Introduction to isogenies and their cryptologic applications

F. Morain

Laboratoire d'Informatique de l'École polytechnique

POLYTECHNIQUE CNRS INRIA

Isogeny party, July 18th, 2006

Welcome to the isogeny party!

Goal: shed some light on the use of isogenies in cryptology.

Schedule

- 9.00- 9.45: FM, Introduction to isogenies and their cryptologic applications.

Coffee break

- 10.00-10.45: M. Fouquet, Isogeny cycles and volcanoes.
- 10.50-11.35: A. Enge, Fast computation of modular polynomials.
- 11.40-12.25: É. Schost, Fast algorithms for isogeny computation in large characteristic

Lunch break

- 13.30-14.15: I. Déchène, Cryptographic Potential of Generalized Jacobians
- 14h20-15h05: R. Lercier, Computing isogenies in small or medium characteristic

Coffee break

- 15.20-16.05: E. Teske, Trapdooring with isogenies
- 16.10-16.55: A. Stolbunov, Public key cryptosystem based on isogenies

Motivations

In cryptography: find reasonable objects to work with.

Reasonable $=$ "small" group G, easy to perform operations in, resistant to attacks ($\#G \approx 2^{200}$).

Finite fields are too easy. Algebraic curves are worth a try. See I. Déchène's talk.

Why focus on isogenies?

- Computational Number Theory:
  - First life (1985–1997): Schoof-Elkies-Atkin (SEA), Couveignes, Lercier;
  - Second life (1996–): Kohel, Fouquet/FM (cycles and volcanoes); Couveignes/Henocq, Bröker and Stevenhagen (CM curves using p-adic method).
- More direct cryptologic applications (1999–): Galbraith; Galbraith/Hess/Smart; Smart; Jao/Miller/Venkatesan; Teske; Rostovtsev/Stolbunov; etc.

Plan

I. Elliptic curves.

II. Isogenies.

III. Isogeny graphs.

IV. Cryptologic applications.

I. Elliptic curves

$$q = p^r, E/\mathbb{F}_q : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

Thm. (Hasse) $\#E = q + 1 - t$, $|t| \leq 2\sqrt{q}$.

It is important that $\#E$ not be smooth, for cryptographic reasons (ECDLP should not be trivially easy).

Methods for computing $\#E$:

- Shanks/Pollard: $\tilde{O}(q^{1/4})$.
- Schoof family (any field)
  - Original: any fi eld$\tilde{O}((\log q)^5)$ deterministic.
  - Improvements by Elkies/Atkin (SEA): $\tilde{O}((\log q)^4)$ probabilistic for p large. Rather slow for p small (Couveignes, Lercier).
  - p medium: (Joux/Lercier) SEA over $\mathbb{Q}_q$ (unramifi ed extension of $\mathbb{Q}_p$), $\tilde{O}((\log q)^4)$. See talk by Lercier.
- p-adic methods (Satoh; Kedlaya), $\tilde{O}(r^3)$ ($q = p^r$). Very efficient for p small.

Torsion

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

Thm. $E[n] \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ when $\gcd(n, p) = 1$.

$$E[p^k] = \begin{cases} \mathbb{Z}/p^k\mathbb{Z} & \text{if } E \text{ is ordinary} \\ \{O_E\} & \text{if } E \text{ is supersingular} \end{cases}$$

Rem. E supersingular iff $p \mid t$; typical example is $Y^2 = X^3 - X$ over $\mathbb{F}_p$ when $p \equiv 3 \bmod 4$.

In this talk: almost always E is ordinary over $\mathbb{F}_p$, $p \geq 5$, hence:

$$E : Y^2 = X^3 + AX + B \text{ over } \mathbf{K}, \mathrm{char}(\mathbf{K}) \notin \{2, 3\}.$$

Division polynomials

$$[n](X, Y) = \left(\frac{\phi_n(X, Y)}{\psi_n(X, Y)^2}, \frac{\omega_n(X, Y)}{\psi_n(X, Y)^3}\right)$$

$$\phi_n = x\psi_n^2 - \psi_{n+1}\psi_{n-1}, \quad 4Y\omega_n = \psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2$$

In $\mathbf{K}[X, Y]/(Y^2 - (X^3 + AX + B))$, one has:

$$\psi_{2m+1}(X, Y) = f_{2m+1}(X), \quad \psi_{2m} = 2Yf_{2m}(X)$$

$$f_{-1} = -1, f_0 = 0, f_1 = 1, f_2 = 1, f_3(X, Y) = 3X^4 + 6AX^2 + 12BX - A^2$$

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

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

$$\deg(f_n(X)) = (n^2 - \{1, 4\})/2$$

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

Schoof's algorithm in a slide

1. Compute L s.t. $\prod_{\ell \leq L} \ell > 4\sqrt{q}$ ($\Rightarrow L = O(\log q)$).
2. **for** $\ell \leq L$ **do**

   compute $t_\ell \equiv t \bmod \ell$.
3. recover t using CRT.

To find t_ℓ, exploit characteristic polynomial of the Frobenius $(X, Y) \mapsto (X^q, Y^q)$, i.e.

$$(X^{q^2}, Y^{q^2}) \ominus [t_\ell](X^q, Y^q) \oplus [q](X, Y) = 0$$

in $A_\ell = \mathbb{F}_q[X, Y]/(Y^2 + a_1 XY + \ldots, f_\ell(X))$.

Involves heavy polynomial computations ($\deg(f_\ell) = O(\ell^2)$).

II. Isogenies

Def. non-constant rational map $I : E \to \tilde{E}$, preserving the group structure (in particular $I(O_E) = O_{\tilde{E}}$).

First examples
1. Separable:

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

2. Complex multiplication: $[i](x, y) = (-x, iy)$ on $E : y^2 = x^3 - x$.
3. Inseparable: $\varphi(x, y) = (x^p, y^p)$, $\mathbf{K} = \mathbb{F}_p$.

In the sequel: only separable isogenies.

How does an isogeny look like?

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

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

Extending Vélu, Dewaghe:

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

Fundamental proposition. The isogeny I can be written as

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

Ex. $E : Y^2 = X^3 + bX$, $F = \langle (0, 0) \rangle$; we find $\tilde{E} : Y^2 = X^3 - 4bX$, and

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

Dual isogeny

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

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

Coro. $D \mid \psi_\ell^2$ (resp. $g \mid f_\ell$).

From Schoof to SEA

Key point of Elkies: find a prime ℓ for which there exists a rational ℓ-isogeny from E; (happens with proba $1/2$). Then $g(x) \mid f_\ell(x)$ with $\deg(g) = (\ell-1)/2$.

How do we know that E and $\tilde{E}$ are ℓ-isogenous? there exists $\Phi_\ell(X,Y) \in \mathbb{Z}[X,Y]$ (a modular polynomial) s.t. E and $\tilde{E}$ are isogenous only if

$$\Phi_\ell(j(E), j(\tilde{E})) = 0.$$

cf. A. Enge's talk.

Black box: there exists formulas to compute $(\tilde{E}, \sigma)$ given $\mathbf{K}$, E, ℓ, Φ_ℓ (see green book).

Computing I from $(A, B, \ell, \tilde{A}, \tilde{B}, \sigma)$: see talks by É. Schost (p large) + R. Lercier (p small or medium).

III. Isogeny graphs

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

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

In order to understand the graph, we must study the 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.

Endomorphism rings for elliptic curves over $\mathbb{C}$

Over $\mathbb{C}$, $E = \mathbb{C}/L = \mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z})$, $\Im(\tau) > 0$.

Prop. $\mathrm{End}(E) \sim \{\alpha \in \mathbb{C}, \alpha L \subset L\}$.

Prop. $\mathrm{End}(E)$ contains more than $\mathbb{Z}$ iff $\tau \in \mathbf{K} = \mathbb{Q}(\sqrt{-D})$. E is said to have complex multiplications.

Prop. If τ is quadratic, $\mathrm{End}(E)$ is an order in $\mathcal{O}_K$ (ring of integers of $\mathbf{K}$), of conductor $c = [\mathcal{O}_K : \mathrm{End}(E)]$.

Thm. (Class field theory) If $\mathrm{End}(E) = \mathcal{O}$, E can be defined over the ring class field of $\mathcal{O}$. This is an extension of degree $h = h(\mathcal{O})$ of $\mathbf{K}$; it can be realized via the special values of $j(\mathfrak{a})$ for $\mathrm{Cl}(\mathcal{O}) = \{\mathfrak{a}_1, \ldots, \mathfrak{a}_h\}$, where j is the modular function $j(x) = 1/x + 744 + \cdots$. Cf. A. Enge's talk.

Thm. E is isogenous to $E/\mathfrak{a}$, and this forms cycles of length the order of $\mathfrak{a}$ in $\mathrm{Cl}(\mathcal{O})$.

Endomorphism rings for curves over finite fields

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 $\mathcal{O}$ in $\mathbf{K} = \mathbb{Q}(\sqrt{-D})$ where $-D = \mathrm{disc}(\mathbf{K})$.

Deuring lifting: given $E/\mathbb{F}_q$, one can lift it over $\mathbb{C}$ (actually over the ring class field of $\mathcal{O}$) and preserve the endomorphism ring.

Rem. inefficient in practice unless p is small (see for instance Couveignes/Henocq; Bröker and Stevenhagen).

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

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

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

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

How do we find $\mathrm{End}(E)$?

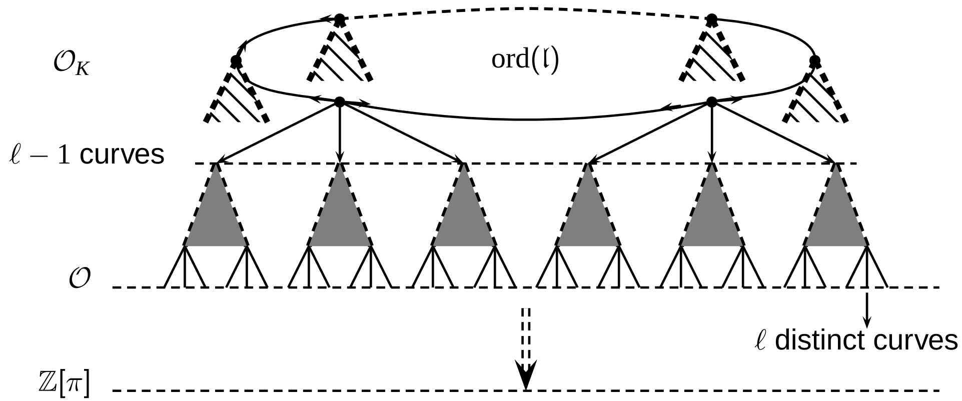
Thm. (Kohel) Let $I : E_1 \to E_2$ s.t. $\mathrm{End}(E_1) \subset \mathrm{End}(E_2)$ (resp. $\mathrm{End}(E_2) \subset \mathrm{End}(E_1)$). Suppose $\ell \mid [\mathrm{End}(E_2) : \mathrm{End}(E_1)]$ (resp. $\ell \mid [\mathrm{End}(E_1) : \mathrm{End}(E_2)]$). Then $\ell \mid \deg(I)$.

Classification: If I isogeny of prime degree ℓ.
1. If $\mathrm{End}(E_1) \simeq \mathrm{End}(E_2)$, then I is horizontal ($\rightarrow$) at ℓ.
2. $[\mathrm{End}(E_1) : \mathrm{End}(E_2)] = \ell$: down ($\downarrow$) at ℓ.
3. $[\mathrm{End}(E_2) : \mathrm{End}(E_1)] = \ell$: up ($\uparrow$) at ℓ.

$\Rightarrow$ cycles, volcanoes.

Volcano

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



Navigating in the structure is relatively easy, using modular polynomials.

See M. Fouquet's talk for more.

Two graphs

G: complete isogeny graph.

If we fix $\mathcal{O}$, there is a subgraph, which corresponds to the Cayley graph of $\mathrm{Cl}(\mathcal{O})$: vertices are ideals of $\mathrm{Cl}(\mathcal{O})$; two ideals $[\mathfrak{a}_1]$ and $[\mathfrak{a}_2]$ are related iff there is some $\mathfrak{b}$ s.t. $[\mathfrak{a}_1\mathfrak{b}] = [\mathfrak{a}_2]$.

Given an edge on the Cayley graph, it is relatively easy to compute the corresponding edge on the isogeny graph.

The converse seems difficult.

Even more fundamental difference: exponentiation is easy on the Cayley graph; it is not on the isogeny graph.

Galbraith's algorithm

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

Thm. (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.

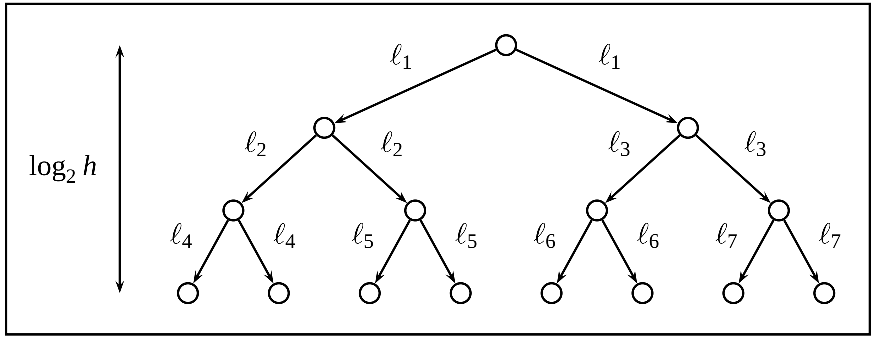
Algorithm:
INPUT: E_1 and E_2 which are isogenous.
OUTPUT: an isogeny path from E_1 to E_2.
1. Find E_i' isogenous to E_i s.t. $\mathrm{End}(E_i') = \mathcal{O}_K$.
2. Find two paths from E_1' and E_2' that meet in some point.
3. Assemble the isogeny.

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.

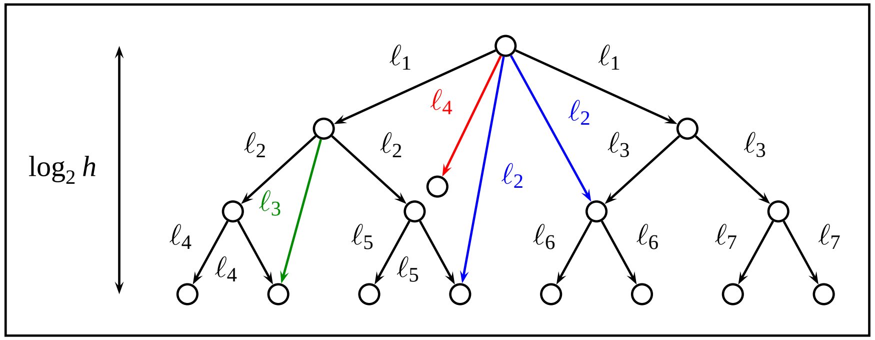
Building a binary tree

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).
Generically, $\Phi_\ell(X, j(E))$ has two roots.



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)

$\mathcal{G} = (\mathcal{V}, \mathcal{E})$ where $(E_1, E_2) \in \mathcal{E}$ 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. $\mathcal{G}$ 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 $\dfrac{\log(2h/|S|^{1/2})}{\log(k/c)}$ starting from x will land in S with probability at least $\dfrac{|S|}{2h} = \dfrac{|S|}{2|G|}$.

Coro. ECDLP is not stronger among an isogeny class.

IV. Cryptologic applications

A) The setting

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 attack: Galbraith's in $O(\sqrt{h})$.

Two propositions: E. Teske; A. Stolbunov.

B) ECDLP

Gaudry/Hess/Smart attack: transform ECDLP in $E_1(\mathbb{F}_{q^n})$ into one on a curve of genus g over $\mathbb{F}_q$.

Rem. 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 talk.

C) Hash function (D. Charles, E. Goren, K. Lauter)

When E is supersingular, for fixed ℓ, $\mathrm{End}(E)$ is connected (property of quaternions, actually).

Idea: use graph of 2-isogenies of a supersingular elliptic curve. The graph is 3-connected.

$H(m_0 m_1 \ldots m_{k-1})$: start from a given E; use m_i to decide to go left or right at each step; hash value is the last curve.

Security: given E_{orig} and E_{final}, find another path so as to make a collision. Could only be doable in $O(\sqrt{h})$.

D) Miscellaneous

- Brier & Joye (CHES-2003): for crypto reasons, one prefers $Y^2 = X^3 - 3X + b$. If original E is not isomorphic to this type of curve, find an isogenous one that is ($[A, B] \sim [u^4 A, u^6 B]$).
- Smart (CHES-2003): preventing the existence of “special points” à la Goubin (points (x, y) with $x = 0$ or $y = 0$).
- Doche, Icart, Kohel (PKC06): speed up the computation of $[k]P$ when small degree isogeny exist ($\ell = 2, 3$).

Conclusions

In this talk:

- Isogeny classes form a graph with interesting properties.
- Navigating in the graph is relatively easy.
- ECDLP can be transported from a curve to another in the same isogeny class.

Open problems:

- Is the isogeny-path problem really difficult?
- In higher genus: make algorithms practical; understand the isogeny graph.

More to come: after the coffee break!