Elliptische Kurven

Koblitz:

Vorschlag ECC = elliptic curve crypto

Angriffe:

- Pollard-ρ, Pollard-λ $\Rightarrow$ exponentiell
- Spezialfälle: polynomiell
  subexponentiell

$\rightarrow$ 256 Bits Schlüssellänge

$\longrightarrow$ ECC hat

- weniger Platzverbrauch
- weniger CPU-Belastung

1990

subexp.

RSA, DSA

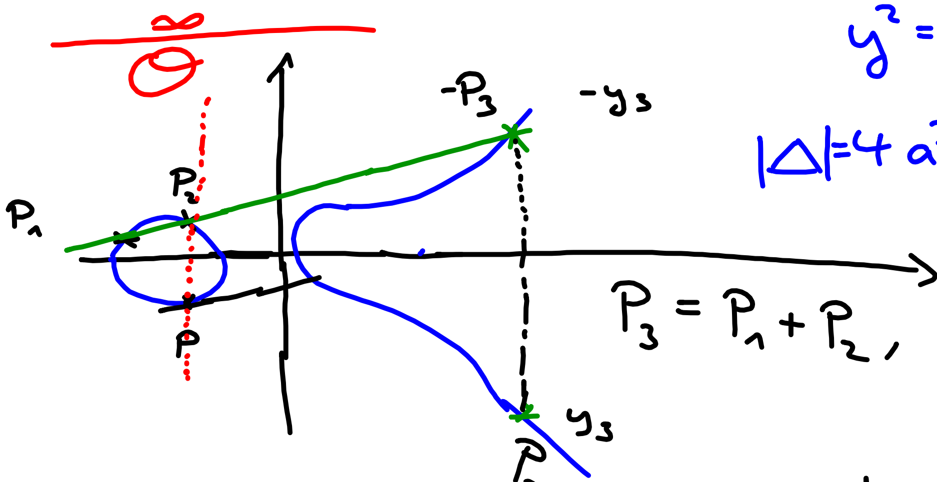
$\boxed{\text{512-Bit}}$

Weltrekorde

Faktorisieren + DL

429 Bits

Algorithmische Fragestellungen



$y^2 = x^3 + ax + b$

$|\Delta| = 4a^3 + 27b^2 \neq 0$

$P_3 = P_1 + P_2$, $(E,+)$ Gruppe

Berechnung der Koordinaten von P_3

- Steigung der Geraden

$$m = \frac{y_2 - y_1}{x_2 - x_1} \quad \text{bzw.} \quad m = \frac{3x^2 + a}{2y}$$

$P_1 \neq P_2$ $\qquad$ $P_1 = P_2$ $\qquad$ 3

$y(x)^2 = x^3 + ax + b$

$2 \cdot y \cdot y' = 3x^2 + a$

$\Rightarrow y' = \dfrac{3x^2 + a}{2 \cdot y}$

- $x_3 = m^2 - x_1 - x_2$, $\quad y_3 = m \cdot (x_1 - x_3) - y_1$ $\quad$ 4

$-y_3 = m \cdot x_3 + d$

$y_1 = m \cdot x_1 + d$

$-y_3 = m \cdot (x_3 - x_1) + y_1$

$\Rightarrow y_3 = m(x_1 - x_3) - y_1$

$P_3 = (x_3, y_3)$

- $P + \mathcal{O} = P$ $\quad$ 1
- $P + (-P) = \mathcal{O}$, hierbei $-P = (x, -y)$ $\quad$ 2

Algorithmen ECC

1. Arithmetik der Punktaddition
2. Anzahl der Punkte bestimmen
   (Ausprobieren: p Schritte → exponentiell, Schoof-Elkies-Atkin $\log^6(p)$)
3. Punkte bestimmen
   a) Kurve + Punkt bestimmen
      x, y, a wählen → b ausrechnen
   b) Kurve fest
      x wählen + y ausrechnen
      → Quadratwurzeln mod p sind nötig

$$y^2 \equiv x^3 + ax + b \mod p$$

$$E = \{(x,y) \mid y^2 \equiv x^3 + ax + b \mod p\} \cup \{\mathcal{O}\}$$

Beispiel:

$y^2 \equiv x^3 + x + 4 \mod 7$

x	0	1	2	3	4	5	6
y^2	4	6	0	6	2	1	2
y	2, 5	—	0	—	3, 4	1, 6	3, 4

y	y^2
0	0
1	1
2	4
3	2
4	2
5	4
6	1

$\Rightarrow E = \{(0,2), (0,5), (0,0), \ldots, (6,3), (6,4), \mathcal{O}\}$

$|E| = 10$

Punktaddition:

1. $(4,3) + (4,4) = \mathcal{O}$

$(x,y) + (x,-y) = \mathcal{O}$

2. $(4,3) + (5,6) = ?$

$$m \equiv \frac{y_2 - y_1}{x_2 - x_1} \mod 7$$

$$\equiv \frac{6-3}{5-4} \equiv \frac{3}{1} \equiv 3 \mod 7$$

$$x_3 \equiv m^2 - x_1 - x_2 \equiv 3^2 - 4 - 5 \equiv 2 - 4 - 5 \equiv -7 \equiv 0 \mod 7$$

$$y_3 \equiv m \cdot (x_1 - x_3) - y_1 \equiv 3 \cdot (4 - 0) - 3 \equiv 2 \mod 7$$

$\Rightarrow P_3 = (0,2)$

3. $(4,3) + (4,3) = ?$

$$m \equiv \frac{3 \cdot x^2 + a}{2 \cdot y} \equiv \frac{3 \cdot 4^2 + 1}{2 \cdot 3} \equiv \frac{49}{6} \equiv \frac{0}{-1} \equiv 0 \mod 7$$

$$x_3 \equiv m^2 - x_1 - x_2 \equiv 0^2 - 4 - 4 \equiv 6 \mod 7$$

$$y_3 \equiv m \cdot (x_1 - x_3) - y_1 \mod p$$

$$\equiv 0 \cdot (4 - 6) - 3 \equiv 4 \mod 7$$

$\Rightarrow P_3 = (6,4)$