Introduction to elliptic curve cryptography
Cryptography from isogeny graphs

Sorina Ionica

Laboratoire MIS, Université de Picardie Jules Verne, France

May 16, 2018

Les ordinateurs quantiques - la crypto-apocalypse

- Algorithme de Shor : resout le logarithme discret et la factorisation en temps polynomial sur un ordinateur quantique

- Aug. 2015: NSA announces plans to transition to quantum-resistant algorithms

- February 2016: NIST calls for quantum secure submissions. Deadline 30 Nov. 2017

Isogenies

Definition

An isogeny is a morphism $\phi : E \to E'$ such that $\phi(O_E) = O_{E'}$.

For all $P, Q \in E$, $\phi(P + Q) = \phi(P) + \phi(Q)$.

Examples

- multiplication by $\ell \in \mathbb{Z}$, i.e. $[\ell]$:P$\rightarrow \ell P$
  - $\mathrm{End}(E)$ is a ring containing a subring isomorphic to $\mathbb{Z}$
- The Frobenius for $E/\mathbb{F}_q$

$$\begin{aligned} \pi : E &\rightarrow E \\ (x, y) &\rightarrow (x^q, y^q) \end{aligned}$$

- π is not a multiplication by ℓ map $\Rightarrow \mathbb{Z}[\pi] \subseteq \mathrm{End}(E)$

Properties of isogenies

- The kernel is finite subgroup

$$\mathrm{Ker}(\phi) = \phi^{-1}(O_{E'}).$$

- We define the degree of an isogeny ϕ as $deg\phi = \#\mathrm{Ker}(\phi)$.
- Given two isogenies ϕ and ψ we have:

$$deg(\phi \circ \psi) = (deg\phi)(deg\psi).$$

The torsion group

$E[\ell]$ is the ℓ-torsion subgroup

$$E[\ell] = \{P \in E(\bar{\mathbb{F}}_q) | \ell P = 0\}$$

Theorem

- *If* $(\ell, p) = 1$, *then* $E[\ell] \simeq \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$.
- *Either* $E[p^e] = 0$, *for all* $e \in \mathbb{Z}$ *or* $E[p^e] \simeq \mathbb{Z}/p^e\mathbb{Z}$, *for all* $e \in \mathbb{Z}$.

What is the degree of $[\ell] : E \to E$, for $(\ell, p) = 1$?

Properties of isogenies

- Every isogeny has a dual, i.e. given $\phi : E \to E'$, there is $\hat{\phi} : E' \to E$ such that :

$$\phi \circ \hat{\phi} = [\ell] \text{ and } \hat{\phi} \circ \phi = [\ell],$$

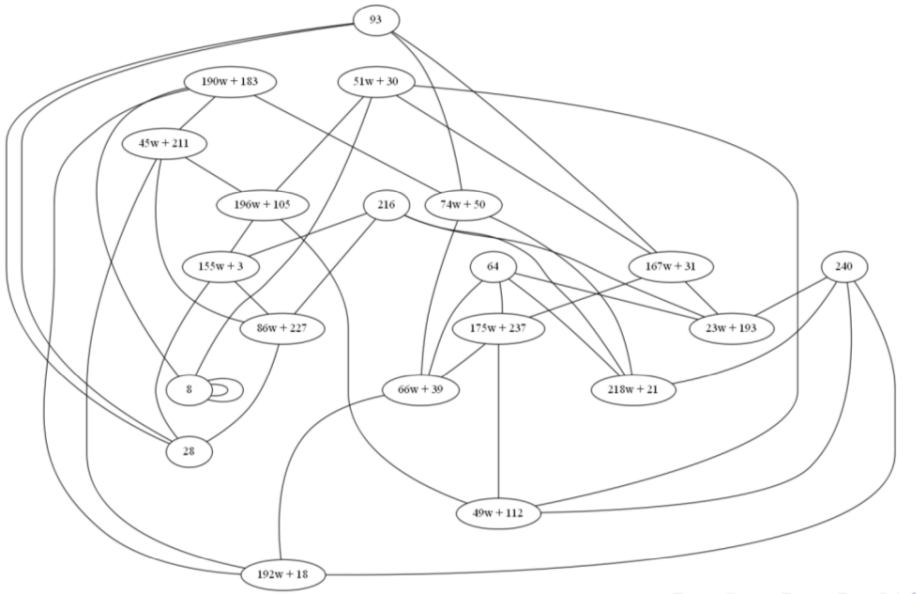
with ℓ the degree of the isogeny.

The isogeny graph

A theorem of Tate

Two elliptic curves E, E' are isogenous over $\mathbb{F}_q$ if and only if $\#E(\mathbb{F}_q) = \#E'(\mathbb{F}_q)$.

- The vertices: all elliptic curves E s.t. $\#E(\mathbb{F}_q) = N$.
- The edges: isogenies between these curves.



Computing isogenies - Vélu formulae

For a given $\mathbb{G}$ a subgroup of order ℓ, there is an isogeny with $\mathrm{Ker}\ \phi = G$ that we denote by $\phi : E \to E' = E/\langle \mathbb{G} \rangle$.

We construct this isogeny:

$$P \quad \to \quad \begin{cases} O_{E'} & \text{if } P = O_E, \\ (x_P + \sum_{Q \in G - \{O_E\}} x_{P+Q} - x_Q, & \\ y_P + \sum_{Q \in G - \{O_E\}} y_{P+Q} - y_Q) & \text{if } P \neq O_E \end{cases}$$

Assume points of order ℓ are defined over $\mathbb{F}_q$.

Complexity $O(\ell)$

Example

Let $E : y^2 = (x^2 + b_1x + b_0)(x - a)$. The point $(a, 0)$ has order 2; the quotient of E by $\langle (a, 0) \rangle$ gives an isogeny

$$\phi : E \to E' = E/\langle (a, 0) \rangle$$

where $E' : y^2 = x^3 + (-(4a + 2b_1))x^2 + (b_1^2 - 4b_0)x$
and ϕ maps (x, y) to

$$\left(\frac{x^3 - (a - b_1)x^2 - (b_1a - b_0)x - b_0a}{x - a}, \frac{(x^2 - (2a)x - (b_1a + b_0))y}{(x - a)^2} \right)$$

The torsion group

$E[\ell]$ is the ℓ-torsion subgroup

$$E[\ell] = \{P \in E(\bar{\mathbb{F}}_q) | \ell P = 0\}$$

Theorem

- *If* $(\ell, p) = 1$, *then* $E[\ell] \simeq \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$.
- *Either* $E[p^e] = 0$, *for all* $e \in \mathbb{Z}$ *or* $E[p^e] \simeq \mathbb{Z}/p^e\mathbb{Z}$, *for all* $e \in \mathbb{Z}$.

$$E[\ell](\mathbb{F}_q) = \{P \in E(\mathbb{F}_q) | \ell P = 0\}$$

Isogenies of degree ℓ

How many isogenies of degree ℓ (up to isomorphism) are there?

Isogenies and discrete logarithm

DLP on E

Solve $\lambda P = Q$.

DLP on E'

Solve $\lambda\phi(P) = \phi(Q)$.

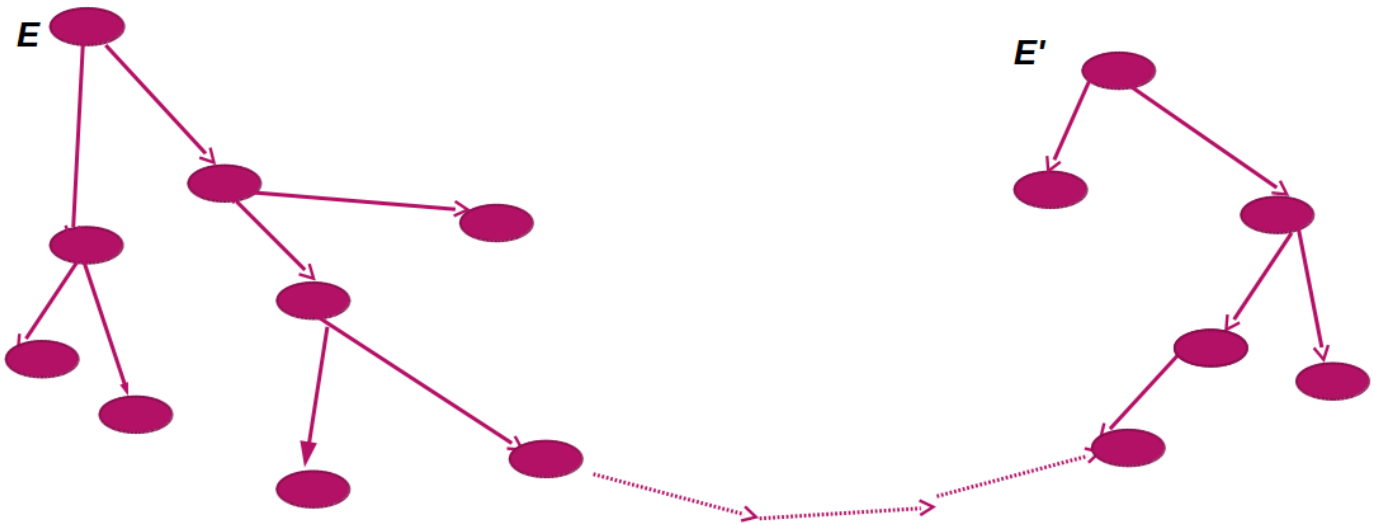
The isogeny path problem

Let E and E' be two elliptic curves defined over $\mathbb{F}_q$ of equal cardinality. Find an isogeny $\phi : E \to E'$.

Weak curves defined over $\mathbb{F}_{p^3}$: $y^2 = h(x)(x-\alpha)(x-\alpha^p)$, with $\alpha \in \mathbb{F}_{p^3} \backslash \mathbb{F}_p$ and $h \in \mathbb{F}_q[x]$, $\deg h \leq 2$.

Galbraith's algorithm

Let $\delta_v(X)$ is the set of vertices in the graph which are connected to a vertex in X by an edge of degree ℓ.



Complexity of Galbraith's algorithm

Input: E, E'
Output: $I : E \to E'$

$X \leftarrow \{E\}$, $Y \leftarrow \{E'\}$.
while $X \cap Y \neq 0$ **do**
  $X \leftarrow X \cup \delta_v(X)$
  $Y \leftarrow Y \cup \delta_v(Y)$
end while
Return path

Using the birthday paradox, we show that the algorithm will find a path in

$$O(\sqrt{\#\text{nb. of vertices in the graph}})$$

Supersingular curves

All supersingular curves admit a model over $\mathbb{F}_{p^2}$.

Let S_{p^2} be the set of all (classes of isomorphism) of supersingular elliptic curves over $\mathbb{F}_{p^2}$.

Theorem

$\#S_{p^2} = \lfloor \frac{p}{12} \rfloor + b,\ b \in \{0, 1, 2\}.$

Supersingular curve isogeny graph

- The vertices: all elliptic curves E defined over $\mathbb{F}_{p^2}$.
- The edges: Isogenies of degree ℓ.

Theorem (Mestre)

This isogeny graph is connected.

De Feo-Jao-Plût Key Exchange

Public parameters:

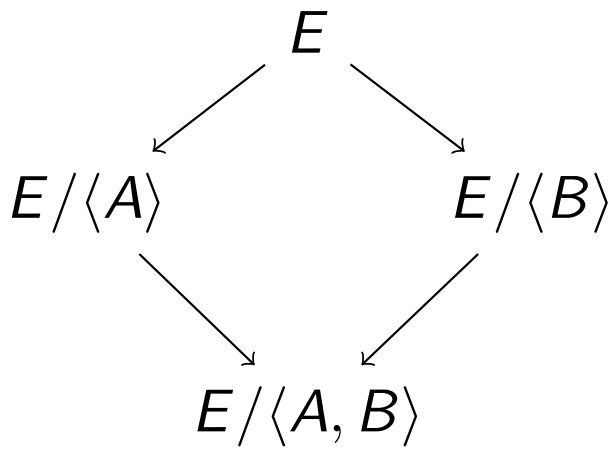
E a supersingular curve over $\mathbb{F}_{p^2}$.

A basis $\langle P_A, Q_A \rangle$ of $E[\ell_A^{e_A}]$.

A basis $\langle P_B, Q_B \rangle$ of $E[\ell_B^{e_B}]$.

$A = m_A P_A + n_A Q_A$

$B = m_B P_B + n_B Q_B$



Supersingular Isogeny Diffie Hellman (SIDH)

Alice chooses
$A = m_A P_A + n_A Q_A$.

She computes $\alpha : E \to E/\langle A \rangle$.

She sends $E_A, \alpha(P_B), \alpha(Q_B)$.

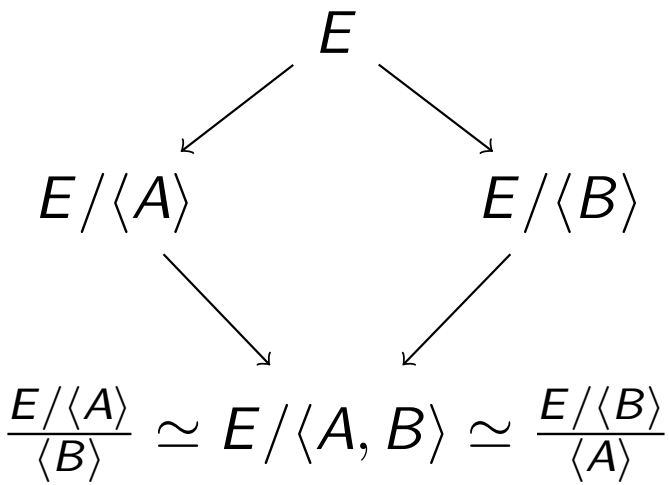
Computes $E_B \to E_B/\langle A \rangle$.

Bob chooses
$B = m_B P_B + n_B Q_B$.

He computes $\beta : E \to E/\langle B \rangle$.

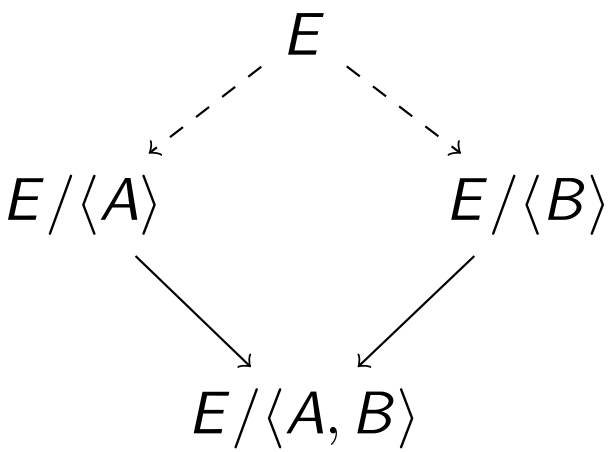
He sends $E_B, \beta(P_A), \beta(Q_A)$.

Computes $E_A \to E_A/\langle B \rangle$



The security of the SIDH protocol

The security of SIDH relies on the hardness of finding an isogeny of degree $\ell_A^{e_A}$ between E and E_A and of finding an isogeny of degree $\ell_B^{e_B}$ between E and E_B.



Group structure of supersingular curves

Let p be a prime, and let E be a supersingular curve defined over a finite field $\mathbb{F}_q$ with $q = p^2$ elements. Let t be the trace of the Frobenius endomorphism of E, then :

- $t^2 = 4q$, or
- $t^2 = q$, and $j(E) = 0$
- $t^2 = 0$, and $j(E) = 1728$

The group structure is one of the following:

- $t = \pm 2\sqrt{q}$, then $E(\mathbb{F}_q) \simeq \mathbb{Z}/(\sqrt{q} \mp 1)^2\mathbb{Z}$.
- If $t^2 = q$, then $E(\mathbb{F}_q)$ is cyclic;
- If $t = 0$, then $E(\mathbb{F}_q)$ is either cyclic, or isomorphic to

$$\mathbb{Z}/\frac{q+1}{2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Constructing curves for SIDH

Fix $\ell_A^{e_A}$ and $\ell_B^{e_B}$ and take $p = \ell_A^{e_A}\ell^{e_B}f \pm 1$, where f is a small factor.

Take $\ell_A^{e_A} \approx \ell_B^{e_B}$.