Isogenies in cryptography

F. Morain

Laboratoire d'Informatique de l'École polytechnique

University of Waterloo, June 17, 2009

Plan

I. Introduction.

II. Elliptic curves and isogenies.

III. Computations and algorithms.

IV. Isogeny graphs and cryptographic applications.

I. Introduction

A short history:

- 1990ff: Schoof-Elkies-Atkin (SEA), Couveignes-FM, Dewaghe (isogeny cycles);
- Kohel, Galbraith, Fouquet-FM (volcanoes);
- Galbraith-Hess-Smart; Smart; Jao-Miller-Venkatesan; Teske; Rostovtsev-Stolbunov; Charles-Goren-Lauter.
- Quite recently: finding good Edwards curves (FM); CRT methods for computing class (resp. modular) polynomials(Sutherland *et al.*).

Bibliography:

- Silverman; Lang's *Elliptic functions*.
- green book (Blake, Seroussi, Smart). Don't forget to read the original papers, when available...
- Gathen & Gerhard, etc.

Different usages

- Generalize $[m]$ on E:
  - factor f_m: SEA.
  - speed up the computation of $[k]P$ when small degree isogeny exist (Doche-Icart-Kohel).
- Replace E by some sister or cousin having better or stronger properties:
  - find $\tilde{E}$ of the same cardinality, but $Y^2 = X^3 - 3X + b$ (Brier-Joye);
  - preventing the existence of “special points” à la Goubin (Smart);
  - find a convenient Edwards curve (FM).
- Hide a curve in a graph for cryptographic applications (see later).
- New CRT methods for computing modular or class polynomials (Sutherland).

II. Elliptic curves and isogenies

$$E : y^2 = x^3 + Ax + B \text{ over } \mathbf{K}, \mathrm{char}(\mathbf{K}) \notin \{2,3\}.$$

Def. (torsion points) For $n \in \mathbb{N}$, $E[n] = \{P \in E(\overline{\mathbf{K}}), [n]P = O_E\}$.

Division polynomials:

$$[n](x,y) = \left(\frac{\varphi_n(x,y)}{\psi_n(x,y)^2}, \frac{\omega_n(x,y)}{\psi_n(x,y)^3} \right)$$

$$\varphi_n = x\psi_n^2 - \psi_{n+1}\psi_{n-1}$$

$$4y\omega_n = \psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2$$

In $\mathbf{K}[x,y]/(y^2 - (x^3 + Ax + B))$, one has:

$$\psi_{2m+1}(x,y) = f_{2m+1}(x), \quad \psi_{2m} = 2yf_{2m}(x)$$

for some $f_m(x) \in \mathbf{K}[A,B,x]$.

$$f_n(x) = \begin{cases} \psi_n(x,y) & \text{for } n \text{ odd} \\ \psi_n(x,y)/(2y) & \text{for } n \text{ even} \end{cases}$$

$$f_{-1} = -1, \quad f_0 = 0, \quad f_1 = 1, \quad f_2 = 1$$

$$f_3(x,y) = 3x^4 + 6Ax^2 + 12Bx - A^2$$

$$f_4(x,y) = x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3$$

$$f_{2n} = f_n(f_{n+2}f_{n-1}^2 - f_{n-2}f_{n+1}^2)$$

$$f_{2n+1} = \begin{cases} f_{n+2}f_n^3 - f_{n+1}^3 f_{n-1}(16y^4) & \text{if } n \text{ is odd} \\ (16y^4)f_{n+2}f_n^3 - f_{n+1}^3 f_{n-1} & \text{otherwise.} \end{cases}$$

$$\deg(f_n(x)) = \begin{cases} (n^2-1)/2 & \text{if } n \text{ is odd} \\ (n^2-4)/2 & \text{otherwise.} \end{cases}$$

Thm. $P = (x,y) \in E[\ell] \iff [2]P = O_E$ or $f_\ell(x) = 0$.

Isogenies

Def. $\phi : E \to \tilde{E}$, $\phi(O_E) = O_{\tilde{E}}$; induces a morphism of groups.

First examples

1. Separable:

$$[k](x,y) = \left(\frac{\varphi_k}{\psi_k^2}, \frac{\omega_k}{\psi_k^3} \right),$$

$\tilde{E} = E$ (endomorphism).

2. Complex multiplication: $[i](x,y) = (-x, iy)$ on $E : y^2 = x^3 - x$; $\tilde{E} = E$ (endomorphism).

3. Inseparable: $\pi(x,y) = (x^p, y^p)$, $\mathbf{K} = \mathbb{F}_p$; $\tilde{E} = E^p$.

In the sequel:

- only separable isogenies;
- finite fields.

Properties of isogenies

Thm. If F is a finite subgroup of $E(\overline{\mathbf{K}})$, there exists ϕ and $\tilde{E}$ s.t.

$$\phi : E \to \tilde{E} = E/F, \quad \ker(\phi) = F.$$

Def. (Separable) *degree* of ϕ is $\#F$.

Problem 0: given E, F, compute an equation for $\tilde{E}$ and formulas for ϕ.

Thm. (dual isogeny) There is a unique $\hat{\phi} : \tilde{E} \to E$, $\hat{\phi} \circ \phi = [m]$, $m = \deg \phi$.

$$\begin{tikzcd}
E \arrow[r, "\phi"] \arrow[dr, "{[m]}"'] & \tilde{E} \arrow[d, "\hat{\phi}"] \\
 & E
\end{tikzcd}$$

$\Rightarrow$ we can get a factorization of f_ℓ.

Finding isogenous curves

Key fact: for all integers n there exists a polynomial $\Phi_n(X,Y) \in \mathbb{Z}[X,Y]$ (modular polynomial) s.t. E and E' are n-isogenous iff $\Phi_n(j(E),j(E')) = 0$.

Problem 1: given E, find all roots of $\Phi_n(X,j(E))$ and construct from this all (E',ϕ) that are n-isogenous.

Rem. If ℓ is prime $\deg(\Phi_\ell) = \ell+1$ and can be computed in $\tilde{O}(\ell^3)$ operations (Enge).

Thm. When ℓ is prime, $\Phi_\ell(X,j(E))$ has 0, 1, 2 or $\ell+1$ roots over $\mathbf{K}$.

$\Rightarrow$ we can build a graph of isogenies starting from E.

Atkin and Elkies (1986–1990)

The Frobenius $\pi : (X,Y) \mapsto (X^q, Y^q)$ has minimal equation

$$\pi_\ell^2 \ominus [t]\pi_\ell \oplus [q] = 0, \quad \Delta = t^2 - 4q.$$

If $(\Delta/\ell) = +1$, then over $\mathbb{F}_\ell$,
$\mathrm{Mat}(\pi_\ell) \simeq \left(\begin{array}{cc} \lambda_1 & 0 \\ 0 & \lambda_2 \end{array}\right) \Leftrightarrow \exists F, \pi_\ell(F) = F \Leftrightarrow F$ is a cyclic subgroup of order ℓ, defined over $\mathbf{K}$; E is ℓ-isogenous to $\tilde{E} = E/F$.

As a consequence, f_ℓ has a factor of degree $(\ell - 1)/2$.

Computational primitive: $E \mapsto \tilde{E}$ in direction λ.

III. Computations and algorithms

But what does an isogeny look like? Let

$$D(x) = \prod_{Q \in F^*} (x - x_Q) = x^{\ell-1} - \sigma x^{\ell-2} + \sigma_2 x^{\ell-3} - \sigma_3 x^{\ell-4} + \cdots .$$

where $\sigma = \sum_{Q \in F^*} x_Q$.

Rem. When ℓ is odd, $D(x) = g(x)^2$.

Fundamental proposition. $\tilde{E} : Y^2 = X^3 + \tilde{A}X + \tilde{B}$ where $\tilde{A} = A - 5t$, $\tilde{B} = B - 7w$ with

$$t = A(\ell-1) + 3(\sigma^2 - 2\sigma_2), w = 3A\sigma + 2B(\ell-1) + 5(\sigma^3 - 3\sigma\sigma_2 + 3\sigma_3);$$

$$\phi(x,y) = \left(\frac{N(x)}{D(x)}, y\left(\frac{N(x)}{D(x)}\right)'\right),$$

$$\frac{N(x)}{D(x)} = \ell x - \sigma - (3x^2 + A)\frac{D'(x)}{D(x)} - 2(x^3 + Ax + B)\left(\frac{D'(x)}{D(x)}\right)'$$

Numerical examples

Ex 1. $E : y^2 = x^3 + bx$, $F = \langle (0,0) \rangle$;

$$\tilde{E} : y^2 = x^3 - 4bx,$$

$$\phi : (x,y) \mapsto \left(\frac{x^3 + bx}{x^2}, y\frac{x^2 - b}{x^2} \right).$$

A curiosity: $E : y^2 = x^3 + x + 3$ defined over $\mathbb{F}_{1009}$; E is 6-isogenous to

$$\tilde{E} : y^2 = x^3 + 830x + 82$$

and $\sigma = 739$ (formulas for prime ℓ valid here too!!!) for which

$$\frac{N(x)}{D(x)} = \frac{x^6 + 270x^5 + 325x^4 + 566x^3 + 382x^2 + 555x + 203}{x^5 + 270x^4 + 289x^3 + 659x^2 + 533x + 399}.$$

The denominator factors as

$$(x - 66)(x - 23)^2 (x - 818)^2.$$

$x = 66$ is the abscissa of a point of 2-torsion;
23 is the abscissa of a point of 3-torsion;
818 is the abscissa of a primitive point of 6-torsion.

Numerical examples

Ex 1. $E : y^2 = x^3 + bx$, $F = \langle (0,0) \rangle$;

$$\tilde{E} : y^2 = x^3 - 4bx,$$

$$\phi : (x,y) \mapsto \left(\frac{x^3 + bx}{x^2}, y\,\frac{x^2 - b}{x^2} \right).$$

A curiosity: $E : y^2 = x^3 + x + 3$ defined over $\mathbb{F}_{1009}$; E is 6-isogenous to

$$\tilde{E} : y^2 = x^3 + 830x + 82$$

and $\sigma = 739$ (formulas for prime ℓ valid here too!!!) for which

$$\frac{N(x)}{D(x)} = \frac{x^6 + 270x^5 + 325x^4 + 566x^3 + 382x^2 + 555x + 203}{x^5 + 270x^4 + 289x^3 + 659x^2 + 533x + 399}.$$

The denominator factors as

$$(x - 66)\,(x - 23)^2\,(x - 818)^2\,.$$

$x = 66$ is the abscissa of a point of 2-torsion;
23 is the abscissa of a point of 3-torsion;
818 is the abscissa of a primitive point of 6-torsion.

Isogenies and complexity (1/2)

Goal: compute an isogenous curve of degree ℓ over $\mathbb{F}_{p^n}$.

Basic algorithm:
Given p, n, $E/\mathbb{F}_{p^n}$,
for j_0 a root of $\Phi_\ell(X, j(E))$, compute $\tilde{E}$ and $\phi : E \to \tilde{E}$.

- Case $p \gg \ell$: (Elkies, Atkin), finding $\tilde{E}$ costs $O(\ell)$ operations; finding ϕ costs $O(\ell^2) + O(\mathsf{M}(\ell))$ (Bostan-FM-Salvy-Schost).
- Case $p \ll \ell$:
  - $p = 2$: super fast algorithm by Lercier, complexity not proven $O(\ell^2)$ or $O(\ell^3)$?.
  - $p > 2$: Couveignes's Artin Schreier approach (remember L. De Feo's talk, joint work with É. Schost), $\tilde{O}(\ell^2)$. To be confronted with Lercier-Sirvent's p-adic approach.

Isogenies and complexity (2/2)

Two easy problems:

- Problem 0: given E, F, compute an equation for $\tilde{E}$ and formulas for ϕ (Vélu's formulas).
- Problem 1: given E, find all roots of $\Phi_n(X, j(E))$ and construct from this all (E', ϕ) that are n-isogenous (Elkies, Atkin, etc., but $\tilde{O}(n^3)$).

Two difficult problems:

- Problem 2: given E_1 and E_2, are they isogenous? (modular polynomials can help if bound on degree or very efficient SEA to use Tate's theorem).
- Problem 3: given that E_1 and E_2 are isogenous, find an isogeny between them (probably best to solve Problem 0 and use an isomorphism from $\tilde{E}$ to E_2; bound required).

IV. Isogeny graphs and cryptographic applications

Def. $G = (\mathscr{V}, \mathscr{E})$ where $(E_1, E_2) \in \mathscr{E}$ if and only if E_1 and E_2 are isogenous.

Thm. (Tate) isogenous curves (over $\mathbb{F}_q$) have the same cardinality.

$\Rightarrow$ G is complete. It is more interesting to study particular paths between curves.

For instance: graph of ℓ-isogenies for ℓ fixed.

It turns out that endomorphisms are important:
$\mathrm{End}(E) = \{I : E \to E\}$.

First task: classify curves according to their endomorphism ring.

A) Fixing ℓ: volcanoes

Thm. If E is ordinary, write $\#E = q+1-t$ and $t^2-4q = d = f^2 D$. Then $\mathrm{End}(E)$ is an order $\mathscr{O}$ in $\mathbf{K} = \mathbb{Q}(\sqrt{D})$ where $D = \mathrm{disc}(\mathbf{K}) < 0$.

General picture: $\mathbb{Z}[\pi] = \mathbb{Z}[(d+\sqrt{d})/2] \subset \mathrm{End}(E) \subset \mathscr{O}_K$.

Class polynomial: $H_d(X) = \prod_{\mathrm{End}(E)=\mathscr{O}}(X - j(E)) \in \mathbb{Z}[X]$.

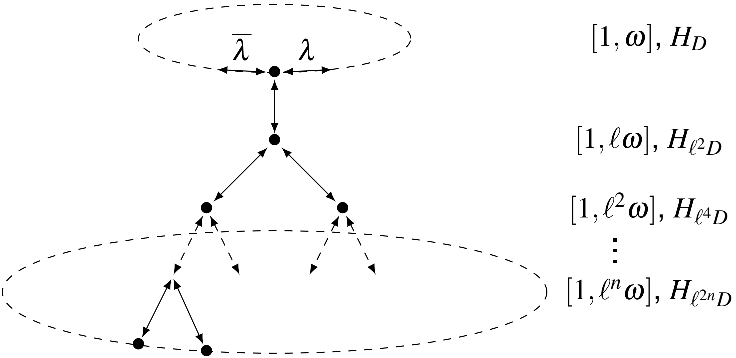
Important result: (Deuring, Waterhouse, Schoof) number of isomorphism classes of curves having the same cardinal is

$$H(d) = \sum_{\mathbb{Z}[\pi]\subset\mathscr{O}\subset\mathscr{O}_K} h(\mathscr{O}).$$

$\Rightarrow \#\mathscr{V}$ is reasonably large ($h(\Delta) = O(|\Delta|^{1/2+\varepsilon})$).

Volcano

Most interesting case is $\left(\frac{D}{\ell}\right) = +1$ and $\ell^{2n} \mid\mid \mathrm{disc}(\pi) = t^2 - 4q$:



Navigating in the structure is relatively easy, using modular polynomials: solve $\Phi_\ell(X, j(E_i))$ to get E_{i+1} in direction λ; see Kohel, Fouquet-FM.

B) Varying ℓ

Problem: given $E_1, E_2 \in \mathscr{V}$, find a path from E_1 to E_2.

Thm. (Galbraith, over $\mathbb{F}_p$) there exists a probabilistic algorithm that builds an isogeny $I : E_1 \to E_2$ requiring $O(p^{3/2} \log p)$ expected time and expected space $O(p \log p)$ at worse.

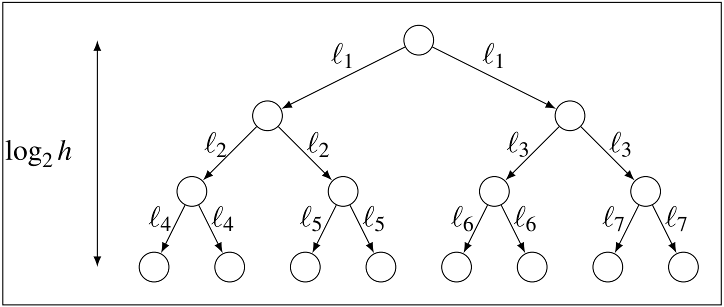
Algorithm:
INPUT: E_1 and E_2 which are isogenous.
OUTPUT: an isogeny path from E_1 to E_2.
1. Find E_i' isogenous to E_i s.t. $\mathrm{End}(E_i') = \mathscr{O}_K$.
2. Find two paths from E_1' and E_2' that meet in some point.
3. Assemble the isogeny.

Idea: build paths using ℓ-isogenies of prime degree $\ell \leq L = O((\log D)^2$ (under GRH).

Conjecture: this will terminate after $O(\log h_K)$ iterations.

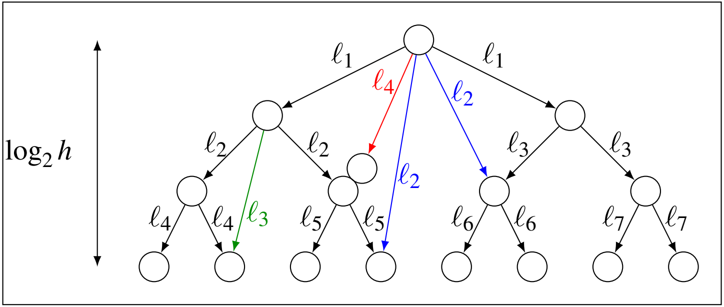
Building a binary tree

Start from any curve and build a tree, at each node selecting some ℓ at random (this is needed since for fixed ℓ, we find a cycle).



Classical property of binary trees: if height is $\log_2 h$, then the total number of nodes is h, half of which are leaves.

Building a “bushy” tree



At each iteration ℓ, for each vertex j, compute the roots of $\Phi_\ell(X,j)$. Expect the tree to have size $O(\sqrt{h})$ after $O(\log h)$ iterations.

Using two trees and a birthday-paradox approach, there exists a common vertex in both trees after $O(\log h)$ iterations.

Build the respective paths and that's it.

Jao, Miller, Venkatesan (ASIACRYPT 2005)

$\mathscr{G} = (\mathscr{V}, \mathscr{E})$ where $(E_1, E_2) \in \mathscr{E}$ if and only if $\exists I : E_1 \to E_2, \deg(I) = \ell \in O((\log q)^{2+\delta})$ for some $\delta > 0$.

Prop. $\mathscr{G}$ is an expander graph, hence there is a rapid mixing property for random walks.

Prop. Let G be a regular graph of degree k on h vertices. Suppose that the eigenvalue λ of any nonconstant eigenvector satisfies the bound $|\lambda| \leq c$ for some $c < k$. Let S be any subset of the vertices of G, and x be any vertex in G. Then a random walk of any length at least $\frac{\log(2h/|S|^{1/2})}{\log(k/c)}$ starting from x will land in S with probability at least $\frac{|S|}{2h} = \frac{|S|}{2|G|}$.

Coro. ECDLP is not stronger among an isogeny class.

Some cryptographic applications

Where is the difficult problem? Given two isogenous curves E_1 and E_2, build an explicit isogeny $I : E_1 \to E_2$.

Only known way: Galbraith's in $O(\sqrt{h})$.

Using the graphs:

- Key exchange: (Rostovtsev, Stolbunov) using two routes and $R_A(R_B(E)) = R_B(R_A(E))$.
- ECDLP: the GHS attack is not invariant under isogeny, hence we could dream of finding an isogenous curve E_2 for which the GHS is more (resp. less) successful. Confirmed by JaMiVe05. $\Rightarrow$ key for trapdoors, see E. Teske's (*J. Cryptology*).
- Hash function: (D. Charles, E. Goren, K. Lauter): $H(m_0 m_1 \ldots m_{k-1})$: start from a given (supersingular) E; use m_i to decide to go left or right at each step; hash value is the last curve.

Conclusions

- Isogenies prove their interest outside classical number theory, and even outside the original SEA context.
- Not all algorithmic problems solved: see the current cleaning of Couveignes's algorithm, the use of p-adic methods, etc.
- New applications appear: CRT again; more crypto things?
- Higher genus: almost everything has to be done (see FM's slides for ANTS8).

$\Rightarrow$ not the end of the story!