

Motivação

Tipo algoritmo	Segurança			
	80	128	192	256
RSA	1024 bits	3072 bits	7680 bits	15360 bits
Diffie-Hellman	1024 bits	3072 bits	7680 bits	15360 bits
Curvas elípticas	160 bits	256 bits	384 bits	512 bits

- ▶ Curvas elípticas são vulneráveis apenas aos ataques genéricos contra grupos

História e outros

- ▶ Inventado independentemente por N. Koblitz (1987) e V. Miller (1986)
- ▶ Não adotado inicialmente devido especulações sobre sua segurança
- ▶ Adoção a partir dos anos 2000 padrões bancários
- ▶ Problemas com patentes
- ▶ Mais em <http://eprint.iacr.org/2008/390.pdf>

Curva elíptica

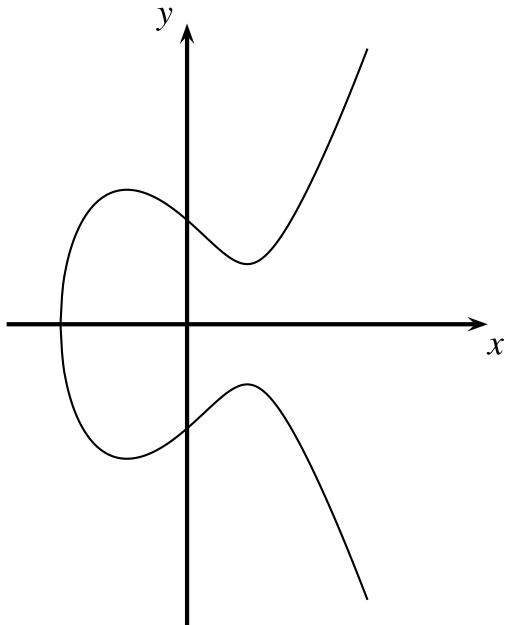
- ▶ Curva elíptica em \mathbb{Z}_p , $p > 3$ é o conjunto de pares $(x, y) \in \mathbb{Z}_p$ que atende

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

em conjunto com ponto “imaginário” do infinito \mathcal{O}

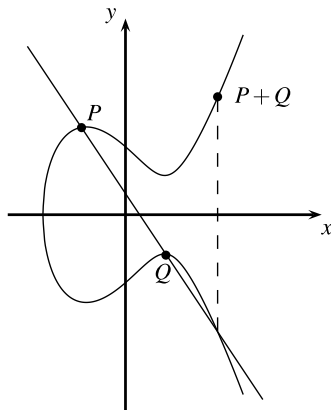
- ▶ onde $a, b \in \mathbb{Z}_p$ e vale que $4 \cdot a^3 + 27 \cdot b^2 \not\equiv 0 \pmod{p}$
- ▶ Operações são baseadas em um método de desenho chamado “tangente e corda”

Curva elíptica: $y^2 = x^3 - 3x + 3$



Operações de grupos em curvas elípticas

- ▶ Como fazer $(x_1, y_1) + (x_2, y_2) = R$?
 $P + Q = R$?
 - ▶ “desenhar reta passando por P e Q para pegar ponto de interseção com a curva elíptica: R vai ser esse ponto espelhado no eixo horizontal”

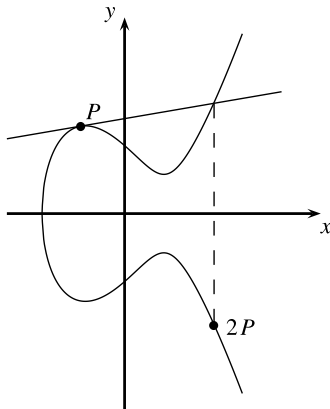


Operações de grupos em curvas elípticas

- ▶ Como fazer $(x_1, y_1) + (x_1, y_1) = R$?

$$P + P = R?$$

- ▶ “desenhar tangente a P para pegar ponto de interseção com a curva elíptica: $2P$ vai ser esse ponto espelhando no eixo horizontal”



Soma e duplicação de pontos em uma curva elíptica

- ▶ $x_3 \equiv s^2 - x_1 - x_2 \pmod{p}$
- ▶ $y_3 \equiv s(x_1 - x_3) - y_1 \pmod{p}$ onde
- ▶ se $P \neq Q$, $s = \frac{y_2 - y_1}{x_2 - x_1} \pmod{p}$ (soma)
- ▶ se $P = Q$, $s = \frac{3x_1^2 + a}{2y_1} \pmod{p}$ (duplica)
 - ▶ observe que s equivale à tangente da curva elíptica

Elemento neutro da curva elíptica

- Imagine um ponto \mathcal{O} no infinito positivo do eixo vertical, então

$$A + \mathcal{O} = A$$

- E também $A + (-A) = \mathcal{O}$ onde $-A = (x_A, p - y_A)$,
 $-y_A = p - y_A$

Exemplo

- ▶ Testar com $y^2 \equiv x^3 + 2x + 2 \pmod{17}$
- ▶ Se $P = (5, 1)$, quanto é $2P$ e $P + (2, 1)$?
- ▶ Qual é o x tal que $P = xP$?
- ▶ Qual é o Q tal que $P + Q = \mathcal{O}$

A ordem do grupo definido pela curva elíptica

- ▶ Limite de Hasse

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

- ▶ sendo $\#E$ o número estimado de elementos do grupo

Problema do logaritmo discreto em curvas elípticas

- ▶ Em uma curva elíptica E , um ponto primitivo P e outro elemento T o problema do logaritmo discreto é encontrar o inteiro $1 \leq d \leq \#E$ tal que

$$P + P + \dots + P = dP = T$$

Problema do logaritmo discreto: exercícios

- ▶ Sendo $y^2 \equiv x^3 + 2x + 2 \pmod{17}$:
 - ▶ computar d tal que $dP = (16, 4)$ com $P = (5, 1)$ (computacional).
 - ▶ verificar se $d = 13$ é solução para $d(6, 2) = (3, 5)$ (decisional)

Algoritmo “duplicar e somar” para multiplicação de pontos

Algorithm 1 “Duplicar e somar” para multiplicar pontos elípticos

Require: curva elíptica E , um ponto na curva P , um escalar $d = \sum_{i=0}^t d_i 2^i$ com $d_i \in \{0, 1\}$ e $d_t = 1$

Ensure: $T = dP$

- 1: Inicializar $T \leftarrow P$
 - 2: **for** $i \leftarrow t - 1 \dots 0$ **do**
 - 3: $T \leftarrow T + T \bmod n$
 - 4: **if** $d_i = 1$ **then**
 - 5: $T \leftarrow T + P \bmod n$
 - 6: **end if**
 - 7: **end for**
 - 8: **return** T
-

Exercício

- ▶ Usar “duplicar e somar” em
 $26P = (11010_2)P = (d_4d_3d_2d_1d_0)P$

Troca de chaves de Diffie-Hellman com Curvas Elípticas (ECDHKE)

- ▶ Passo 1: escolher primo p e curva $E : y^2 \equiv x^3 + a \cdot x + b \pmod{p}$
- ▶ Passo 2: escolher um elemento primitivo $P = (x_P, y_P)$
 - ▶ Parâmetros públicos: p, a, b, x_P, y_P
- ▶ Alice:
 - ▶ Escolher $a \in \{2, 3, \dots, \#E - 1\}$
 - ▶ Computar e enviar $A = aP$
- ▶ Bob:
 - ▶ Escolher $b \in \{2, 3, \dots, \#E - 1\}$
 - ▶ Computar e enviar $B = bP$
- ▶ Chave secreta: $aB = bA$ pois $a(bP) = b(aP)$
- ▶ Como y depende de x , usar somente x para obter chave AES

Questões práticas

- ▶ Possível usar $GF(2^m)$
- ▶ Segurança depende dos parâmetros da curva elíptica
- ▶ Díficil escolher bons parâmetros...
 - ▶ ... para garantir que está usando um subgrupo cíclico grande
- ▶ Padrões
 - ▶ Certicom - <http://www.secg.org/sec2-v2.pdf>
 - ▶ NIST - <http://csrc.nist.gov/groups/ST/toolkit/documents/dss/NISTReCur.pdf>
- ▶ É possível confiar nos padrões?
 - ▶ <http://crypto.stackexchange.com/questions/10263/should-we-trust-the-nist-recommended-ecc-parameters>
- ▶ Existem diversas variantes de curvas elípticas