Isolated Curves and Cryptography

Travis Scholl

University of California, Irvine

March 23, 2019
Elliptic Curve Discrete Log Problem (ECDLP)

Given an elliptic curve $E/\mathbb{F}_p$ and points $P, Q \in E(\mathbb{F}_p)$, find $k \in \mathbb{Z}$ such that $Q = kP$. 

If $\varphi : E \to E'$ is an isogeny of elliptic curves and $P, Q \in E(\mathbb{F}_p)$, then

$$Q = kP \implies \varphi(Q) = k\varphi(P).$$
Isogeny Class

Weak Curves

\( E \)
Isogeny Class

Weak Curves

$E'$  $\varphi$  $E$
Isogeny Class

$E$
Definition

$E$ is super-isolated if its isogeny class contains only $E$.

Goal

Find super-isolated curves.
Let $I$ be the isogeny class of $E/\mathbb{F}_p$, and assume that $E$ is ordinary.

**Facts**

- $\text{End } E$ is an order $\mathcal{O}$ in a quadratic imaginary field $K$.
- $\mathcal{O} \supseteq \mathbb{Z}[\pi]$ where $\pi$ is the Frobenius endomorphism.
- $\# \{E' \in I : \text{End } E' \cong \mathcal{O} \}$ is the class number of $\mathcal{O}$. 
Example

Figure: The isogeny class of $E : y^2 = x^3 + x$ over $\mathbb{F}_{37}$ partitioned into endomorphism classes. Here $\pi = 1 + 6i$. 
Theorem

$E$ is super-isolated if and only if $\mathbb{Z}[\pi] = \mathcal{O}_K$ and $h(K) = 1$. 

Example

Let $E/F_5$ be the curve $y^2 = x^3 + 2x$. Then $\pi = 2 + i$, so $E$ is super-isolated.
Theorem

$E$ is super-isolated if and only if $\mathbb{Z}[[\pi]] = \mathcal{O}_K$ and $h(K) = 1$.

Example

Let $E/\mathbb{F}_5$ be the curve $y^2 = x^3 + 2x$. Then $\pi = 2 + i$, so $E$ is super-isolated.
Introduction

Background

Construction

Generalization
Complex Multiplication (CM) Method

(1) Find an integer $A \in \mathbb{Z}$ such that $p = A^2 + 1$ is a large prime.

(2) Choose $\lambda \in \mathbb{F}_p$ such that the elliptic curve $E$ given by $y^2 = x^3 + \lambda x$ over $\mathbb{F}_p$ has $A^2 - 2A + 2$ points.
Complex Multiplication (CM) Method

(1) Find an integer $A \in \mathbb{Z}$ such that $p = A^2 + 1$ is a large prime.

(2) Choose $\lambda \in \mathbb{F}_p$ such that the elliptic curve $E$ given by $y^2 = x^3 + \lambda x$ over $\mathbb{F}_p$ has $A^2 - 2A + 2$ points.

This works because the Frobenius of $E$ is $\pi = A + i$ so $\mathbb{Z}[\pi] = \mathbb{Z}[i]$. 
Complex Multiplication (CM) Method

(1) Find an integer \( A \in \mathbb{Z} \) such that \( p = A^2 + 1 \) is a large prime.
(2) Choose \( \lambda \in \mathbb{F}_p \) such that the elliptic curve \( E \) given by \( y^2 = x^3 + \lambda x \) over \( \mathbb{F}_p \) has \( A^2 - 2A + 2 \) points.

This works because the Frobenius of \( E \) is \( \pi = A + i \) so \( \mathbb{Z}[\pi] = \mathbb{Z}[i] \).

**Question**

How many \( A \) are there?
Open Question

\[
\# \{ A \in \mathbb{Z} : A^2 + 1 \text{ is prime} \} \not= \infty.
\]
Open Question

\[
\# \{A \in \mathbb{Z} : A^2 + 1 \text{ is prime}\} \neq \infty.
\]

Conjecture

\[
\# \{A \in \mathbb{Z} : A^2 + 1 \text{ is prime, } A \leq M\} = \Theta \left( \frac{\sqrt{M}}{\log M} \right).
\]
Open Question

\[ \# \{ A \in \mathbb{Z} : A^2 + 1 \text{ is prime} \} = \infty. \]

Conjecture

\[ \# \{ A \in \mathbb{Z} : A^2 + 1 \text{ is prime, } A \leq M \} = \Theta \left( \frac{\sqrt{M}}{\log M} \right). \]

Heuristic

\[ \{ E/\mathbb{F}_p : E \text{ super-isolated, } p \leq M \} = \Theta \left( \frac{\sqrt{M}}{\log M} \right). \]
Introduction

Background

Construction

Generalization
Definition
An abelian variety $A/F_q$ is super-isolated if $\#I = 1$. 

Theorem ([Wat69])
Let $A/F_q$ be a simple ordinary abelian variety, $\pi$ a root of the characteristic polynomial of the Frobenius endomorphism, and let $K = \mathbb{Q}(\pi)$. Then $A$ is super-isolated if and only if $\mathcal{O}_K = \mathbb{Z}[\pi, \pi]$ and $K$ has class number $1$. 
Definition
An abelian variety $A/\mathbb{F}_q$ is super-isolated if $\#I = 1$.

Theorem ([Wat69])

Let $A/\mathbb{F}_q$ be a simple ordinary abelian variety, $\pi$ a root of the characteristic polynomial of the Frobenius endomorphism, and let $K = \mathbb{Q}(\pi)$. Then $A$ is super-isolated if and only if $\mathcal{O}_K = \mathbb{Z}[\pi, \bar{\pi}]$ and $K$ has class number 1.
Example (Dimension 4)
The Jacobian of the genus 4 hyperelliptic curve over $\mathbb{F}_2$ given by

$$y^2 + (x^5 + x^3 + 1)y = x^9 + x^6$$

is super-isolated. The minimal polynomial of $\pi$ is

$$x^8 + 3x^7 + 7x^6 + 13x^5 + 19x^4 + 26x^3 + 28x^2 + 24x + 16.$$  

[link]

http://www.lmfdb.org/Variety/Abelian/Fq/4/2/d_h_n_t
Heuristic (S.)

Let $S(M)$ denote the number of simple ordinary super-isolated abelian varieties of dimension $g$ over $\mathbb{F}_q$ with $q \leq M$. Then

$$S(M) = \begin{cases} \Theta \left( \frac{\sqrt{M}}{\log M} \right), & \text{if } g = 1 \text{ (related to [BH62])} \\ \Theta (\log \log M), & \text{if } g = 2 \text{ (related to [CP05])}. \end{cases}$$

Theorem (S.)

If $g \geq 3$, then $S(M) = O(1)$. 
Ideas

Looking for super-isolated curves reduces to finding Weil $q$-numbers $\pi$ such that $\mathbb{Z}[\pi, \bar{\pi}]$ is maximal. We instead count Weil generators in a CM field $K$, which are $\pi \in K$ such that

- $\pi \bar{\pi} \in \mathbb{Z}$
- $\mathbb{Z}[\pi, \bar{\pi}] = \mathcal{O}_K$
To count Weil generators in a CM field $K$ of degree $2g$, we split into cases by $g$.

$g = 1$
Here $\mathcal{O}_K = \mathbb{Z}[\omega]$, and we are counting $a \in \mathbb{Z}$ with $h(a \pm \omega) \leq N$.

$g = 2$
Here $W$ corresponds to some proportion of $\mathcal{O}_F^\times$.

$g \geq 3$
Here $W$ essentially corresponds to integer points on a degree $g$ curve with $g$ distinct points at infinity, so we may apply Siegel’s theorem.
Theorem (S.)

Let $K$ be a CM field of degree $2g$, and let $W$ be the set of Weil generators in $K$. Then

$$\# \{ \alpha \in W : h(\alpha) \leq N \} = \begin{cases} 4N + O(1) & g = 1 \\ \rho \log N + O(1) & g = 2 \text{ and } W \neq \emptyset \\ O(1) & g \geq 3. \end{cases}$$

Note
This is a theorem because it does not include the word “prime”.
Thank you for listening.

