Criptografia de Curvas Elípticas

Ezequiel S. Dos Santos

Origem

- Criptografia de chave pública
  - Base: estrutura algébrica de curvas elípticas sobre corpos finitos.
- Sugerida por Neal Koblitz e Victor S.Miller em 1985

O que são curvas elípticas?

$$E = \{(x, y) | y^2 = x^3 + ax + b\}$$

$$a, b \in F_p$$

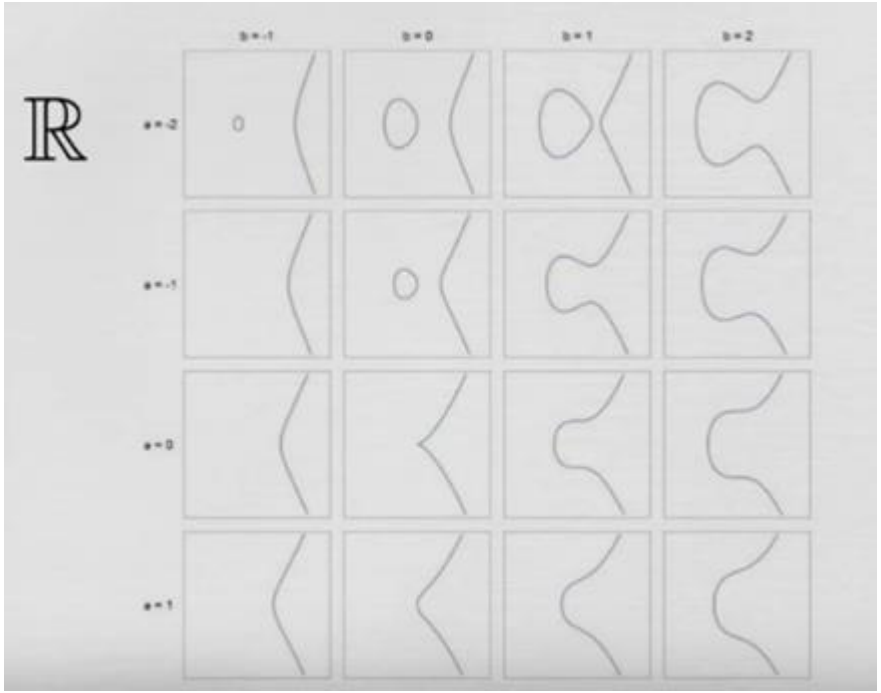
$F_p \Rightarrow$ Conjunto de inteiros módulo p (entre 0 e p-1)

$4a^3 + 27b^2 \neq 0 \longrightarrow$ De forma simples, essa restrição é para evitar uma singularidade (mais informações, nas referências)

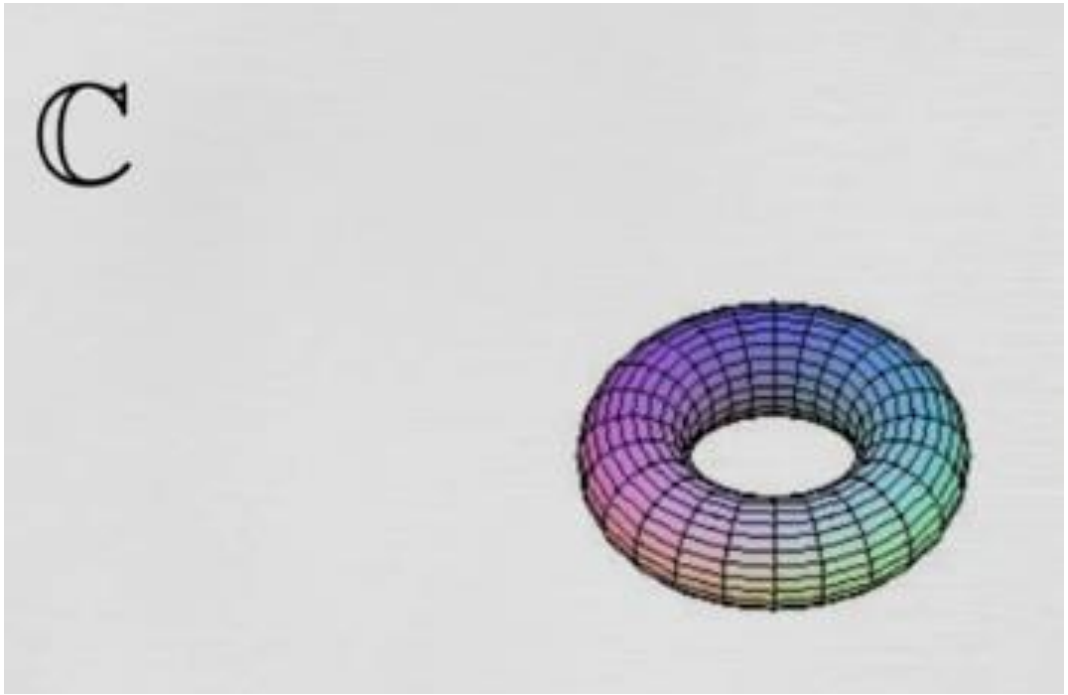
Ponto no infinito: O

$F : R, Q, C, Z/pZ$

Exemplos de Curvas Elípticas

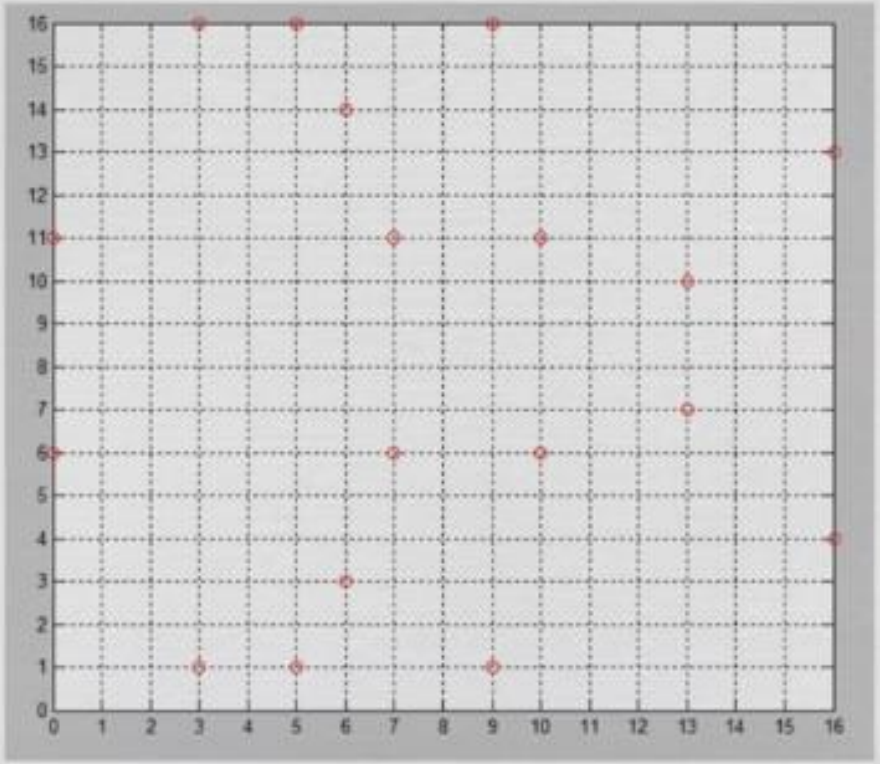


Exemplos de Curvas Elípticas



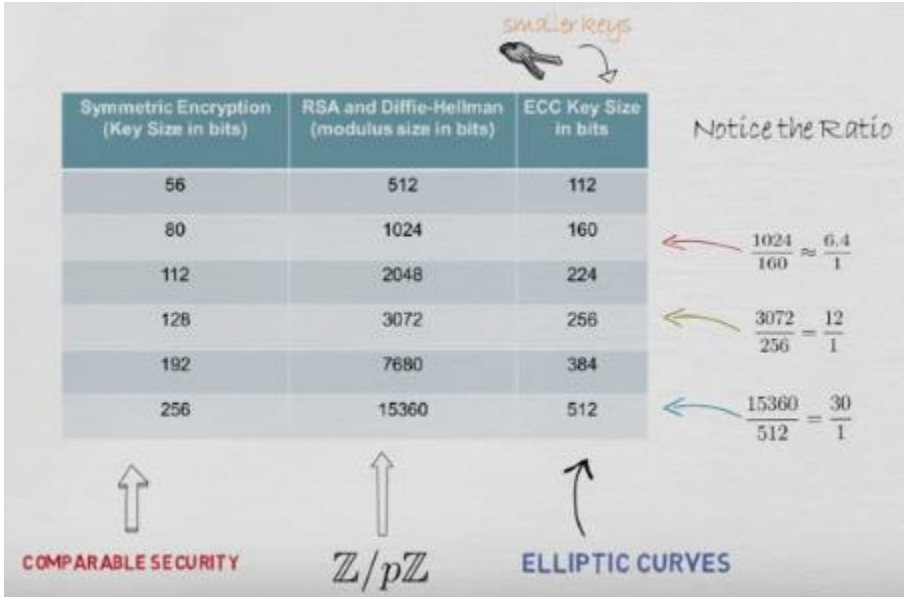
Exemplos de Curvas Elípticas

$\mathbb{Z}/17\mathbb{Z}$



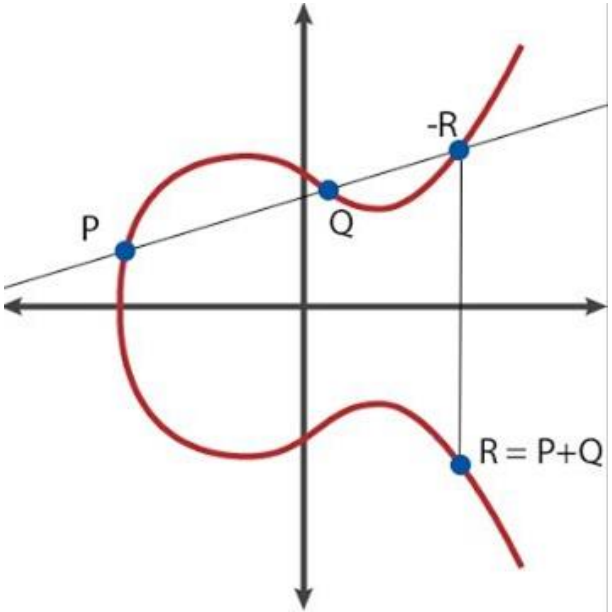
Por que utilizar CCE?

- As chaves de criptografia necessárias são menores do que as do RSA
  - Utiliza menos memória e recursos de CPU



Características

- Os pontos em uma curva elíptica dão forma a um grupo abeliano (E(Fp),+) com O o ponto distinto na infinidade.

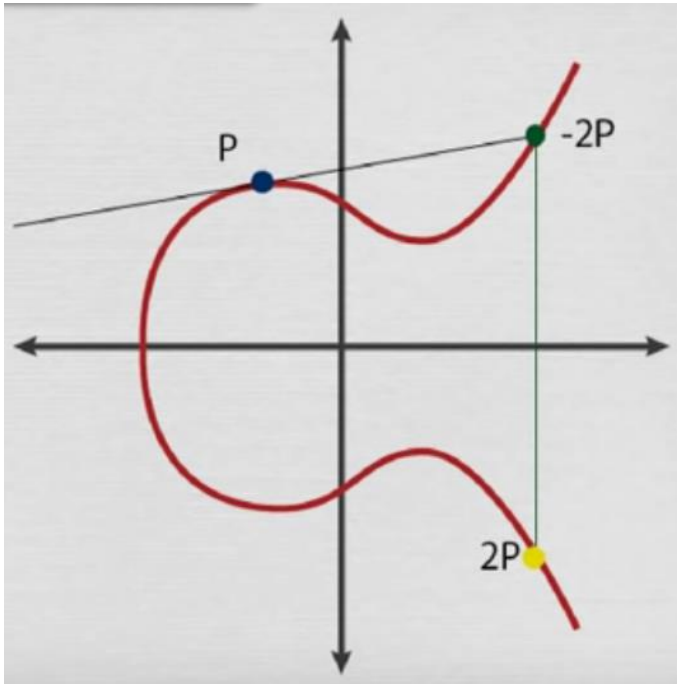


$$s = \frac{y_P - y_Q}{x_P - x_Q}$$

$$x_R = s^2 - (x_P + x_Q)$$

$$y_R = s(x_P - x_R) - y_P$$

Características

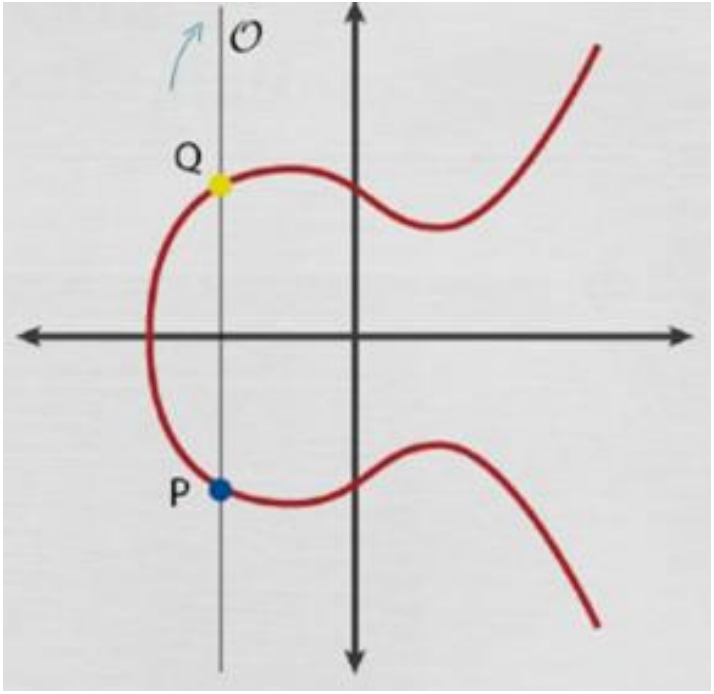


$$s = \frac{3x_P^2 + a}{2y_P}$$

$$x_R = s^2 - 2x_P$$

$$y_R = s(x_P - x_R) - y_P$$

Características



$$P + Q = O, \quad \text{se} \quad x_P = x_Q$$

$$P + P = O, \quad \text{se} \quad y_P = 0$$

Características

$$P \in E$$
$$k \in Z$$
$$Q = kP = P + P + \ldots + P$$

k vezes

Problema do Logaritmo Discreto da Curva Elíptica

- A multiplicação escalar é uma função unidirecional.
- Dados:

$$Q, P \in E(Z/pZ)$$

- Encontrar:

$$k, \text{ tal que } Q = kP$$

O Ponto Base (Gerador)

$$G \in E(Z/pZ)$$

$$ord(G) = n \qquad\qquad kG = O$$

$$h = \frac{|E(Z/pZ)|}{n}$$

Parâmetros do Domínio

$$\{p, a, b, G, n, h\}$$

p : campo (módulo p)

a, b : parâmetros da curva

G : Ponto Gerador

n : $ord(G)$

h : cofator

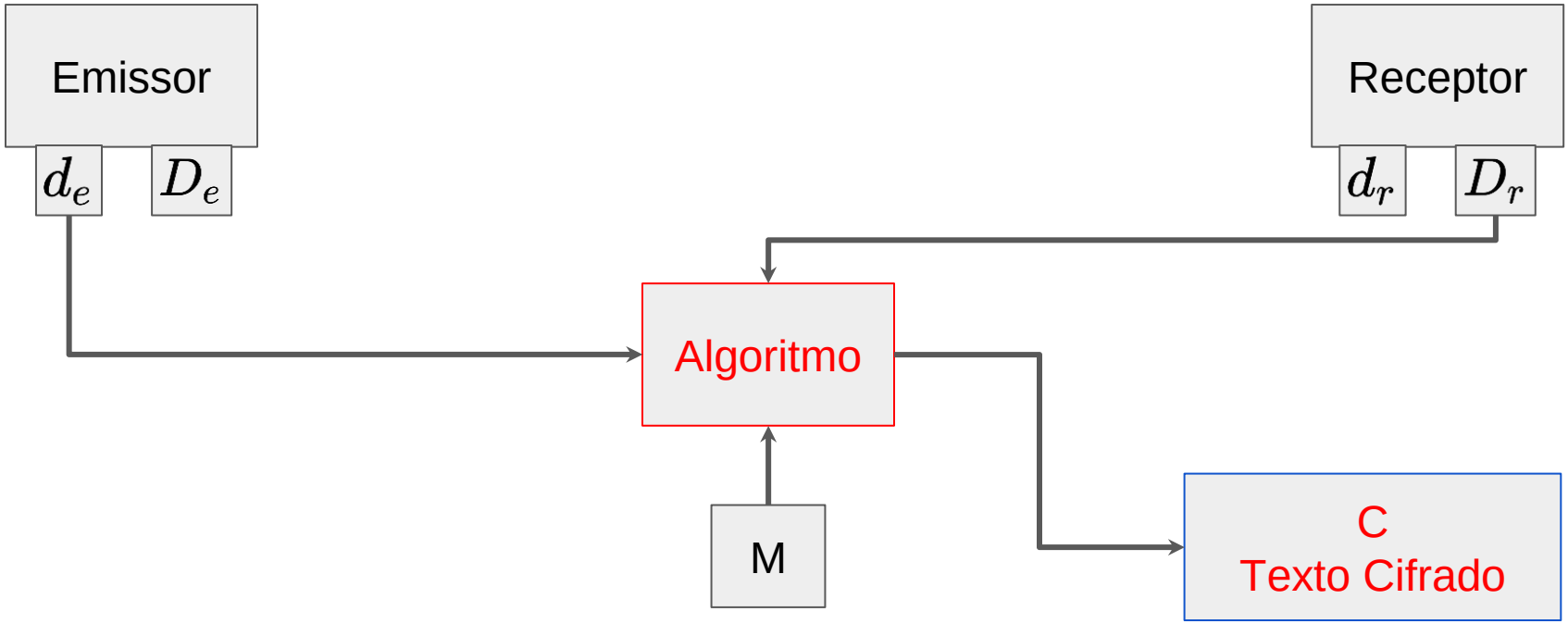
Chaves

- Chave privada: Escolhe-se um inteiro d tal que:
  $1 \leq d \leq n-1$
- Chave pública: $D = dG$

Criptografia e Descriptografia

$$C = M + d_e D_r$$
$$M = C - d_r D_e$$

Esquema da Criptografia CE



Referências:

- https://pt.wikipedia.org/wiki/Criptografia_de_curva_el%C3%ADptica
- https://www.youtube.com/watch?v=F3zzNa42-tQ&t=36s
- http://www.geometer.org/mathcircles/ecc.pdf
- https://www.researchgate.net/publication/229026452_Elliptic_Curve_Cryptography
- https://impa.br/wp-content/uploads/2017/04/30CBM_08.pdf
- https://www.sbm.org.br/docs/coloquios/CO-1-04.pdf