

## 9. Criptosistemas de curvas elípticas (ECC)

- Provee el mismo nivel de seguridad que RSA o sistemas de logaritmos complejos con operandos considerablemente más cortos.
- Basado en el problema de logaritmo discreto generalizado.
- RSA con llaves cortas es mucho más rápido que ECC

### 9.1 Cómo hacer cálculos con curvas elípticas

Paso 1: Encontrar un grupo cíclico en el cual construir un criptosistema  
¡No sólo debe existir un grupo cíclico!

Debemos encontrar un grupo cíclico en el que el problema del logaritmo discreto sea computacionalmente complicado

#### 9.1.1 Definición de curvas elípticas

→ Por curva nos referimos a puntos que satisfacen una ecuación.

##### Definición

La **curva elíptica** sobre  $\mathbb{Z}_p$ ,  $p > 3$ , es el conjunto de pares  $(x, y) \in \mathbb{Z}_p^2$  que satisfacen

$$y^2 \equiv x^3 + a \cdot x + b \pmod{p}$$

en conjunto con un punto imaginario de infinito  $\mathcal{O}$  donde  $a, b \in \mathbb{Z}_p$  y la condición

$$4 \cdot a^3 + 27 \cdot b^2 \neq 0 \pmod{p} \quad (*)$$

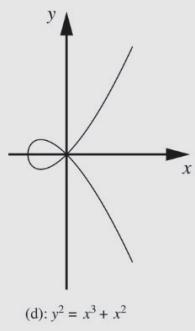
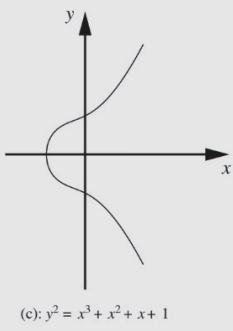
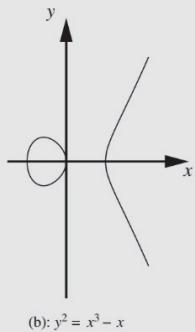
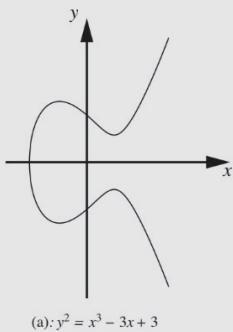
## La condición (\*)

$$4 \cdot a^3 + 27 \cdot b^2 \neq 0 \pmod{p} \Leftrightarrow \underbrace{-16(4a^3 + 27b^2)}_{\text{determinante de la curva}} \neq 0 \quad (p > 3 \text{ primo})$$

$\Leftrightarrow$  la imagen no tiene puntos de autointersección

### Observación

Podemos graficar sobre  $\mathbb{R}$  para obtener algo que se ve como una curva y notar algunas propiedades:



(1) Las curvas elípticas son simétricas respecto al eje  $x$ .

$$\begin{aligned} y^2 &\equiv x^3 + a \cdot x + b \pmod{p} \\ \Rightarrow y_i &= \sqrt{x_i^3 + ax_i + b} \\ y'_i &= -\sqrt{x_i^3 + ax_i + b} \end{aligned}$$

(2) Hay 0, 1, 2 o 3 intersecciones con el eje  $x$

$$\begin{aligned} &\left( \begin{array}{l} \text{las soluciones a la ecuación} \\ 0 = x^3 + ax + b \end{array} \right) \end{aligned}$$

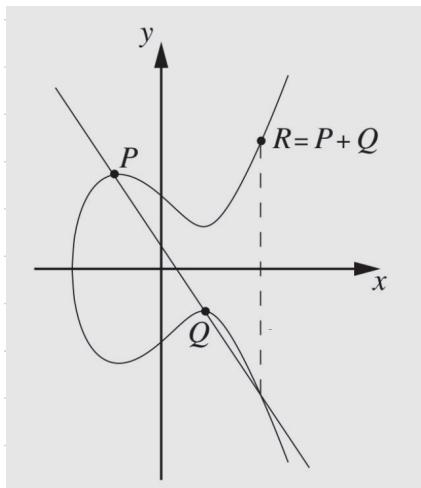
Recordemos:

Paso 1: Encontrar un grupo cíclico en el cual construir un criptosistema

Conjunto: soluciones a un curva elíptica, Operación:  $\circ$ ?

## 9.1.2 Operaciones de grupo en curvas elípticas

→ Suma de puntos distintos  $P+Q$



1: Dibujar una línea recta que pasa por  $P$  y  $Q$

2: Obtener un tercer punto de intersección entre la linea recta y la curva elíptica.

3: Tomar la reflexión de dicho punto sobre el eje  $x$

4: Definimos  $R := P+Q$  como dicho punto.

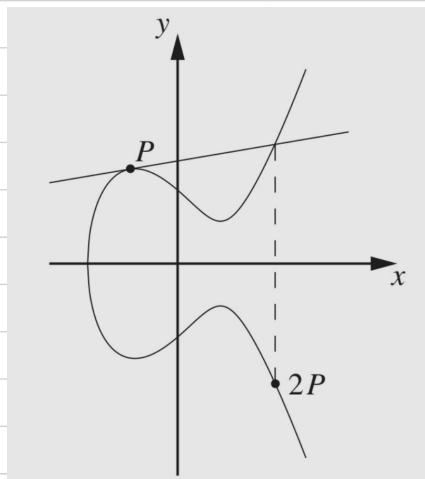
→ Suma de puntos iguales  $P+P$

1: Dibujamos la línea tangente a la curva elíptica en el punto  $P$ .

2: Obtenemos un segundo punto de intersección entre esta línea y la curva elíptica.

3: Tomar la reflexión de este punto sobre el eje  $x$ .

4: Definimos  $R := 2P$  como dicho punto.



**Nota:** A este proceso se le llama el método tangente y cuerda y cumple los axiomas de grupo.

→ Pasemos de los reales a un campo primo  $GF(p)$  y traduzcamos esta suma a algo más aritmético /analítico y menos geométrico.

### Adición y multiplicación por 2 en curvas elípticas

$$x_3 \equiv s^2 - x_1 - x_2 \pmod{p}$$

$$y_3 \equiv s(x_1 - x_3) - y_1 \pmod{p}$$

$$P = (x_1, y_1)$$

$$Q = (x_2, y_2)$$

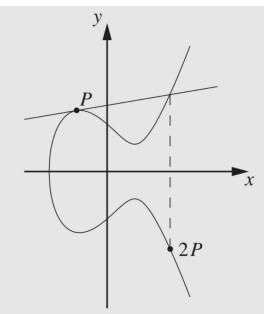
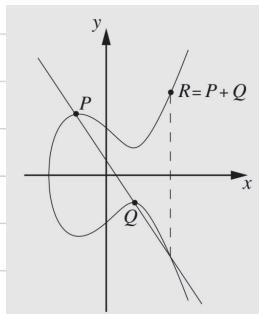
$$R = (x_3, y_3)$$

donde

$$s \equiv \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} \pmod{p}, & \text{si } P \neq Q \\ \frac{3x_1^2 + a}{2y_1} \pmod{p} & \text{si } P = Q \end{cases}$$

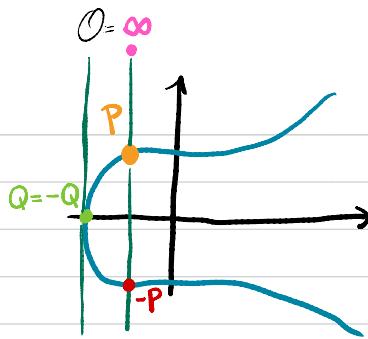
### Observación

- En la adición,  $s$  es la pendiente de la curva que pasa por  $P$  y  $Q$
- En la multiplicación por 2,  $s$  es la pendiente de la recta tangente en el punto  $P$



Ya tenemos una operación **¿Cuál es el neutro?**

! No hay un punto  $(x,y)$  que se comporte como neutro



Neutro = punto al infinito

¿Cuáles son los inversos?

$$\text{Sea } P = (x, y) \Rightarrow -P = (x, p-y)$$

Encontrar el inverso es fácil:  $-y \equiv p-y \pmod{p}$

$$\Rightarrow -P = (x, p-y)$$

Esto nos da un grupo  $(GF(p), +)$

## 9.2 Construyendo un problema del logaritmo discreto con curvas elípticas

### Teorema

Los puntos de una curva elíptica en conjunto con el punto al infinito tiene subgrupos cíclicos. Bajo ciertas condiciones todos los puntos de una curva elíptica son un grupo cíclico.

Ejemplo: El grupo cíclico de una curva elíptica

Queremos encontrar todos los puntos de la curva

$$E: y^2 = x^3 + 2 \cdot x + 2 \pmod{17}$$

Sucede que el número de puntos en la curva y el orden del grupo son  $\#E=19 \Rightarrow$  El grupo es cíclico

Veamos cuáles son estos elementos

Comenzamos con el elemento primitivo  $P = (5, 1)$ . Calculando las potencias de  $P$  obtenemos los siguientes elementos

$$2P = (5, 1) + (5, 1) = (6, 3)$$

$$3P = 2P + P = (10, 6)$$

$$4P = (3, 1)$$

$$5P = (9, 16)$$

$$6P = (16, 13)$$

$$7P = (0, 6)$$

$$8P = (13, 7)$$

$$9P = (7, 6)$$

$$10P = (7, 11)$$

$$11P = (13, 10)$$

$$12P = (0, 11)$$

$$13P = (16, 4)$$

$$14P = (9, 1)$$

$$15P = (3, 16)$$

$$16P = (10, 11)$$

$$17P = (6, 14)$$

$$18P = (5, 16)$$

$$19P = \emptyset$$

**Nota:** Para construir un criptosistema de logaritmo discreto es importante conocer la cardinalidad del grupo con el que estamos trabajando.

El sig. teo. nos da un aproximado

### Teorema (Hasse's Theorem)

Dada una curva elíptica  $E$  módulo  $p$ , el número de puntos en la curva se denota por  $\#E$  y satisface lo sig

$$p+1-2\sqrt{p} \leq \#E \leq p+1+2\sqrt{p}$$

⇒ el orden del grupo  $\approx p$

- Si queremos usar una curva elíptica con  $2^{256}$  elementos  
⇒ necesitamos un primo de longitud  $\approx 256$  bits

### Definición (Problema del logaritmo discreto para curvas elípticas (ECDLP))

Dada una curva elíptica  $E$ , consideramos un elemento primitivo  $P$  y algún otro elemento  $T$ . El problema DL es encontrar el entero  $d$ , con  $1 \leq d \leq \#E$ , tal que

$$\underbrace{P + P + \dots + P}_{d-\text{veces}} = d \cdot P = T$$

En criptosistemas:

- $d \leftarrow$  llave privada
- $T \leftarrow$  llave pública

→ punto de la curva elíptica de coordenadas  $T = (x_T, y_T)$

**Observación:** Cuando hacíamos DL en  $\mathbb{Z}_p^*$  ambas llaves eran enteros (aquí ya no)

**Ejemplo:**

→ Resolveremos el problema DL en la curva

$$y^2 \equiv x^3 + 2x + 2 \pmod{17}$$

→ Elementos dados:  $P = (5, 1)$  elemento primitivo  
 $T = (16, 4)$  llave pública

Recordemos los cálculos dados en el ejemplo previo

$$\begin{aligned} 2P &= (5, 1) + (5, 1) = (6, 3) \\ 3P &= 2P + P = (10, 6) \\ 4P &= (3, 1) \\ 5P &= (9, 16) \\ 6P &= (16, 13) \\ 7P &= (0, 6) \\ 8P &= (13, 7) \\ 9P &= (7, 6) \\ 10P &= (7, 11) \end{aligned}$$

$$\begin{aligned} 11P &= (13, 10) \\ 12P &= (0, 11) \\ 13P &= (16, 4) \\ 14P &= (9, 1) \\ 15P &= (3, 16) \\ 16P &= (10, 11) \\ 17P &= (6, 14) \\ 18P &= (5, 16) \\ 19P &= \mathcal{O} \end{aligned}$$

$$\Rightarrow 13 \cdot P = (16, 4) = T$$

$$\Rightarrow d = 13$$

↑ llave privada

¿Cómo realizamos estos cálculos de forma eficiente?

↓ "análogo" al algoritmo elevar al cuadrado - multiplicar

Algoritmo Doble-y-Suma para Multiplicación de puntos

Input: - curva elíptica  $E$

- punto  $P$  de la curva

- número  $d = \sum_{i=0}^t d_i 2^i$  (con  $d_i \in \{0, 1\}$  y  $d_t = 1$ )

Output:  $T = d \cdot P$

## Algoritmo:

$$T = P$$

Para  $i = t-1$  hasta 0 (va disminuyendo)

$$T = T + T$$

$$\left[ \begin{array}{l} \text{Si } d_i = 1 \\ T = T + P \end{array} \right]$$

Return ( $T$ )

- Para un escalar con longitud de  $t+1$  bits, el algoritmo requiere  $1.5t$  multiplicaciones por 2 y sumas (en promedio)

Ejemplo: Multiplicación escalar 26P

$$26P = (11010_2)P = (d_4 d_3 d_2 d_1 d_0)_2 \cdot P$$

Step

$$\#0 \quad P = 1_2 P$$

initial setting, bit processed:  $d_4 = 1$

$$\#1a \quad P + P = 2P = \mathbf{10}_2 P$$

DOUBLE, bit processed:  $d_3$

$$\#1b \quad 2P + P = 3P = 10_2 P + 1_2 P = \mathbf{11}_2 P$$

ADD, since  $d_3 = 1$

$$\#2a \quad 3P + 3P = 6P = 2(11_2 P) = \mathbf{110}_2 P$$

DOUBLE, bit processed:  $d_2$

$$\#2b$$

no ADD, since  $d_2 = 0$

$$\#3a \quad 6P + 6P = 12P = 2(110_2 P) = \mathbf{1100}_2 P$$

DOUBLE, bit processed:  $d_1$

$$\#3b \quad 12P + P = 13P = 1100_2 P + 1_2 P = \mathbf{1101}_2 P$$

ADD, since  $d_1 = 1$

$$\#4a \quad 13P + 13P = 26P = 2(1101_2 P) = \mathbf{11010}_2 P$$

DOUBLE, bit processed:  $d_0$

$$\#4b$$

no ADD, since  $d_0 = 0$

## 9.3 Intercambio de llaves Diffie-Hellman (DHKE) con curvas elípticas

Parámetros dominio ECDH

1: Escoger un primo  $p$  y la curva elíptica

$$E: y^2 \equiv x^3 + a \cdot x + b \pmod{p}$$

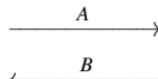
2: Escoger un elemento primitivo  $P = (x_p, y_p)$

Parámetros:  $\begin{cases} p \\ a, b \text{ (que determinan la curva } E\text{)} \\ P \end{cases}$

### Elliptic Curve Diffie-Hellman Key Exchange (ECDH)

Alice

choose  $k_{prA} = a \in \{2, 3, \dots, \#E - 1\}$   
compute  $k_{pubA} = aP = A = (x_A, y_A)$



compute  $aB = T_{AB}$

Bob

choose  $k_{prB} = b \in \{2, 3, \dots, \#E - 1\}$   
compute  $k_{pubB} = bP = B = (x_B, y_B)$

compute  $bA = T_{AB}$

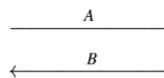
## ¿Porqué funciona?

Alice calcula  $aB = a(bP)$   
Bob calcula  $bA = b(aP)$

) = por asociatividad y commutatividad  
de la suma ✓

Ejemplo:

Alice  
choose  $a = k_{pr,A} = 3$   
 $A = k_{pub,A} = 3P = (10, 6)$



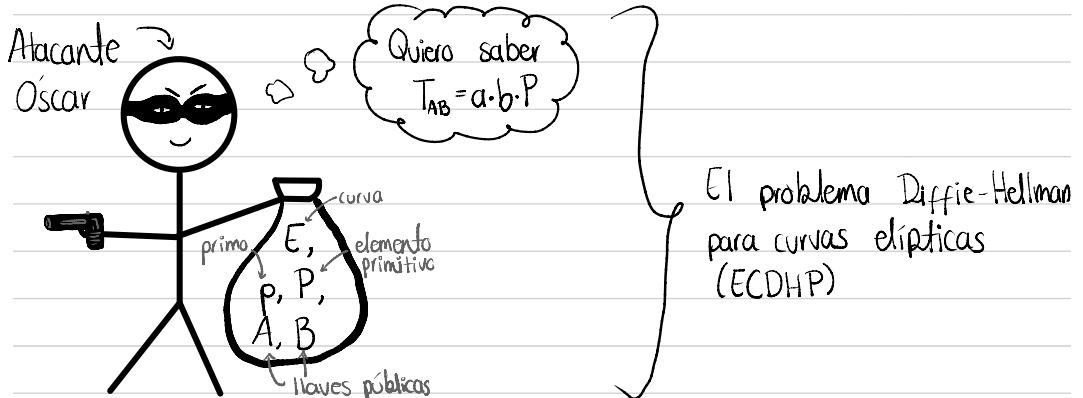
$$T_{AB} = aB = 3(7, 11) = (13, 10)$$

Bob  
choose  $b = k_{pr,B} = 10$   
 $B = k_{pub,B} = 10P = (7, 11)$

$$T_{AB} = bA = 10(10, 6) = (13, 10)$$

## 9.4 Seguridad

- Buenas propiedades de una dirección



⇒ necesita resolver alguno de los problemas de logaritmo discreto  
 $a = \log_p A$  ó  $b = \log_p B$

Si la curva elíptica se elige con cuidado, entonces los mejores ataques conocidos contra ECDLP son considerablemente más débiles que los mejores algoritmos para resolver el problema DL módulo  $p$  y los mejores algoritmos de factorización para ataques contra RSA.

La seguridad se logra sólo si se usan curvas elípticas criptográficamente fuertes.