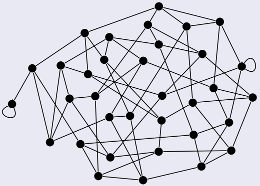
ℓ-isogeny graphs

Example: elliptic curves over $\mathbb{F}_{p^2}$ with $p = 401$, $\ell = 3$.

An ordinary component:



The supersingular component:



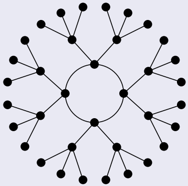
- Each ordinary component has the structure of a volcano.[1]

[1] Andrew Sutherland. *Isogeny Volcanoes*, The Open Book Series 1, Aug 2012.

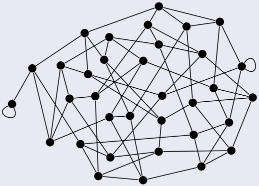
ℓ-isogeny graphs

Example: elliptic curves over $\mathbb{F}_{p^2}$ with $p = 401$, $\ell = 3$.

An ordinary component:



The supersingular component:



- Each ordinary component has the structure of a volcano.[1]
- There is a unique supersingular component, and it has the structure of a Ramanjuan graph[2] (implies that random walks converge rapidly to the uniform distribution).

[1] Andrew Sutherland. *Isogeny Volcanoes*, The Open Book Series 1, Aug 2012.

[2] Pizer, A.K. *Ramanujan Graphs and Hecke Operators*, Bulletin of the AMS, Volume 23, Number 1, July 1990.

Supersingular Isogeny Graphs in Cryptography

Hard Problem:

Given two random supersingular curves E and E', find an isogeny $E \to E'$.

Supersingular Isogeny Graphs in Cryptography

Hard Problem:

Given two random supersingular curves E and E', find an isogeny $E \to E'$.

- Hash function[3]

[3] Denis Charles, Kritin Lauter, Eyal Goren. *Cryptographic Hash Functions from Expander Graphs.* Journal of Cryptology 22, 93–113 (2009).

Supersingular Isogeny Graphs in Cryptography

Hard Problem:

Given two random supersingular curves E and E', find an isogeny $E \to E'$.

- Hash function[3]
- Diffie-Hellman Key Exchange[4]

[3] Denis Charles, Kritin Lauter, Eyal Goren. *Cryptographic Hash Functions from Expander Graphs.* Journal of Cryptology 22, 93–113 (2009).

[4] Luca De Feo, David Jao, Jérôme Plût. *Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies.* Journal of Mathematical Cryptology 8(3), 209-247.

Supersingular Isogeny Graphs in Cryptography

Hard Problem:

Given two random supersingular curves E and E', find an isogeny $E \to E'$.

- Hash function[3]
- Diffie-Hellman Key Exchange[4]
- CSIDH (a modified approach to Diffie-Hellman)[5]

[3] Denis Charles, Kritin Lauter, Eyal Goren. *Cryptographic Hash Functions from Expander Graphs.* Journal of Cryptology 22, 93–113 (2009).

[4] Luca De Feo, David Jao, Jérôme Plût. *Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies.* Journal of Mathematical Cryptology 8(3), 209-247.

[5] Wouter Castryck et al. *CSIDH: An Efficient Post-Quantum Commutative Group Action.* IACR Cryptol. ePrint Arch. (2018): 383.

Supersingular Isogeny Graphs in Cryptography

Hard Problem:

Given two random supersingular curves E and E', find an isogeny $E \to E'$.

- Hash function[3]
- Diffie-Hellman Key Exchange[4]
- CSIDH (a modified approach to Diffie-Hellman)[5]
- And more!

---

[3] Denis Charles, Kritin Lauter, Eyal Goren. *Cryptographic Hash Functions from Expander Graphs.* Journal of Cryptology 22, 93–113 (2009).

[4] Luca De Feo, David Jao, Jérôme Plût. *Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies.* Journal of Mathematical Cryptology 8(3), 209-247.

[5] Wouter Castryck et al. *CSIDH: An Efficient Post-Quantum Commutative Group Action.* IACR Cryptol. ePrint Arch. (2018): 383.

Finding supersingular curves

Rare: about $\frac{1}{12p}$ of elliptic curves over $\mathbb{F}_{p^2}$ are supersingular.

Finding supersingular curves

Rare: about $\frac{1}{12p}$ of elliptic curves over $\mathbb{F}_{p^2}$ are supersingular.

Bröker's algorithm[6] finds one supersingular curve:

- Find an elliptic curve with complex multiplication, defined over a number field K.
- Reduce modulo a prime of K dividing p.
- Under certain congruence conditions, the result is supersingular.

[6] Reinier Bröker. *Constructing supersingular elliptic curves.* Frontiers of Combinatorics and Number Theory, Jan 2009.

Finding supersingular curves

Rare: about $\frac{1}{12p}$ of elliptic curves over $\mathbb{F}_{p^2}$ are supersingular.

Bröker's algorithm[6] finds one supersingular curve:

- Find an elliptic curve with complex multiplication, defined over a number field K.
- Reduce modulo a prime of K dividing p.
- Under certain congruence conditions, the result is supersingular.

Then take a random walk in an ℓ-isogeny graph to obtain a random supersingular curve.

[6] Reinier Bröker. *Constructing supersingular elliptic curves.* Frontiers of Combinatorics and Number Theory, Jan 2009.

Finding hard supersingular curves

A supersingular curve E is "hard" if no one (not even the party who generated E) can efficiently compute $\mathrm{End}(E)$.

Finding hard supersingular curves

A supersingular curve E is "hard" if no one (not even the party who generated E) can efficiently compute $\mathrm{End}(E)$.

Motivation: In some cryptographic applications,[7] knowing $\mathrm{End}(E)$ allows for the creation of backdoors. A hard curve would eliminate the need for trusted setup.

[7] For one example: Luca De Feo, Simon Masson, Christophe Petit, and Antonio Sanso. *Verifiable Delay Functions from Supersingular Isogenies and Pairings*. IACR Cryptology ePrint Archive, 2019.

Finding hard supersingular curves

A supersingular curve E is "hard" if no one (not even the party who generated E) can efficiently compute $\mathrm{End}(E)$.

Motivation: In some cryptographic applications,[7] knowing $\mathrm{End}(E)$ allows for the creation of backdoors. A hard curve would eliminate the need for trusted setup.

Open Problem

Find an explicit hard supersingular elliptic curve.

[7] For one example: Luca De Feo, Simon Masson, Christophe Petit, and Antonio Sanso. *Verifiable Delay Functions from Supersingular Isogenies and Pairings*. IACR Cryptology ePrint Archive, 2019.

Outline

M-small Curves

Consider:

- p: A "cryptographic" prime (e.g. $p \sim 2^{200}$)
- M: A "reasonable" parameter (e.g. $M \sim 2^{10}$)

M-small Curves

Consider:

- p: A "cryptographic" prime (e.g. $p \sim 2^{200}$)
- M: A "reasonable" parameter (e.g. $M \sim 2^{10}$)

Definition

An elliptic curve E over a finite field of characteristic p is M-**small** if there exists $\alpha \in \mathrm{End}(E) - \mathbb{Z}$ with $\deg \alpha \leq M$.

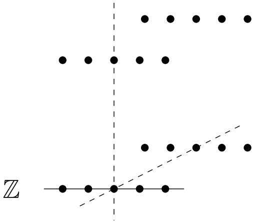
Visualizing M-small endomorphism rings

What does (a 3-dimensional slice of) the endomorphism ring of a supsersingular curve look like?

Visualizing M-small endomorphism rings

What does (a 3-dimensional slice of) the endomorphism ring of a supsersingular curve look like?

Typical:

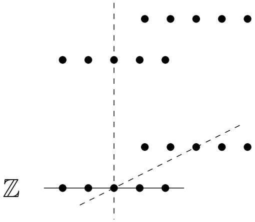


Smallest degree of non-integer endomorphism $\sim p^{2/3}$

Visualizing M-small endomorphism rings

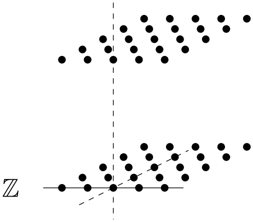
What does (a 3-dimensional slice of) the endomorphism ring of a supsersingular curve look like?

Typical:



Smallest degree of non-integer endomorphism $\sim p^{2/3}$

M-small:



Smallest degree of non-integer endomorphism $\leq M$

Distribution of M-small Curves

Distribution of M-small Curves

- The number of M-small curves is $O(M^{3/2})$.

Distribution of M-small Curves

- The number of M-small curves is $O(M^{3/2})$.
- The set of M-small curves can be generated efficiently using a generalization of Bröker's algorithm.

Distribution of M-small Curves

- The number of M-small curves is $O(M^{3/2})$.
- The set of M-small curves can be generated efficiently using a generalization of Bröker's algorithm.
- When $M \ll p$, approximately half of all M-small curves appear to be supersingular.

Distribution of M-small Curves

- The number of M-small curves is $O(M^{3/2})$.
- The set of M-small curves can be generated efficiently using a generalization of Bröker's algorithm.
- When $M \ll p$, approximately half of all M-small curves appear to be supersingular.
- Endomorphism rings of M-small curves, and isogenies between them, can be computed efficiently.

Distribution of M-small Curves

- The number of M-small curves is $O(M^{3/2})$.
- The set of M-small curves can be generated efficiently using a generalization of Bröker's algorithm.
- When $M \ll p$, approximately half of all M-small curves appear to be supersingular.
- Endomorphism rings of M-small curves, and isogenies between them, can be computed efficiently.
- The set of M-small supersingular curves forms "clusters" indexed by fundamental discriminants.

"Clustering" Theorem

Theorem 1.3

Suppose $p \gg M$. The set of M-small supersingular curves partitions into sets T_D, for fundamental discriminants $-4M \leq D < 0$ with $\left(\frac{D}{p}\right) = -1$.

"Clustering" Theorem

Theorem 1.3

Suppose $p \gg M$. The set of M-small supersingular curves partitions into sets T_D, for fundamental discriminants $-4M \leq D < 0$ with $\left(\frac{D}{p}\right) = -1$.

- If E, E' are in distinct subsets $T_D \neq T_{D'}$, then any isogeny $E \to E'$ has degree at least $\frac{\sqrt{p}}{2M}$.

"Clustering" Theorem

Theorem 1.3

Suppose $p \gg M$. The set of M-small supersingular curves partitions into sets T_D, for fundamental discriminants $-4M \leq D < 0$ with $\left(\frac{D}{p}\right) = -1$.

- If E, E' are in distinct subsets $T_D \neq T_{D'}$, then any isogeny $E \to E'$ has degree at least $\frac{\sqrt{p}}{2M}$.
- If E, E' are in the same subset T_D, then they can be linked[a] by a chain of isogenies of degree at most $\frac{4}{\pi}\sqrt{M}$ between elements of T_D.

"Clustering" Theorem

Theorem 1.3

Suppose $p \gg M$. The set of M-small supersingular curves partitions into sets T_D, for fundamental discriminants $-4M \leq D < 0$ with $\left(\frac{D}{p}\right) = -1$.

- If E, E' are in distinct subsets $T_D \neq T_{D'}$, then any isogeny $E \to E'$ has degree at least $\frac{\sqrt{p}}{2M}$.
- If E, E' are in the same subset T_D, then they can be linked[a] by a chain of isogenies of degree at most $\frac{4}{\pi}\sqrt{M}$ between elements of T_D.

[a] One may need to replace E' with its Frobenius conjugate $E'^{(p)}$.

"Clustering" Theorem

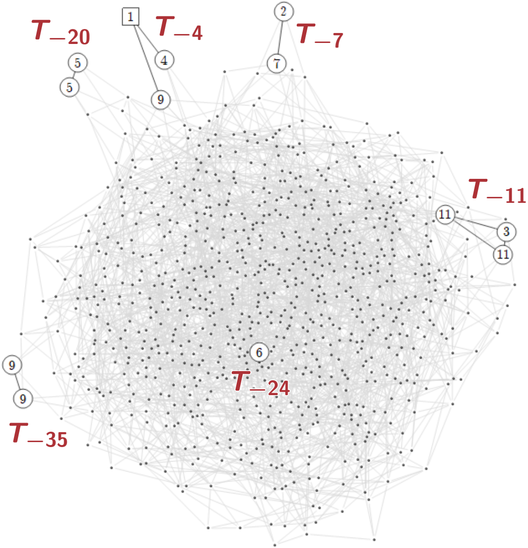


Figure: Supersingular curves in characteristic $p = 20011$ (modulo conjugation on $\mathbb{F}_{p^2}$). Edges: isogenies of prime degree at most $\frac{4}{\pi}\sqrt{12} \approx 4.4$. 12-small curves labelled with smallest degree of a non-integer endomorphism.

“Clustering” Theorem

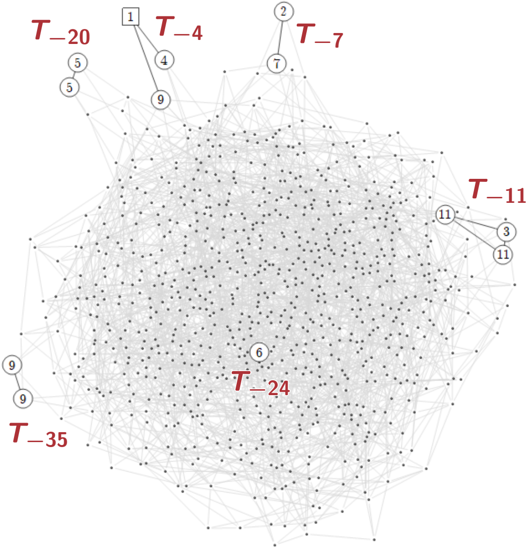


Figure: Supersingular curves in characteristic $p = 20011$ (modulo conjugation on $\mathbb{F}_{p^2}$). Edges: isogenies of prime degree at most $\frac{4}{\pi}\sqrt{12} \approx 4.4$. 12-small curves labelled with smallest degree of a non-integer endomorphism.

Despite their distance, we can compute (large-degree) isogenies between the clusters!

No clustering in ℓ-isogeny graphs

This clustering is not evident in ℓ-isogeny graphs for any individual ℓ. We must consider all sufficiently small primes to see clustering.

No clustering in ℓ-isogeny graphs

This clustering is not evident in ℓ-isogeny graphs for any individual ℓ. We must consider all sufficiently small primes to see clustering.

Corollary C.2

Suppose ℓ is a prime such that an (M/ℓ^2)-small supersingular curve exists. Then there are two M-small supersingular curves E, E', linked by an isogeny of degree ℓ, such that for any isogeny $\phi : E \to E'$ with degree relatively prime to ℓ,

$$\deg \phi \geq \frac{p\ell}{4M}.$$

No clustering in ℓ-isogeny graphs

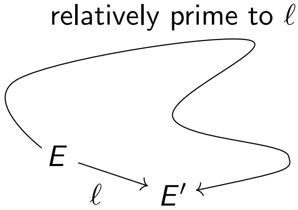
This clustering is not evident in ℓ-isogeny graphs for any individual ℓ. We must consider all sufficiently small primes to see clustering.

Corollary C.2

Suppose ℓ is a prime such that an (M/ℓ^2)-small supersingular curve exists. Then there are two M-small supersingular curves E, E', linked by an isogeny of degree ℓ, such that for any isogeny $\phi : E \to E'$ with degree relatively prime to ℓ,

$$\deg \phi \geq \frac{p\ell}{4M}.$$

In other words,



Conclusion

- We have defined a set of supersingular curves that is relatively easy to analyze and to work with.

Conclusion

- We have defined a set of supersingular curves that is relatively easy to analyze and to work with.
- We can compute isogenies between these curves that could not reasonably be found by an ℓ-isogeny graph search.

Conclusion

- We have defined a set of supersingular curves that is relatively easy to analyze and to work with.
- We can compute isogenies between these curves that could not reasonably be found by an ℓ-isogeny graph search.

Thank you for listening!

Questions/Comments?

jonlove@stanford.edu dabo@cs.stanford.edu