Criptografía de Curva Elíptica

Una introducción básica

Denise Goya (dhgoya@ime.usp.br)

Universidade de São Paulo - Instituto de Matemática e Estatística

Seminario
feb/2009

projeto Fapesp n° 2008/06189-0

Sumario

Motivaciones

Ambiente:

- En criptosistemas de clave pública
- Especialmente los basados en el problema del logaritmo discreto

Un criptosistema basado en curva elíptica puede lograr:

- menores longitudes de las claves
  - mayor rapidez de cálculo
  - menos memoria y ahorro en transferencia de los datos
- con seguridad equivalente
- cuando se compara con criptosistemas clásicos, como el RSA

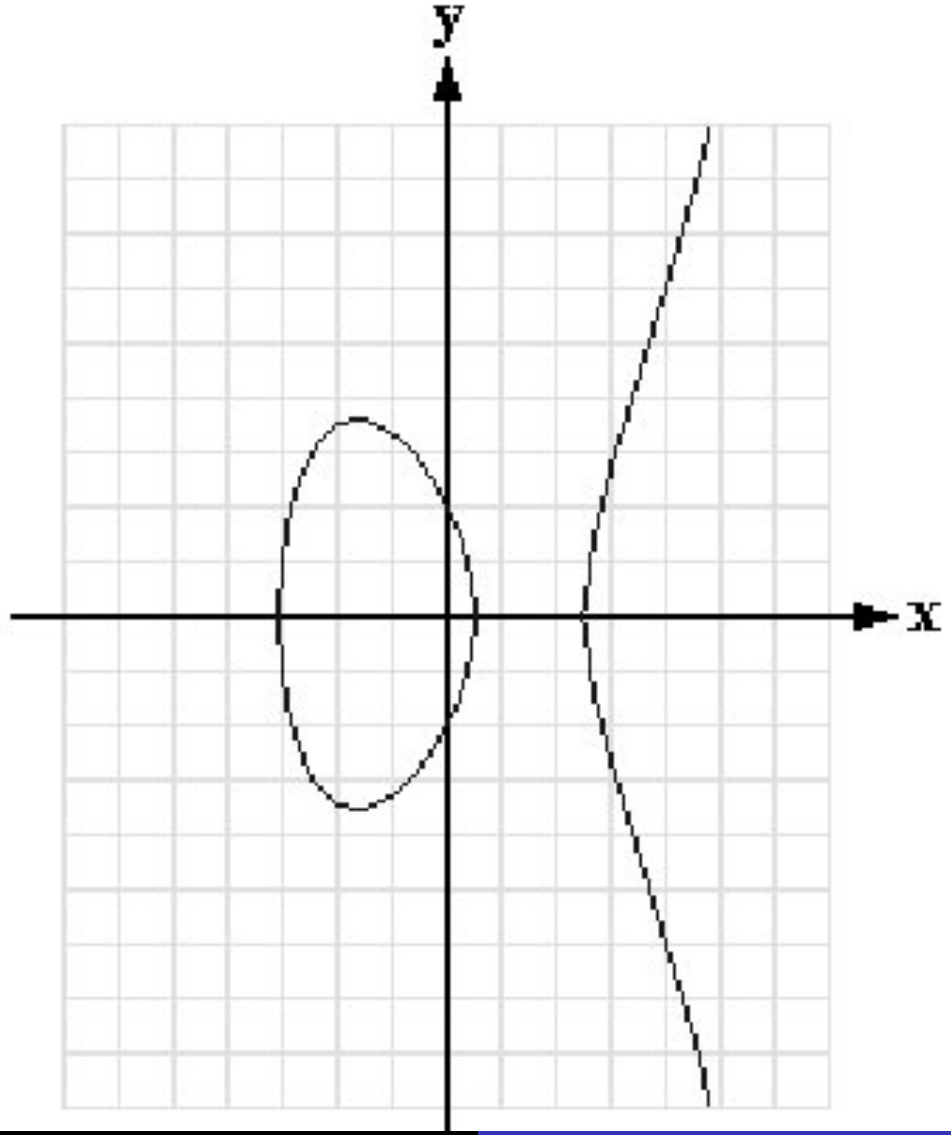
Ecuación de la curva

- Sea K un cuerpo (campo)
- $a, b, c, d, e \in K$
- y la ecuación

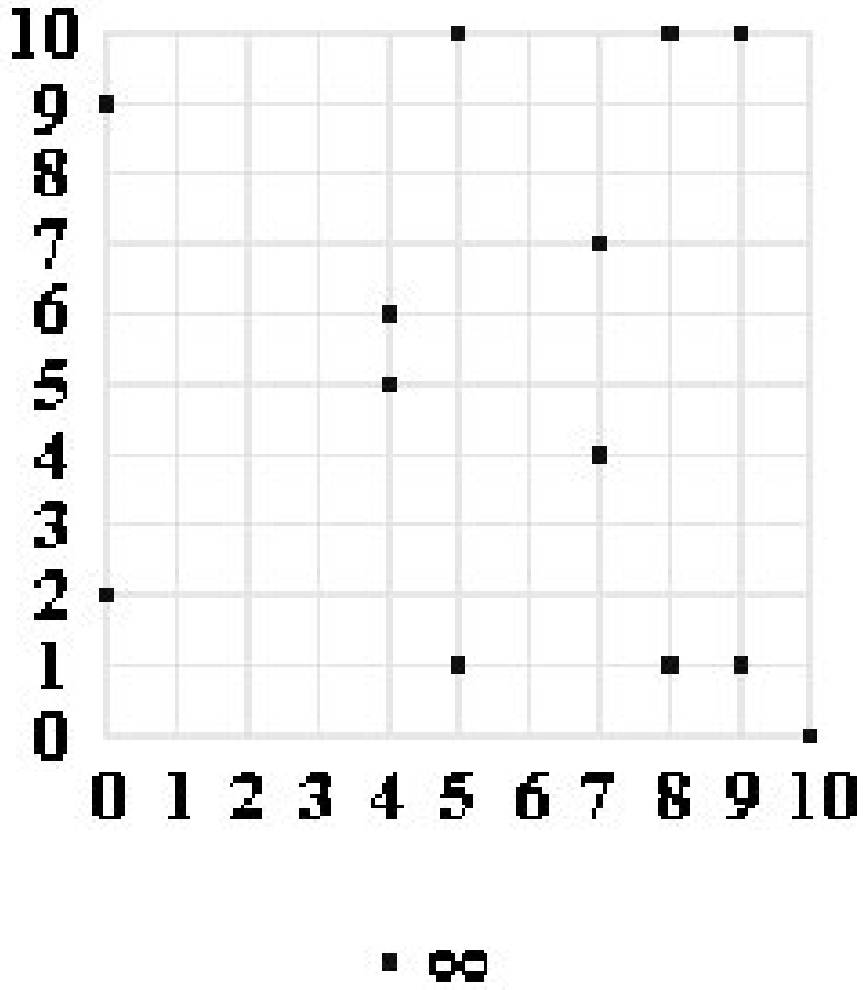
$$y^2 + axy + by = x^3 + cx^2 + dx + e$$

- una curva elíptica $E(K)$ es
  - el conjunto de puntos que satisfacen la ecuación
  - mas un punto $\mathcal{O}$ en el infinito
- según la característica del cuerpo K, usamos transformaciones lineales para simplificar la ecuación

Ejemplo: $y^2 = x^3 - 8x + 4$ sobre $\mathbb{R}$



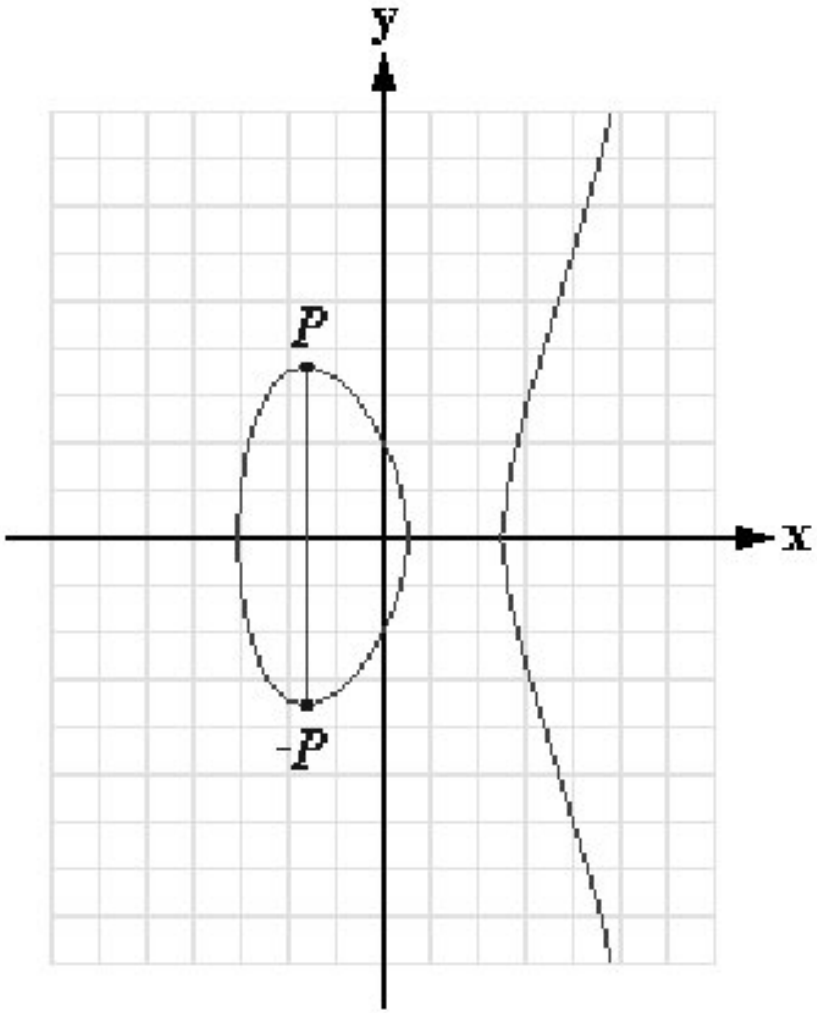
Ejemplo: $y^2 = x^3 - 8x + 4$ sobre $\mathbb{Z}_{11}$



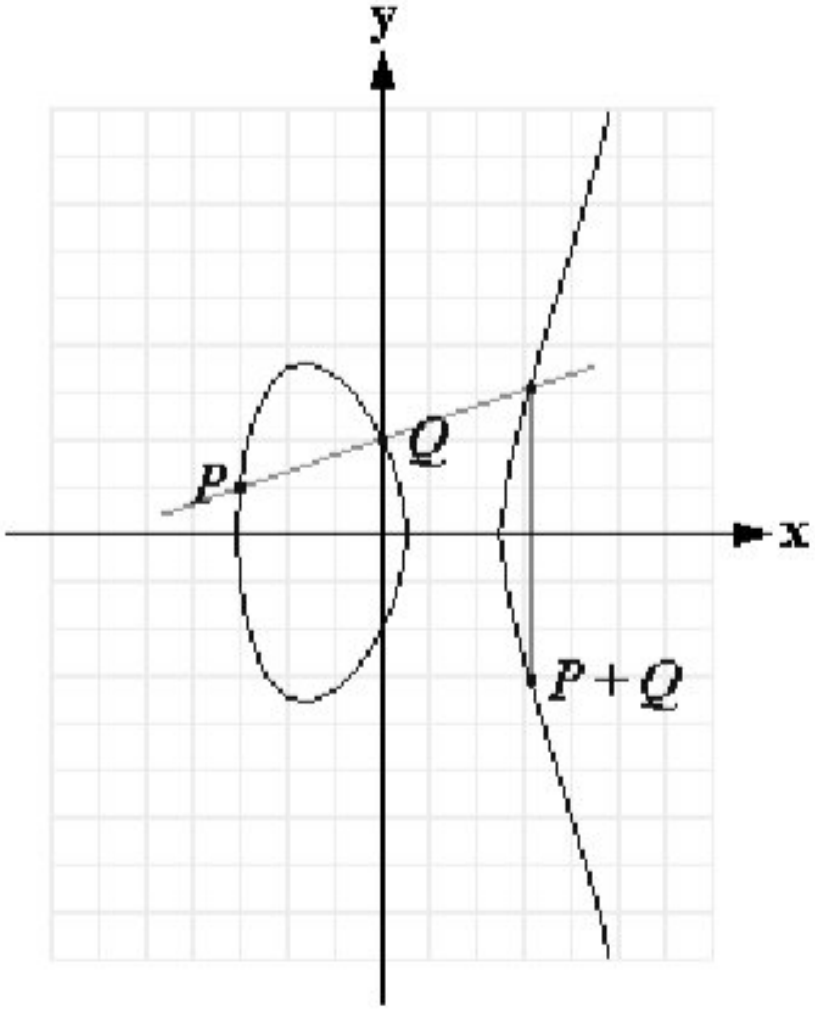
Operaciones con los puntos

- Definimos operaciones geométricas sobre los puntos:
  - recta tangente
  - recta secante
- con el objetivo de obtener un grupo algebraico

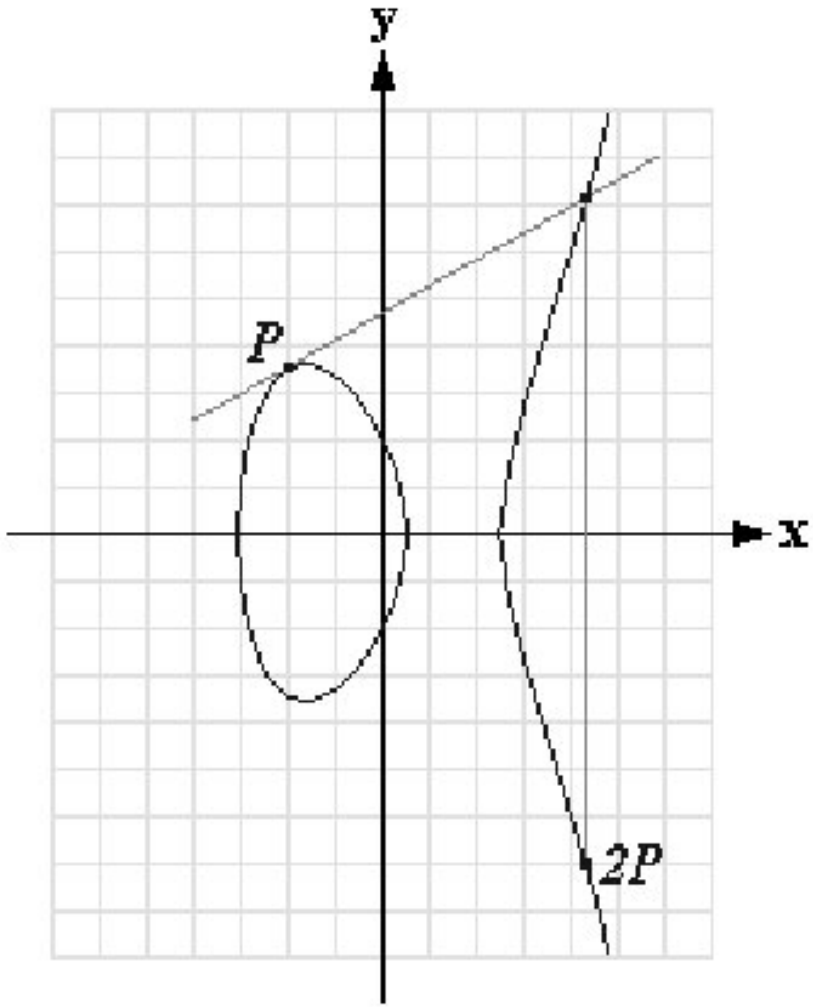
Inverso de un punto



Suma de dos puntos (secante)

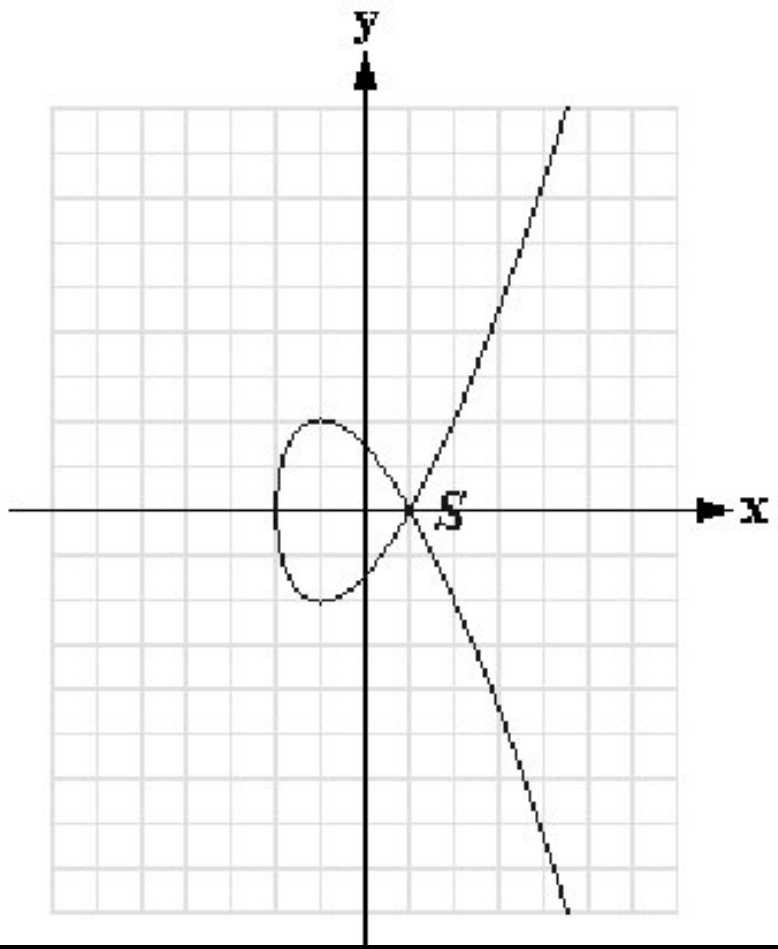


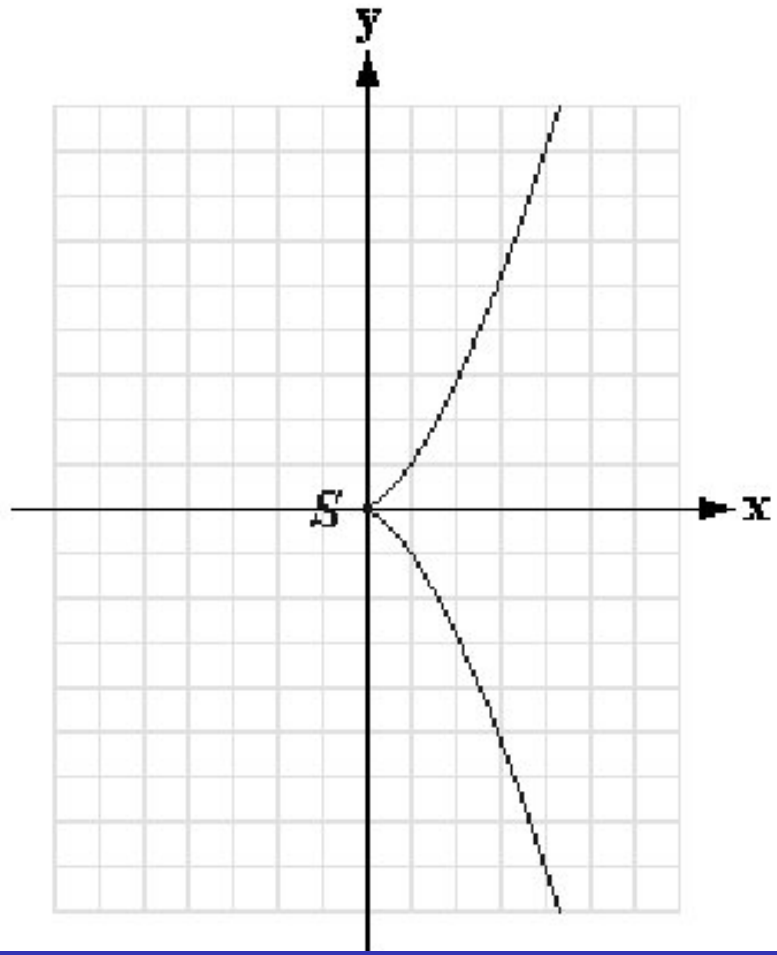
Doble: $P + P = 2P$ (tangente)



Curvas degeneradas

Debemos evitar las curvas con singularidades (tangente no es posible cuando discriminante $= 0$)





El cálculo de la suma

- es posible deducir fórmulas para calcular la suma
- ellas dependerán de la característica del cuerpo K

Ejemplo: suma en $GF(q)$

$y^2 = (x^3 + ax + b)$, con $4a^3 + 27b^2 \neq 0 \ mod \ p$

Sea $P = (x_1, y_1)$ y $Q = (x_2, y_2)$
Se define $P + Q = (x_3, y_3)$ por:

$x_3 = t^2 - x_1 - x_2$
$y_3 = t(x_1 - x_3) - y_1$, donde:

$$t = \begin{cases} \left(\frac{y_2 - y_1}{x_2 - x_1}\right) & \text{si} \quad P \neq Q \\ \left(\frac{3x_1^2 + a}{2y_1}\right) & \text{si} \quad P = Q \end{cases}$$

Ejemplo: suma en $GF(2^m)$

$y^2 + cy = (x^3 + ax + b)$, con $c \neq 0 \ mod \ 2^m$

$$x_3 = \begin{cases} \left(\frac{y_1+y_2}{x_1+x_2}\right)^2 + x_1 + x_2 & \text{si} \quad P \neq Q \\ \frac{x_1^4+a^2}{c^2} & \text{si} \quad P = Q \end{cases}$$

$$y_3 = \begin{cases} \left(\frac{y_1+y_2}{x_1+x_2}\right)(x_1 + x_3) + y_1 + c & \text{si} \quad P \neq Q \\ \left(\frac{x_1^2+a}{c}\right)(x_1 + x_3) + y_1 + c & \text{si} \quad P = Q \end{cases}$$

Grupo elíptico

- Una curva elíptica no-degenerada
- con la operación de suma y con
- $P + (-P) = \mathcal{O}$
- componen un grupo algebraico, llamado grupo elíptico

Criptografía de curva elíptica

- [Miller85] y [Koblitz87] introdujeron las curvas elípticas sobre cuerpos finitos para uso en criptografía
- Algunas ventajas:
  - para cada cuerpo finito, hay muchos grupos elípticos
  - misma seguridad computacional, pero con claves más cortas

Los tamaños de las claves

Tipo de criptografía			
Simétrico	Elíptico	RSA	
		[NIST05]	[ECRYPT05]
80	160	1024	1248
128	256	3072	3248
256	512	15360	15424

(en bits)

Para usar

- Para evitar algunos tipos de ataques:
  - usamos curvas que contienen subgrupos cíclicos de orden prima
  - evitamos curvas anómalas (las que tienen el mismo cardinal que el cuerpo)
  - evitamos algunas curvas supersingulares ($p|t$, donde p es la característica del cuerpo $GF(q)$ y $\#E = q + 1 - t$)
- Creemos que el problema del logaritmo discreto es dificil, excepto en los dos últimos casos (que son la minoría)

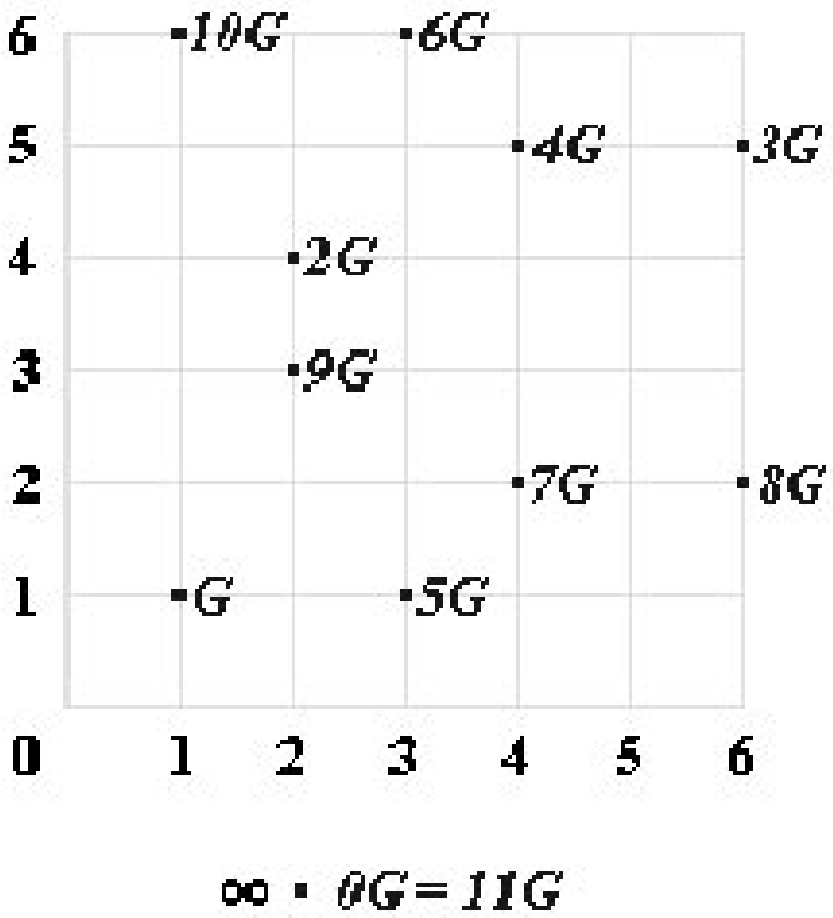
Áreas de investigación

- Son estudiados
  - ¿cómo escoger las curvas?
  - ¿cómo contar los puntos de una curva?
  - ¿cómo optimizar las computaciones (aritmética del cuerpo y de la curva)?
- Estándares
  - ISO, IEEE, ANSI, NIST, etc [lista]

Ejemplo: Diffie-Hellman con curva elíptica

- Diffie-Hellman: protocolo para intercambio de claves
- Sea E una curva elíptica con G un generador de un subgrupo cíclico de orden prima p
- Alice elige un entero secreto x_A; Bob elige x_B
- Las claves públicas correspondientes son
  - $Y_A = x_A \cdot G$
  - $Y_B = x_B \cdot G$
- La clave compartida es
  - $K = x_A \cdot x_B \cdot G$
  - Alice calcula $K = x_A \cdot Y_B$
  - Bob calcula $K = x_B \cdot Y_A$

Ejemplo: $y^2 = x^3 + x - 1$ sobre $\mathbb{Z}_7$, con $G = (1, 1)$



Ejemplo de claves

- Alice elige $x_A = 4$; calcula $Y_A = 4 \cdot G = (4, 5)$
- Bob elige $x_B = 9$; calcula $Y_B = 9 \cdot G = (2, 3)$

- Alice calcula $K = x_A \cdot Y_B = 4 \cdot (2, 3) = (6, 5)$
- Bob calcula $K = x_B \cdot Y_A = 9 \cdot (4, 5) = (6, 5)$

- $K = x_A \cdot x_B \cdot G = 4 \cdot 9 \cdot G = (36 \bmod 11) \cdot G =$
  $= 3 \cdot G = (6, 5)$

Conclusión

- El uso de curvas elípticas es muy actrativo para
  - dispositivos mobiles
  - red de sensores
  - tarjetas inteligentes
  - todas las aplicaciones donde hay restricción de recursos y sea necesaria la seguridad

¿Preguntas?

Enlace

Esta presentación puede ser encontrada en:
www.ime.usp.br/∼dhgoya/ecc.pdf

Referencias(1/2)

V. Miller

Uses of elliptic curves in cryptography.

Crypto'85. LNCS 218, 1986, 417-426.

N. Koblitz

Elliptic curve cryptossystems.

Mathematics of Computation, 117, 1987, 203-209.

NIST

Recommendation for Key Management Part 1: General, Nist Special Publication 800-57. August, 2005.

ECRYPT

Yearly Report on Algorithms and Keysizes (2004), March 2005.

Referencias(2/2)


Elliptic Curve Cryptography Standards
http://www.securitytechnet.com/crypto/algorithm/ecc.html


I. Blake, G. Seroussi, N. Smart
Advances in Elliptic Curve Cryptography.
Cambridge University Press, 2005.


N. Koblitz
Algebraic Aspects of Cryptography.
Springer-Verlag. 3th print, 2004.