Algoritmos y Protocolos Criptográficos con Curvas Elípticas

Josep M. Miret

Escola Politècnica Superior
Departament de Matemàtica
Universitat de Lleida

e-mail: miret@eps.udl.es

Murcia, 24-25 de Noviembre de 2006

Grupo de Criptografía y Matemática Discreta (UdL)

- **Miembros del grupo**

  Josep Conde
  Joan Gimbert
  Josep M. Miret
  Ramiro Moreno
  Jordi Pujolàs
  Magda Valls

- **Estudiantes de Doctorado**

  Xavier Hernández
  Nacho López
  Santi Martínez, *Beca FI*
  Rosana Tomàs, *Beca FI*

- **Docencia**

  Ingenierías en Informática
  Programa de Doctorado de Ingeniería

Líneas de investigación

- **Cardinalidad de curvas elípticas**
  - Subgrupos de Sylow de una curva elíptica
  - Extensión al caso de curvas de género 2
  - Generalización de las fórmulas de Vélu
- **Volcanes de isogenias de curvas elípticas**
  - Algoritmo para recorrer las curvas de un volcán
  - Generalización a cordilleras
  - Criptosistemas basados en isogenias
- **Protocolos criptográficos en sistemas computacionales restringidos**
  - Tarjetas inteligentes
  - Sistemas RFID (Radio Frequency Identification)

Publicaciones

- *Determining the 2-Sylow subgroup of an elliptic curve over a finite field*. J. Miret, R. Moreno, A. Rio and M. Valls. Mathematics of Computation, 74, no. 249, pp. 411-427 (2005)

- *Generalization of Vélu's formulae for isogenies between elliptic curves.* J. Miret, R. Moreno. A. Rio. Publicacions Matemàtiques.

- *An algorithm to compute volcanoes of 2–isogenies of elliptic curves over finite fields.* J. Miret, R. Moreno, D. Sadornil, J. Tena, M. Valls. Applied Mathematics and Computation, 176, no. 2, 739-750 (2006).

- *Volcanoes of ℓ–isogenies of elliptic curves over finite fields: the case ℓ=3.* J. Miret, D. Sadornil, J. Tena, R. Tomàs, M. Valls. Publicacions Matemàtiques.

- *Parallel calculation of volcanoes for cryptographic uses*. S. Martínez, R. Tomàs, C. Roig, M. Valls, R. Moreno. 7th Workshop on Parallel and Distributed Scientific and Engineering Computing at IPDPS (2006).

- *An elliptic curve and zero knowledge based forward secure RFID Protocol.* S. Martínez, M. Valls, C. Roig, F. Giné, J. Miret. Preprint.

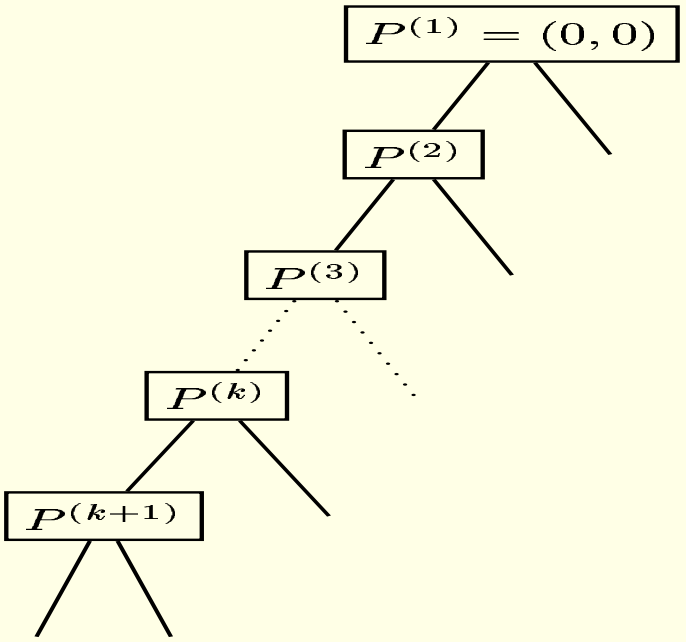
Subgrupos de Sylow de una curva elíptica sobre un cuerpo finito

- Dada una curva elíptica E sobre $\mathbb{F}_q$, determinar los enteros n y r tales que el subgrupo de $E(\mathbb{F}_q)$ de puntos que tienen orden una potencia de ℓ es $\mathbb{Z}/\ell^n\mathbb{Z} \times \mathbb{Z}/\ell^r\mathbb{Z}$. Consecuentemente

$$\#E(\mathbb{F}_q) = \ell^{n+r} \cdot m', \quad \ell \not| m'$$

y si la potencia ℓ^{n+r} es elevada, la curva se puede descartar para usos criptográficos.

- Proceso inductivo para determinar el ℓ–Sylow: (caso $\ell = 2$ y cíclico)

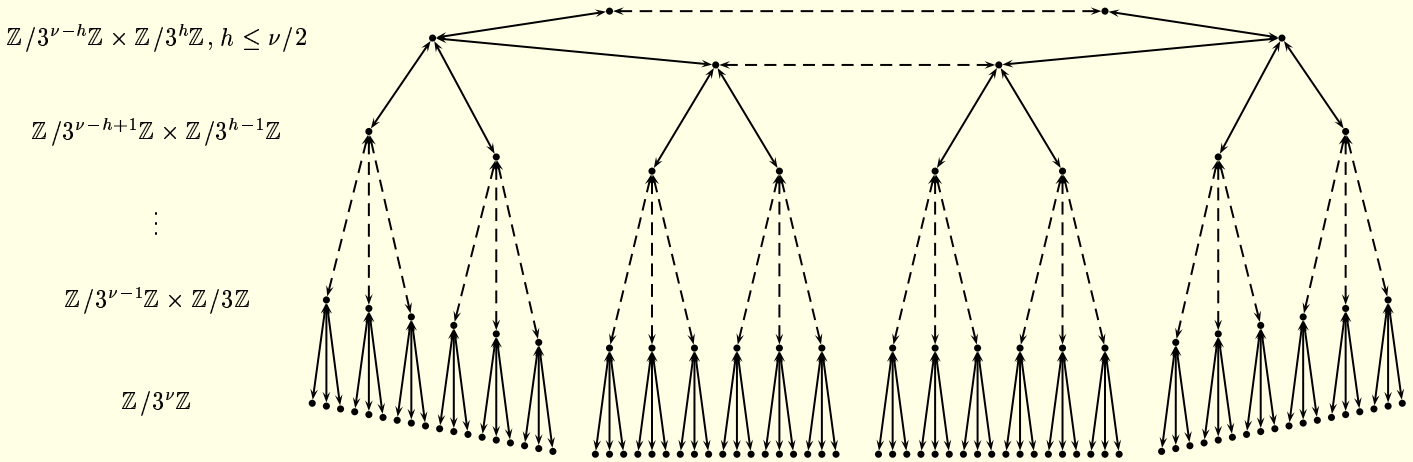


Volcanes de ℓ–isogenias

- Dada una curva $E/\mathbb{F}_q$ con un ℓ–subgrupo racional existen 1, 2 o $\ell+1$ curvas isógenas obtenidas al considerar los distintos subgrupos cíclicos de orden ℓ de $E(\mathbb{F}_q)$

- Una isogenia $\mathcal{I} : E \to E'$ se dice que es *horizontal, descendente o ascendente* según $[\mathcal{O} : \mathcal{O}'] = 1, \ell, \frac{1}{\ell}$, donde $\mathcal{O}$ y $\mathcal{O}'$ son los anillos de endomorfismos de E y E'

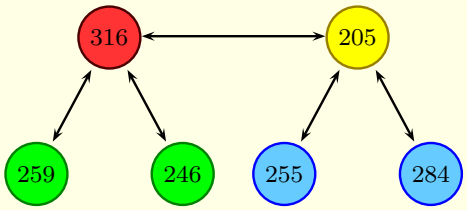
- El conjunto de clases de isomorfía de curvas elípticas sobre $\mathbb{F}_q$ con cardinal m se puede representar mediante un grafo dirigido, que tiene por arcos ℓ-isogenias. Cada componente conexa tiene forma de volcán (Kohel, Fouquet-Morain):

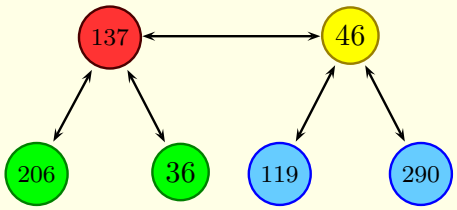


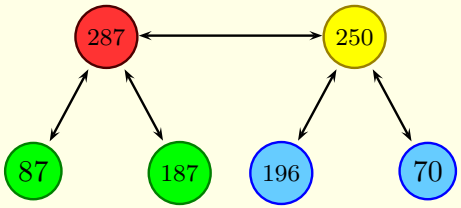
Algoritmo para recorrer las curvas de un volcán

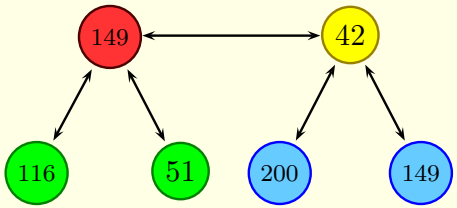
- Fórmulas de Vélu para ecuación curvas isógenas
  Camino ascendente hasta el cráter y recorrido curvas del cráter

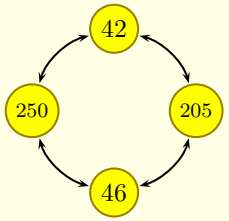
- Curvas $E_\lambda/\mathbb{F}_{317}$ de ecuación $y^2 + xy + \lambda y = x^3$ con $|E_\lambda(\mathbb{F}_{317})| = 312$

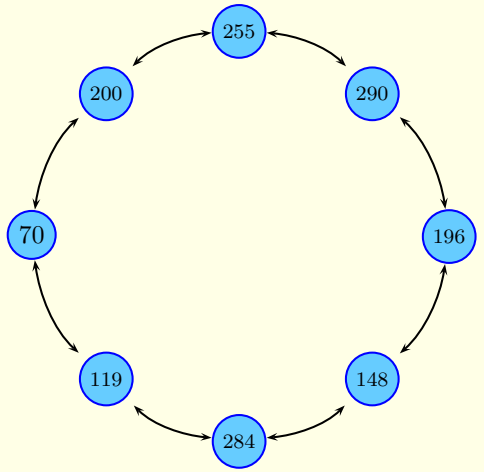


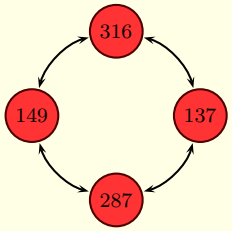


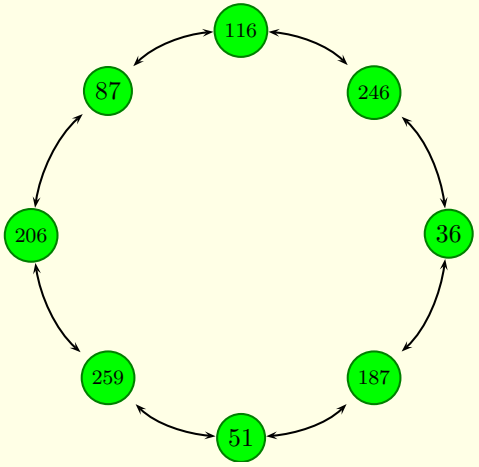








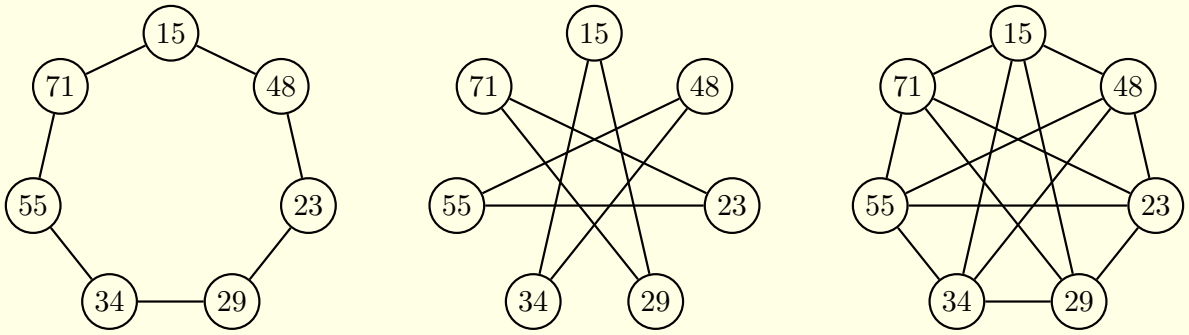




Criptosistema de Rostovsov–Stolbunov

- **Estrella de isogenias**: volcán plano de isogenias sobre $\mathbb{F}_p$ con un número primo de clases de isomorfía, donde el grado ℓ de las isogenias varía en un conjunto finito de primos de Elkies.

  Ejemplo: Estrella de 3 y 5 isogenias sobre $\mathbb{F}_{83}$ con curvas de cardinal 74



- Dada una estrella S, un conjunto de grados de isogenias de Elkies $L = \{\ell_i\}$ y un conjunto de valores propios de los Frobenius $F = \{\pi_i\}$, se define una **ruta sobre la estrella** S como un conjunto de enteros $R = \{r_i\}$, donde r_i indica el número de pasos de ℓ_i–isogenias en la dirección π_i.

- **Problema en que se basa**:
  Dadas dos curvas elípticas isógenas $E/\mathbb{F}_p$ y $E'/\mathbb{F}_p$, encontrar una isogenia $\mathcal{I} : E \longrightarrow E'$ entre ellas.

Cifrado criptosistema

- **Set up criptosistema**:
  Un cuerpo finito $\mathbb{F}_p$
  Una estrella de isogenias S sobre $\mathbb{F}_p$ y una curva $E_{init}/\mathbb{F}_p$ de S

- **Clave privada**: Una ruta R_{priv}
  Clave pública: La curva $E_{pub} = R_{priv}(E_{init})$

Algoritmo (Cifrado criptosistema)

INPUT: La clave pública E_{pub} y el mensaje en claro m
OUTPUT: El mensaje cifrado (s, E_{add})
Escoger una ruta aleatoria R_{enc}
Calcular $E_{enc} = R_{enc}(E_{pub})$
Calcular $s = m \cdot j_{enc} \pmod p$ y la curva $E_{add} = R_{enc}(E_{init})$

Algoritmo (Descifrado criptosistema)

INPUT: La clave pública E_{pub}, la clave privada R_{priv} y el mensaje cifrado (s, E_{add})
OUTPUT: El mensaje en claro m
Calcular $R_{priv}(E_{add}) = R_{priv}(R_{enc}(E_{init})) = R_{enc}(E_{pub}) = E_{enc}$
Calcular el mensaje $m = s \cdot j_{enc}^{-1} \pmod p$

ECC en tarjetas inteligentes

- Requerimientos
  - Representar las curvas elípticas de forma eficiente
  - Usar operaciones con menos coste computacional

- Ataques pasivos conocidos
  - **Side channel attack**
    Obtiene información de k a partir del cálculo de $k \cdot P$
  - **Zero-value point attack**
    Obtiene información al considerar puntos con valores 0:
    $x = 0$, $3x^2 + a = 0$, $x^2 - a = 0$, $x^2 + a = 0$

- Se puede evitar usando curvas isógenas
  La curva $E/\mathbb{F}_p : y^2 = x^3 + ax + b$ definida por

$$\begin{aligned} p &= 4451685225093714772084598273548427 \\ a &= -3, \qquad b = 2061118396808653202909616638851 4 \end{aligned}$$

  tiene puntos con $3x^2 + a = 0$. No tiene su 7-isógena $E'/\mathbb{F}_p : y^2 = x^3 + a'x + b'$,

$$a' = 1, \qquad b' = 81158144203849011712535176693868 2$$

Protocolos RFID seguros

- Los sistemas RFID permiten automatizar procesos de identificación a distancia de objetos. Constan de:
  - Un conjunto de *tags*, etiquetas con un microchip diseñado para transmitir datos vía un canal wireless
  - Una base de datos con información de los tags
  - Un lector/es que comunica con los tags y la base de datos

- Para garantizar la seguridad de un sistema RFID, el lector guarda una clave secreta cuyo conocimiento tiene que demostrar para leer los tags

- Propuesta de autenticación del lector
  - Protocolo de conocimiento nulo con curvas elípticas

- Propuesta de identificación de un tag
  - El tag envía información de su secreto al lector que comprueba si está almacenada en la base de datos
  - El tag calcula y guarda un nuevo secreto