Public Key — RSA / DSA — subexponentiell

> 2048 Bit Schlüssellänge

Symmetrische Verfahren — AES, Twofish, ... — exponentiell

> 128 Bit

Elliptische Kurven

1989/90 Anwendung in Kryptographie

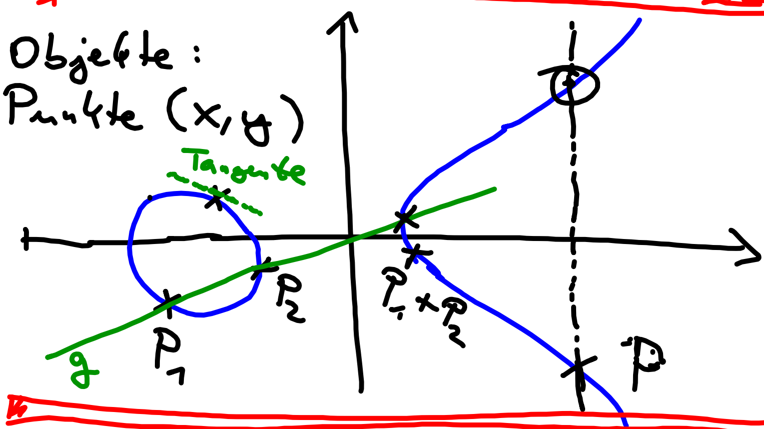
wenige Spezialfälle: polynomiell, subexponentiell

ansonsten nur exponentielle Angriffe ⇝ 256 Bit

Kurvengleichung: $E: y^2 = x^3 + \underbrace{ax + b}_{\text{Parameter}} \cup \{\mathcal{O}\}$

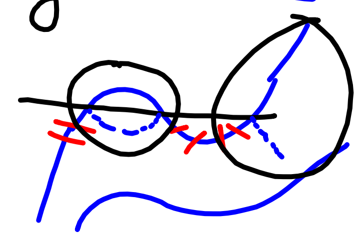
Bsp.: $y^2 = x^3 + x + 1$ (*)

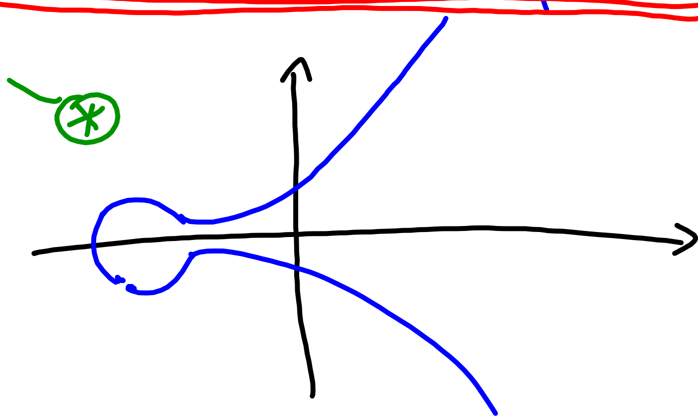
Objekte:
Punkte (x,y)



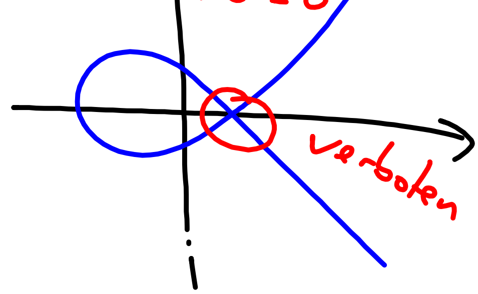
Skizze

$y = \sqrt{x^3 + x + 1}$





$4a^3 + 27b^2 = 0$



$$\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} + \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} = \begin{pmatrix} x_1 + x_2 \\ y_1 + y_2 \end{pmatrix}$$

Vektoraddition funktioniert nicht

(liegt außerhalb der Kurve)

Richtige Methode: Gerade durch P_1, P_2

Schnittpunkt mit E

Spiegelung an x-Achse

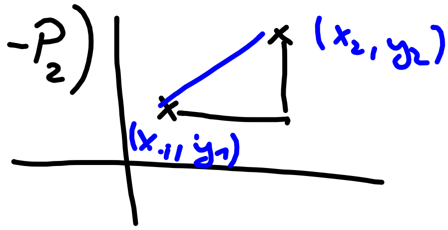
$$(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3) \qquad P_1 + P_2 = P_2 + P_1$$

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

Punktaddition:

$$P_1 = (x_1, y_1), \quad P_2 = (x_2, y_2)$$

Steigung m der Geraden $g(x) = mx + d$ durch P_1 und P_2, $(P_1 \neq P_2,\ P_1 \neq -P_2)$



$$m = \frac{y_2 - y_1}{x_2 - x_1}, \quad x_1 \neq x_2$$

und falls $P_1 = P_2$, Steigung der Tangente

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

$$y(x)^2 = x^3 + ax + b \quad \| \text{ Ableitung}$$

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

$$y'(x) = \frac{3x^2 + a}{2y(x)}$$

$$m = \frac{3x^2 + a}{2y}$$ ist die gesuchte Steigung

$g(x) = mx + d$ wird vom Punkt (x, y) erfüllt

$$\Rightarrow \quad mx + d = y \Rightarrow d = y - mx$$

Falls

$$(x_1, y_1) = (x_2, -y_2)$$

dann wäre die Gerade senkrecht

$$\Rightarrow P_1 + P_2 = \mathcal{O} \quad \text{bzw} \quad P_1 = -P_2$$

Falls $P_1 \neq P_2 \wedge P_1 \neq -P_2$ muss der Schnittpunkt mit E berechnet werden:

$$g(x) = mx + d \quad , \quad y^2 = x^3 + ax + b$$

$$y = mx + d$$

$$(mx+d)^2 = x^3 + ax + b$$

$$m^2x^2 + 2mdx + d^2 = x^3 + ax + b$$

$$x^3 - m^2x^2 + (a - 2md)x + b - d^2 = 0$$

$$(x - x_1) \cdot (x - x_2) \cdot (x - x_3) = 0$$

$$x^3 + (-x_1 - x_2 - x_3)x^2 + (x_1x_2 + x_1x_3 + x_2x_3)x - x_1x_2x_3 = 0$$

$$\Rightarrow +x_1 + x_2 + x_3 = +m^2$$

$$\Rightarrow x_3 = m^2 - x_1 - x_2 \quad , \quad y_3 = -(mx_3 + d)$$

Kryptographie:

diese Rechenregeln gelten auch mod p, p Primzahl

Additionsalgorithmus:

Input: $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ bzw $\mathcal{O}$

Output: $P_3 = (x_3, y_3)$ oder $\mathcal{O}$

if $P_1 = \mathcal{O}$ then return P_2
fi
if $P_2 = \mathcal{O}$ then return P_1
fi
if $P_1 = -P_2$ $[(x_1, y_1) = (x_2, -y_2)]$
then return $\mathcal{O}$
fi
if $P_1 = P_2$ // Tangente
then $m \equiv (3x_1^2 + a)/2y_1 \mod p$
else $m \equiv (y_2 - y_1)/(x_2 - x_1) \mod p$
fi

$x_3 \equiv m^2 - x_1 - x_2 \mod p$

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

return (x_3, y_3)

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

Übung:

$$y^2 \equiv x^3 + x + 1 \mod 7$$

teste auf gültige elliptische Kurve $[4a^3 + 27b^2]$

$P_1 = (0, 1)$

$P_2 = (2, 2)$

Berechne $P_1 + P_1$

$P_1 + P_2$

$P_1 + (-P_1)$