Curvas Elípticas en Criptografía

Trabajo Fin de Grado

Adrián H. Ranea Robles

14 de julio de 2016

Universidad de Granada

Tabla de contenidos

Teoría de curvas elípticas

Definición de curva elíptica

Sea K un cuerpo de característica distinta de 2 y 3.

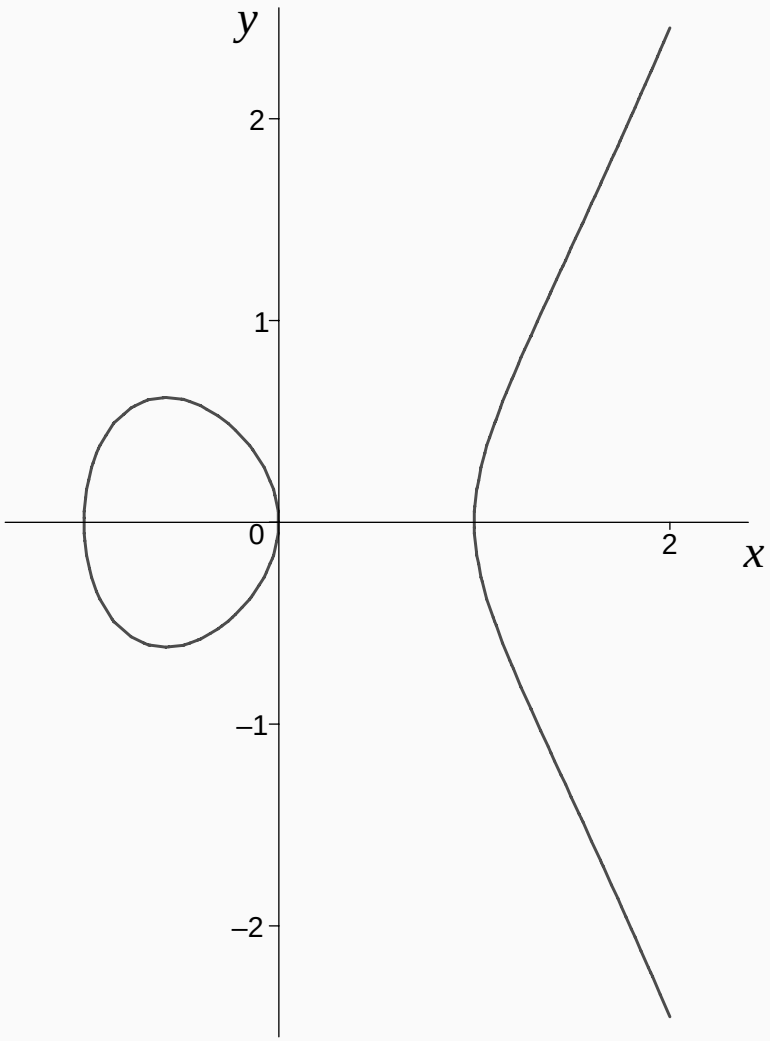
Una curva elíptica E se define por una ecuación de la forma

$$E : y^2 = x^3 + ax^2 + b \tag{1}$$

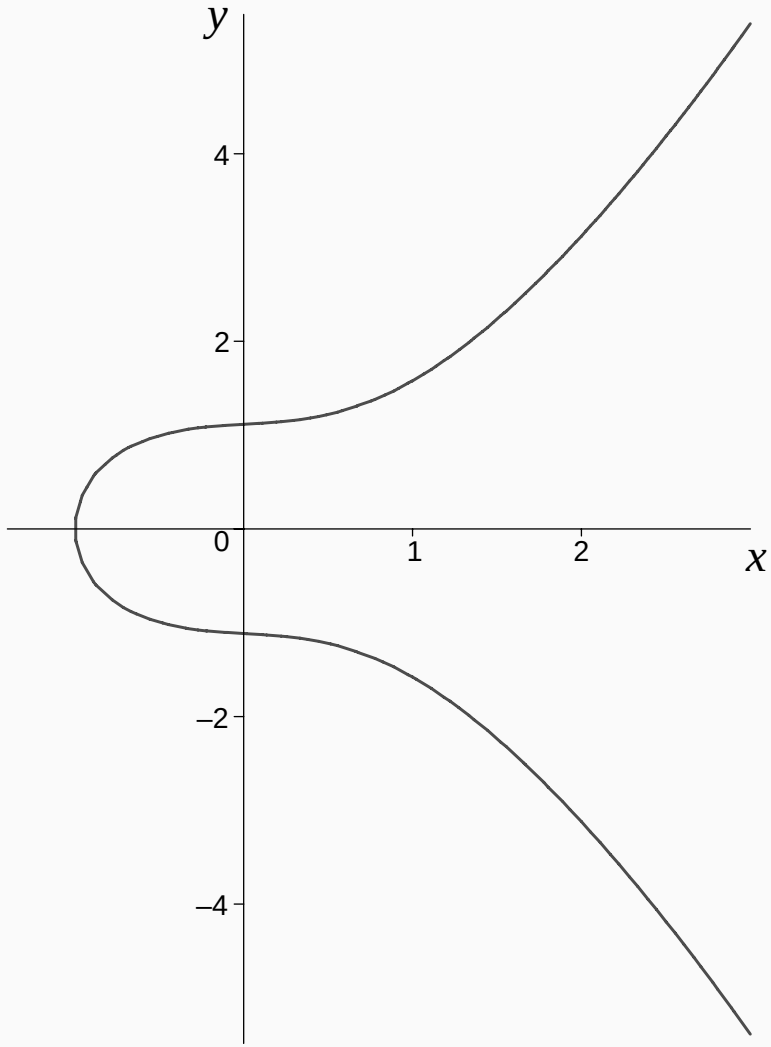
donde $a, b \in K$ y $-16(4a^3 + 27b^2) \neq 0$.

Denotamos por $E(K)$ al conjunto de pares $(x, y) \in K \times K$ que verifican (1) más un punto adicional ∞.

Ejemplos de curvas elípticas sobre $\mathbb{R}$

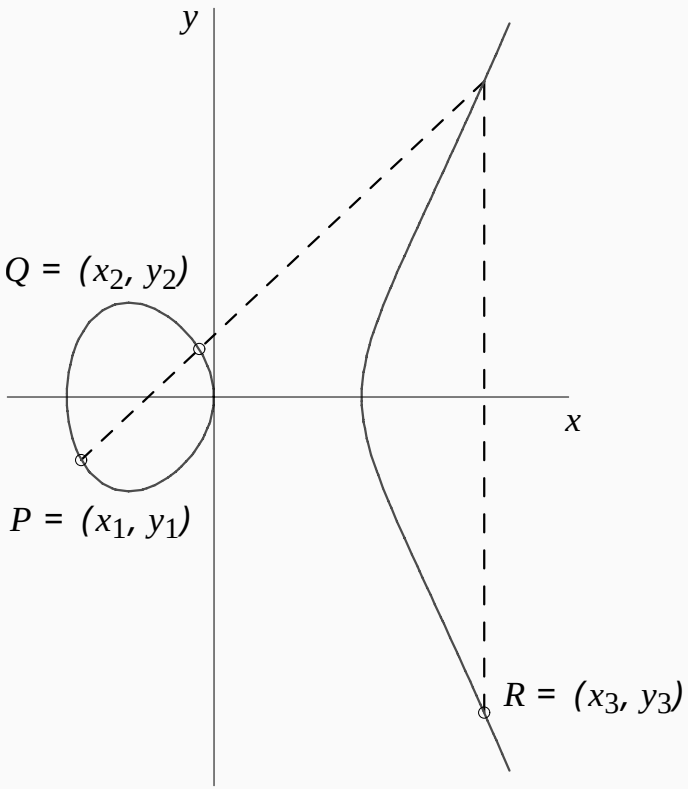


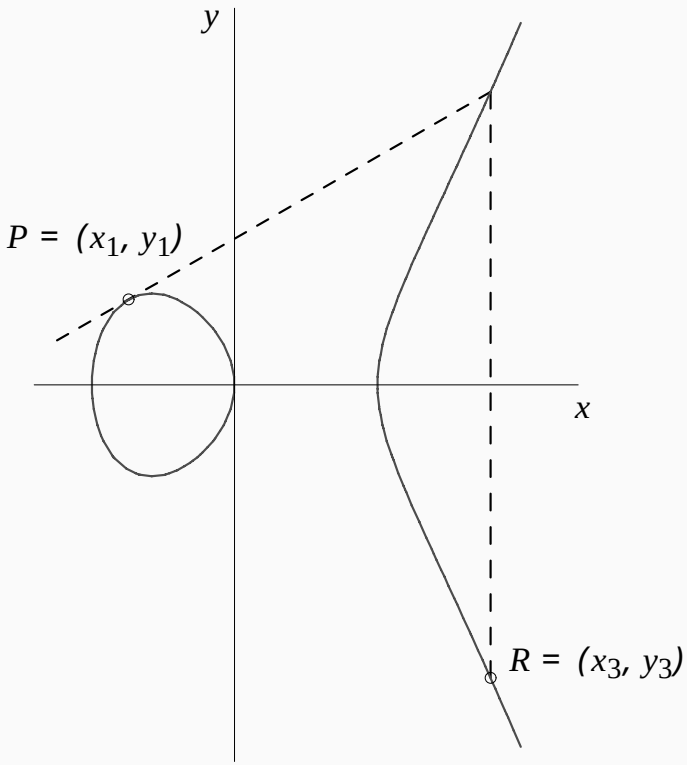
$y^2 = x^3 - x$



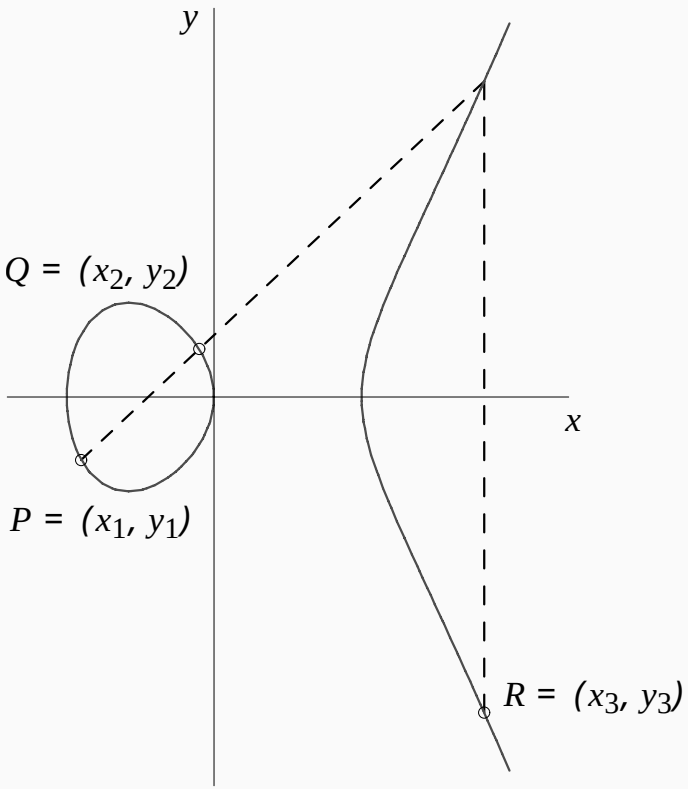
$y^2 = x^3 + x$

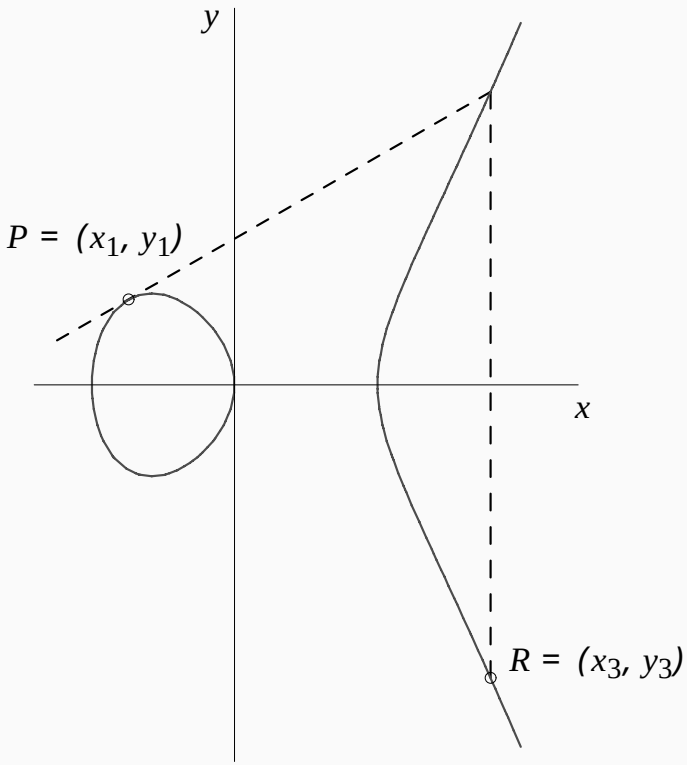
Versión geométrica del método de la cuerda y la tangente





Versión geométrica del método de la cuerda y la tangente





Teorema

$(E(K), +, \infty)$ es un grupo abeliano.

Endomorfismos

Un endomorfismo de E es un homomorfismo $\alpha : E(\overline{K}) \to E(\overline{K})$ dado por funciones racionales r_1, r_2

$$\alpha(x, y) = (r_1(x), r_2(x)y).$$

El grado de α es el grado de r_1.

α es separable si la derivada $r_1(x)'$ no es idénticamente cero.

Un ejemplo es el *endomorfismo multiplicación por n*

$$n(P) = nP, \ \forall P \in E(\overline{K}).$$

Endomorfismos

Proposición

α es separable $\implies$ $\deg(\alpha) = |\ker(\alpha)|$.

α no es separable $\implies$ $\deg(\alpha) > |\ker(\alpha)|$.

Proposición

$\alpha \neq 0 \implies \alpha$ es sobreyectiva.

Proposición

$n(P)$ es separable $\iff$ $car(K) \nmid n$.

Subgrupos de torsión

Un elemento de $E(\overline{K})$ cuyo orden es finito se llama punto de torsión.

El subgrupo de n-torsión es el subgrupo de $E(\overline{K})$ dado por

$$E[n] = \{P \in E(\overline{K}) \mid nP = \infty\}.$$

Subgrupos de torsión

Un elemento de $E(\overline{K})$ cuyo orden es finito se llama punto de torsión.

El subgrupo de n-torsión es el subgrupo de $E(\overline{K})$ dado por

$$E[n] = \{P \in E(\overline{K}) \mid nP = \infty\}.$$

Teorema

Si $car(K) \nmid n$, entonces

$$E[n] \simeq \mathbb{Z}_n \oplus \mathbb{Z}_n.$$

Si $car(K) = p > 0$, y $p|n$, entonces

$$E[n] \simeq \mathbb{Z}_{n'} \oplus \mathbb{Z}_{n'} \text{ o } \simeq \mathbb{Z}_n \oplus \mathbb{Z}_{n'}$$

donde $n = p^r n'$ con $p \nmid n'$.

Curvas elípticas sobre cuerpos finitos

Sea $\mathbb{F}_q$ el cuerpo finito de q elementos.

$E(\mathbb{F}_q)$ es un grupo abeliano *finito*.

Un ejemplo importante de endomorfismo sobre $E(\overline{\mathbb{F}_q})$ es el *endormofirsmo de Frobenius*

$$\phi_q(x, y) = (x^q, y^q), \quad \phi_q(\infty) = \infty$$

Curvas elípticas sobre cuerpos finitos

Sea $\mathbb{F}_q$ el cuerpo finito de q elementos.

$E(\mathbb{F}_q)$ es un grupo abeliano *finito*.

Un ejemplo importante de endomorfismo sobre $E(\overline{\mathbb{F}_q})$ es el *endormofirsmo de Frobenius*

$$\phi_q(x, y) = (x^q, y^q), \quad \phi_q(\infty) = \infty$$

Proposición

Sea E una curva elíptica definida sobre un cuerpo finito $\mathbb{F}_q$ y consideremos el endomorfismo $\phi_q^n - 1$ con $n \geq 1$. Entonces

1. $\ker(\phi_q^n - 1) = E(\mathbb{F}_{q^n})$.
2. $\phi_q^n - 1$ es separable, por lo que $|E(\mathbb{F}_{q^n})| = \deg(\phi_q^n - 1)$.

Teorema de Hasse

Teorema de Hasse

Sea E una curva elíptica definida sobre un cuerpo finito $\mathbb{F}_q$. Entonces el orden de $E(\mathbb{F}_q)$ verifica

$$|q + 1 - |E(\mathbb{F}_q)|| \leq 2\sqrt{q}.$$

Criptografía con curvas elípticas

Seguridad del ECDLP

El problema del logaritmo discreto sobre curvas elípticas
Dada una curva elíptica E sobre $\mathbb{F}_q$, un punto $P \in E(\mathbb{F}_q)$ de orden n y un punto $Q \in \langle P \rangle$, encontrar el entero $k \in [0, n-1]$ tal que $Q = kP$.

Con las siguientes restricciones sobre los parámetros:

- $n > 2^{80}$.
- $p > 2^{160}$.
- $|E(\mathbb{F}_q)| \neq q, q-1$.

se cree que el ECDLP es intratable para los ataques conocidos.

Parámetros de dominio y pareja de llaves

Los participantes de un protocolo suelen acordar unos parámetros de dominio:

- Una curva elíptica E definida sobre un cuerpo finito $\mathbb{F}_q$
- Un punto base $P \in E(\mathbb{F}_q)$ junto a su orden n.

Además, cada uno dispone de una pareja de llaves:

- Una llave privada d
- Una llave pública Q.

Para generar la pareja de llaves, se elige un punto aleatorio $Q = dP$ en el grupo $\langle P \rangle$. La correspondiente llave privada es $d = \log_p Q$.

Porqué usar curvas elípticas en criptografía

Los dos principales problemas intratables usados en los sistemas de llave pública son:

- El problema de factorización de enteros $\rightarrow$ RSA.
- El problema del logaritmo discreto $\rightarrow$ ECC.

Porqué usar curvas elípticas en criptografía

Los dos principales problemas intratables usados en los sistemas de llave pública son:

- El problema de factorización de enteros $\rightarrow$ RSA.
- El problema del logaritmo discreto $\rightarrow$ ECC.

	Nivel de seguridad (bits)				
	80	112	128	192	256
ECC (orden n)	160	224	256	384	514
RSA (módulo n)	1024	2048	3072	8192	15360

Cuadro 1: Comparación de tamaños de parámetros para niveles de seguridad equivalentes.

ECDH

Protocolo de Intercambio de Llaves Diffie-Hellman para Curvas Elípticas (ECDH)

1. Alicia y Bob concuerdan unos parámetros de dominio $D = (q, a, b, P, n)$.
2. Alicia calcula su pareja de llaves (Q_A, d_A).
3. Bob calcula su pareja de llaves (Q_B, d_B).
4. Alicia y Bob intercambian sus llaves pública Q_A, Q_B.
5. Alicia calcula $d_A Q_B$ y Bob calcula $d_B Q_A$. Ambos cálculos devuelven el punto $(d_A d_B)P$.

ccepy

ccepy es una biblioteca escrita en python 3 para implementar técnicas de la criptografía con curvas elípticas.

Herramientas

- Sphinx
- Hypothesis
- Google Style Guide
- Git

Módulos

El software ccepy consta de cuatro módulos principales:

- Aritmética elemental
- Cuerpos finitos
- Curvas elípticas
- Esquemas criptográficos

y uno secundario:

- Listado de curvas elípticas.

Curvas elípticas

Aritmética con curvas elípticas.

Este módulo permite operar con el grupo de puntos de una curva elíptica.

Para utilizar las funciones y las clases de este módulo, debe importarlo previamente:

```
# reemplace ... por la función/clase que desea utilizar
from ccepy.curvas_elipticas import ...
```

Para operar con puntos de una curva elíptica, use las funciones de la forma `curva_eliptica_sobre_*` y los operadores aritméticos habituales.

```
>>> E = curva_eliptica_sobre_Fq(a=2, b=3, p=97)  # y^2 = x^3 + 2x + 3 sobre F97
>>> E.coeficientes
Coeficientes(a=2, b=3)
>>> P = E(0, 10)
>>> P
(0,10)
>>> Q = E(3, 6)
>>> Q
(3,6)
>>> P + Q
(85,71)
>>> -P
(0,87)
>>> 3 * P
(23,24)
```

Usando ccepy

Para instalar la última versión de ccepy:

```
pip install ccepy
```

Un ejemplo de aritmética de curvas elípticas:

```
>>> E = curva_eliptica_sobre_Fq(a=2, b=3, p=97)
>>> E(0, 10) + E(3, 6)
(85,71)
```

Estudio del cifrado de las páginas de la UGR

HTTPS

HTTP envía la información en texto claro.

Problema: cualquiera que intercepte el tráfico de red puede leer lo que se está enviando y recibiendo.

Solución: HTTPS. Utiliza los protocolos criptográficos SSL/TLS de la capa de transporte para cifrar el tráfico HTTP.

HTTPS

HTTP envía la información en texto claro.

Problema: cualquiera que intercepte el tráfico de red puede leer lo que se está enviando y recibiendo.

Solución: HTTPS. Utiliza los protocolos criptográficos SSL/TLS de la capa de transporte para cifrar el tráfico HTTP.

Todas las páginas web que requieran información sensible deberían utilizar HTTPS sobre SSL/TLS y no HTTP.

Páginas web de la UGR vulnerables

Numerosas páginas web de la Universidad de Granada solicitan credenciales y no cifran el tráfico (no implementan HTTPS).

- `http://sucre.ugr.es`
- `http://calidad.ugr.es`
- `http://secretariageneral.ugr.es`
- `http://internacional.ugr.es`
- ...

Páginas web de la UGR vulnerables

Numerosas páginas web de la Universidad de Granada solicitan credenciales y no cifran el tráfico (no implementan HTTPS).

- `http://sucre.ugr.es`
- `http://calidad.ugr.es`
- `http://secretariageneral.ugr.es`
- `http://internacional.ugr.es`
- ...

Otras páginas permiten tanto el envío de las credenciales cifradas o no cifradas (permiten tanto HTTP como HTTPS).

- `http://oficinavirtual.ugr.es/ai`
- `http://sede.ugr.es/sede/mis-procedimientos/index.html`

¿Preguntas?