Elliptische Kurven in der Kryptographie

Sandro Schugk und Günther Nieß

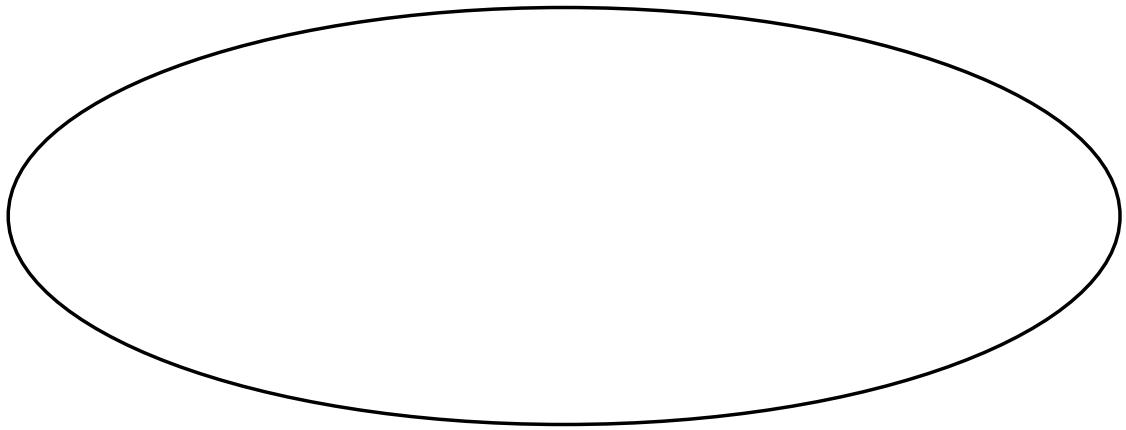
25. Januar 2007

Inhalt

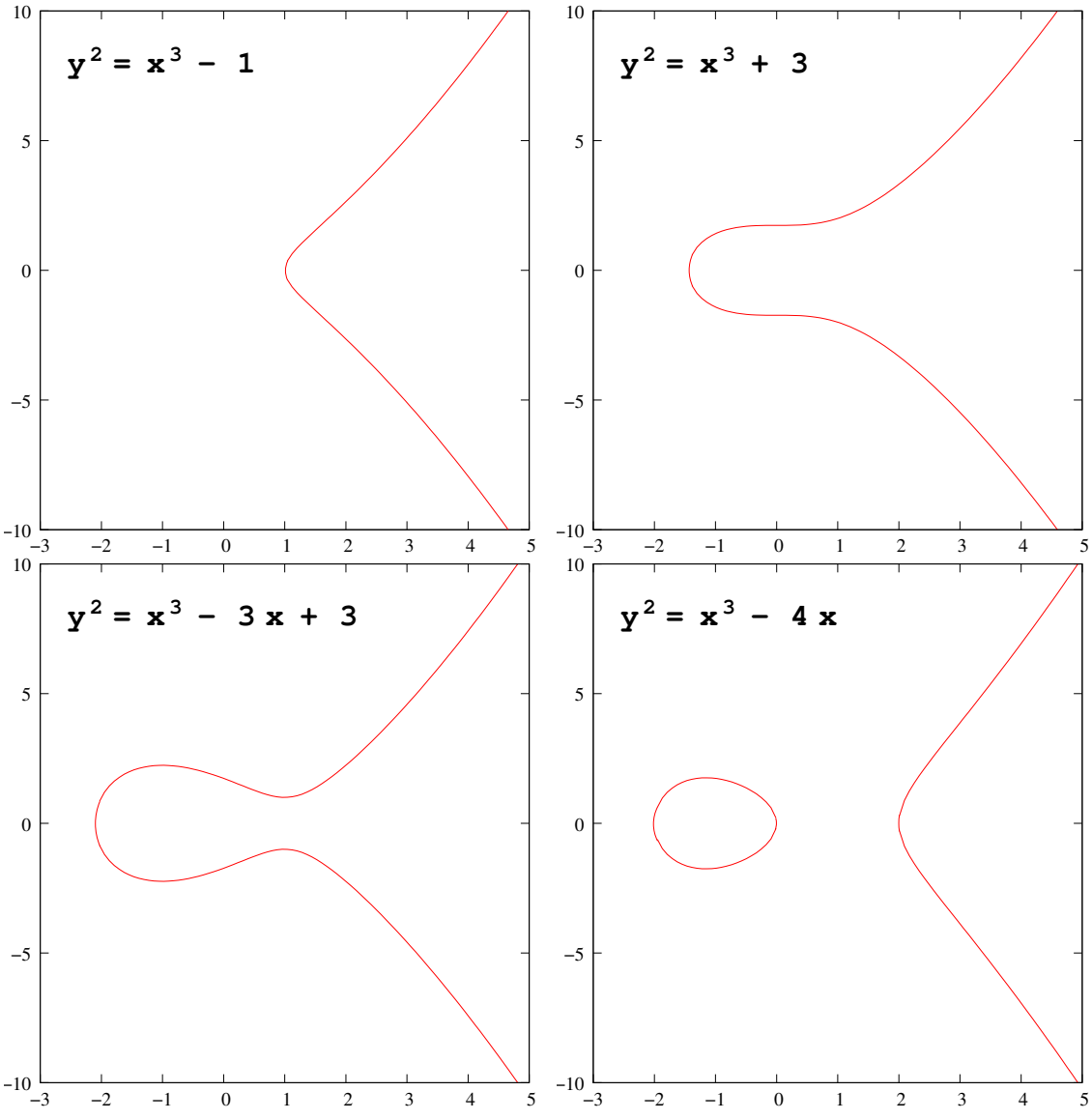
Motivation

- asymmetrisches Verfahren
- 1985 von Neal Koblitz und Victor S. Miller zeitgleich entwickelt
- sicherer und schneller
- darauf aufbauende Krypto-Systeme:
  - hyperelliptisch
  - Torus basierend

Elliptische Kurven über $\mathbb{R}$



Elliptische Kurven über $\mathbb{R}$



Elliptische Kurven über $\mathbb{R}$

Definition

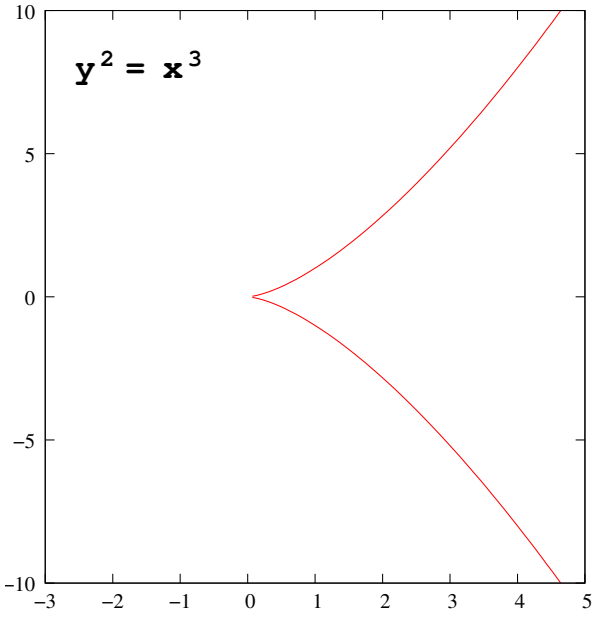
Seien $a, b \in \mathbb{R}$ Konstanten, so dass $4a^3 + 27b^2 \neq 0$ gilt. Eine nicht-singuläre elliptische Kurve ist die Lösungsmenge $(x, y) \in \mathbb{R}^2$ der Gleichung

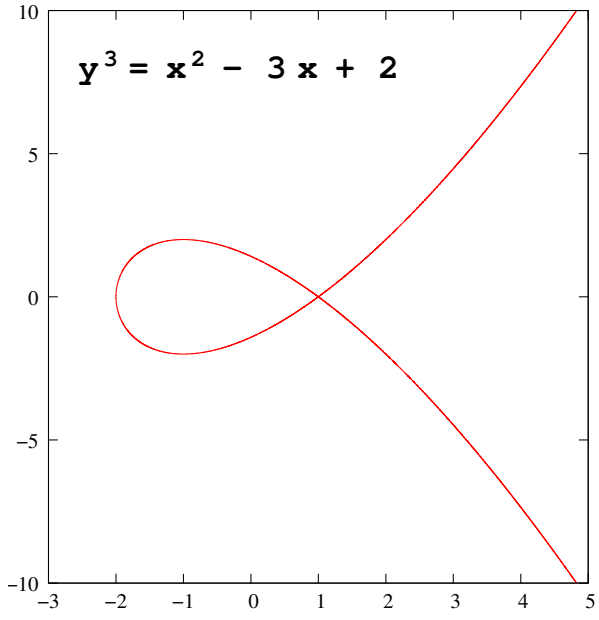
$$y^2 = x^3 + ax + b$$

zusammen mit dem Punkt im Unendlichen O.

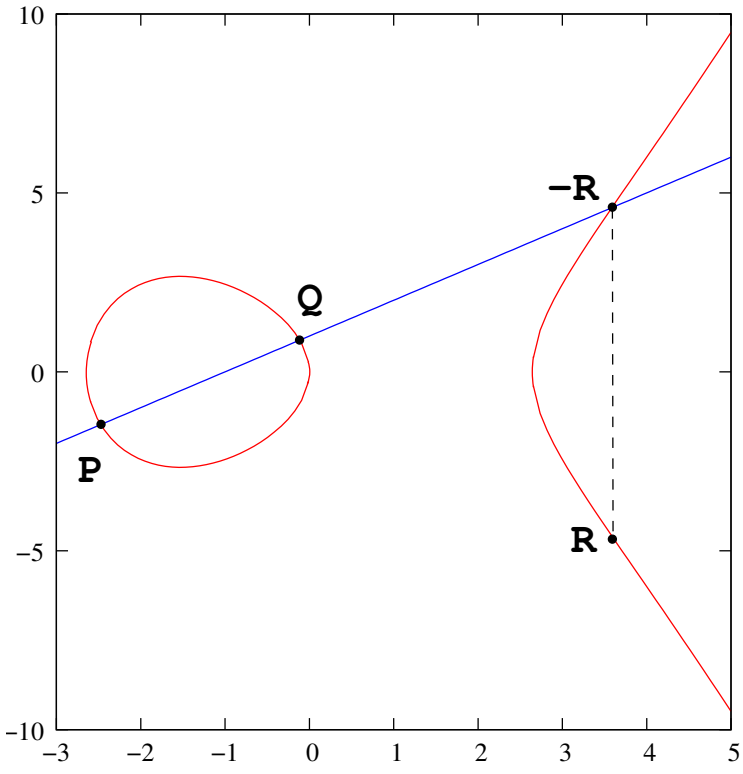
Elliptische Kurven über $\mathbb{R}$

Beispiele für singuläre elliptische Kurven





Addition



$$
\begin{aligned}
P &\quad (2.35, -1.86) \\
Q &\quad (-0.1, 0.836) \\
-R &\quad (3.89, 5.62) \\
R &\quad (3.89, -5.62)
\end{aligned}
$$

Addition

$P + Q = R$ mit $P = (x_1, y_1)$, $Q = (x_2, y_2)$ und $R = (x_3, y_3)$

- Gerade g aus Punkten P und Q bestimmen

$$g(x) = mx + n, \; m = \frac{y_2 - y_1}{x_2 - x_1}, \; n = y_1 - mx_1$$

- in Kurvengleichung einsetzen und lösen

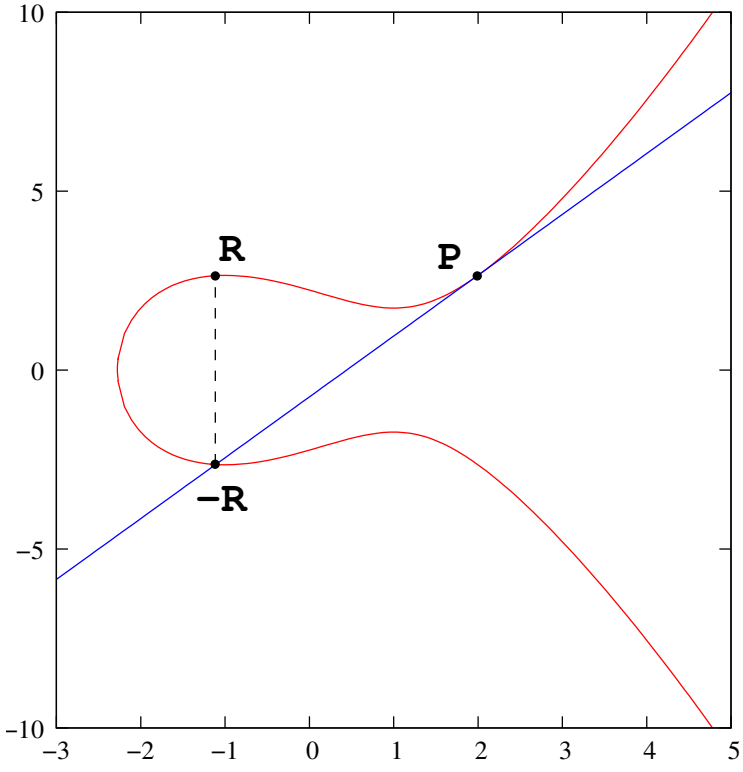
$$x^3 - m^2x^2 + (a - 2mn)x + b - n^2 = 0$$

$$x_3 = m^2 - x_1 - x_2$$

- Punkt R bestimmen

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

Verdoppeln



$$\begin{array}{rc} P & (2, 2.65) \\ -R & (-1.11, -2.64) \\ R & (-1.11, 2.64) \end{array}$$

Verdoppeln

$P + P = 2P = R$ mit $P = (x_1, y_1)$, $R = (x_3, y_3)$ und $y_1 \neq 0$

- Tangentengleichung finden

$$2y\frac{dy}{dx} = 3x^2 + a$$

$$m = \frac{3x_1^2 + a}{2y_1}$$

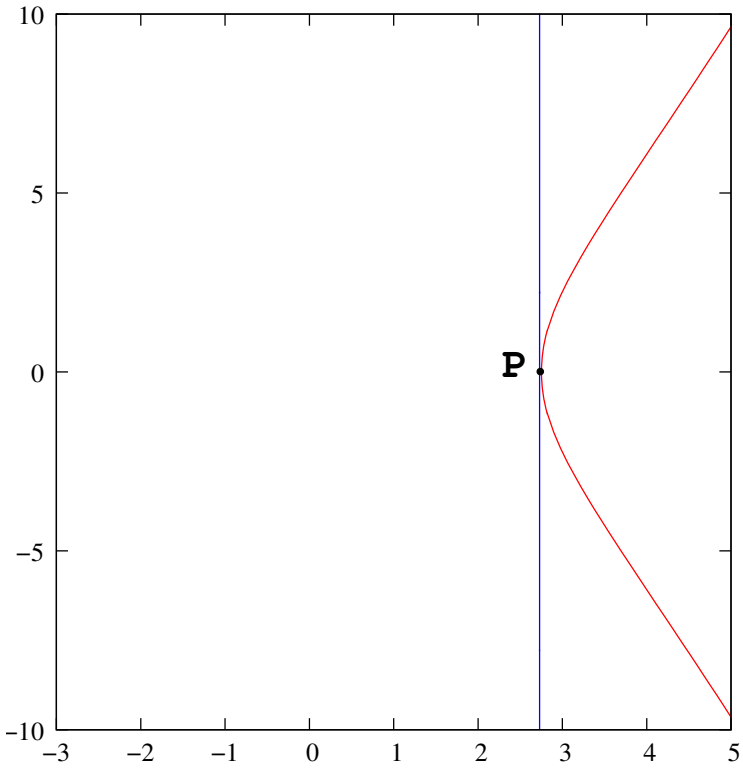
- Punkt R bestimmen

$$x_3 = m^2 - x_1 - x_2$$

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

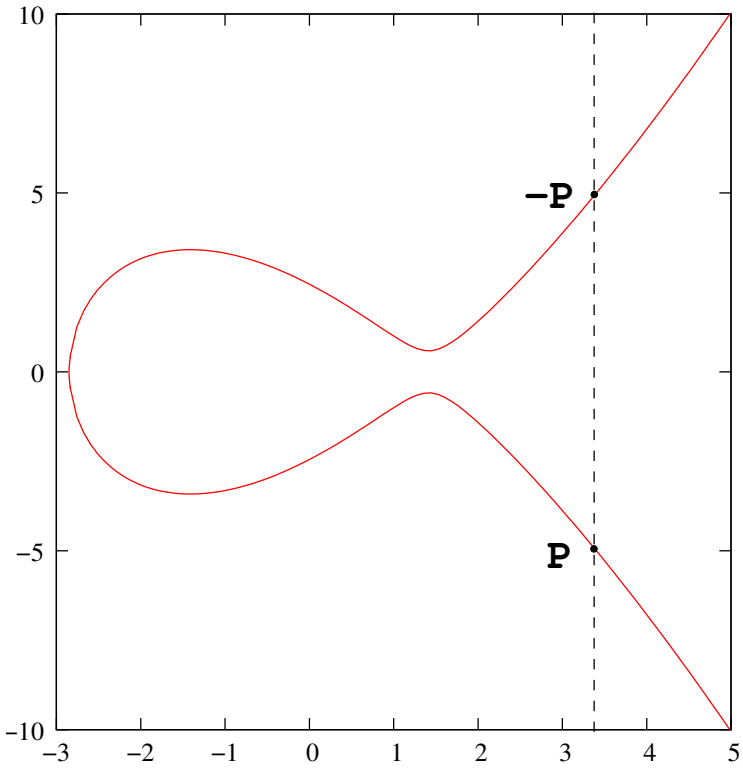
Verdoppeln

$P + P = 2P = O$ mit $P = (x_1, 0)$



$P \quad (2.81, 0)$

Inverses



$$P + (-P) = O$$

Gruppengesetze

- Abgeschlossenheit

$$P + Q = R$$

- Assoziativität

$$(P + Q) + R = P + (Q + R)$$

- neutrales Element

$$P + O = P$$

- inverses Element

$$P + (-P) = O$$

- Kommutativität*

$$P + Q = Q + P$$

Elliptische Kurven über $\mathbb{Z}_p$

Definition

Sei $p > 3$ ein Primzahl. Die elliptische Kurve $y^2 = x^3 + ax + b$ über $\mathbb{Z}_p$ ist die Menge alle Lösungen $(x, y) \in \mathbb{Z}_p^2$ zur Kongruenz

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

zusammen mit dem Punkt im Unendlichen O. Dabei sind $a, b \in \mathbb{Z}_p$ Konstanten, so dass $4a^3 + 27b^2 \not\equiv 0 \ (mod \ p)$ gilt.

Gruppenoperation

$P + Q = R$ mit $P = (x_1, y_1)$, $Q = (x_2, y_2)$ und $R = (x_3, y_3)$

$$\begin{aligned} x_3 &= m^2 - x_1 - x_2 \\ y_3 &= m(x_1 - x_3) - y_1 \\ m &= \begin{cases} (y_2 - y_1)(x_2 - x_1)^{-1}, & P \neq Q \\ (3x_1^2 + a)(2y_1)^{-1}, & P = Q \end{cases} \end{aligned}$$

Sonderfall $y_2 = -y_1$

$$P + Q = O$$

Beispiel

$$y^2 = x^3 + x + 6 \text{ über } \mathbb{Z}_{11}$$

x	$x^3 + x + 6 \ (mod\ 11)$	quad. Rest	y
0	6	no	
1	8	no	
2	5	yes	4,7
3	3	yes	5,6
4	8	no	
5	4	yes	2,9
6	8	no	
7	4	yes	2,9
8	9	yes	3,8
9	7	no	
10	4	yes	2,9

Beispiel: ElGamal-Verschlüsselung

$$
\begin{aligned}
\alpha &= (2,7)\\
2\alpha &= (5,2)\\
3\alpha &= (8,3)\\
4\alpha &= (10,2)\\
5\alpha &= (3,6)\\
6\alpha &= (7,9)\\
7\alpha &= (7,2)\\
8\alpha &= (3,5)\\
9\alpha &= (10,9)\\
10\alpha &= (8,8)\\
11\alpha &= (5,9)\\
12\alpha &= (2,4)
\end{aligned}
$$

- $a = 1$, $b = 6$, $p = 11$
- Bob's Schlüssel
  - $\alpha = (2,7)$, $\beta = (7,2)$
  - $s = 7$ *(privat)*
- Alice: $x = (10,9)$, $k = 3$

$$
\begin{aligned}
y_1 &= 3(2,7)\\
&= (8,3)\\
y_2 &= (10,9) + 3(7,2)\\
&= (10,9) + (3,5)\\
&= (10,2)
\end{aligned}
$$

Beispiel: ElGamal-Entschlüsselung

$$
\begin{aligned}
\alpha &= (2,7)\\
2\alpha &= (5,2)\\
3\alpha &= (8,3)\\
4\alpha &= (10,2)\\
5\alpha &= (3,6)\\
6\alpha &= (7,9)\\
7\alpha &= (7,2)\\
8\alpha &= (3,5)\\
9\alpha &= (10,9)\\
10\alpha &= (8,8)\\
11\alpha &= (5,9)\\
12\alpha &= (2,4)
\end{aligned}
$$

- Bob empfängt:

$$
\begin{aligned}
y &= ((8,3),(10,2))\\
\\
x &= (10,2) - 7(8,3)\\
&= (10,2) - (3,5)\\
&= (10,2) + (3,6)\\
&= (10,9)
\end{aligned}
$$

Beispiel: Diffie-Hellman-Schlüsselvereinbarung

	Alice	Bob
einigen sich	$p = 149$ $a = 5, b = 6$ $G = (66, 34)$ $r = 71$ $\|E\| = 142$	
zufällig	$s_a = 18$	$s_b = 69$
öffentlich	$W_a = s_a \cdot G = (27, 56)$	$W_b = s_b \cdot G = (66, 115)$
tauschen	W_b	W_a
gemeinsames k	$k = s_a \cdot W_b = (27, 93)$	$k = s_b \cdot W_a = (27, 93)$

Parameter zusammengefasst

allgemein:

E	elliptische Kurve
a, b	Koeffizienten a und b
p	Größe zugrundeliegender Primzahlkörper $\mathbb{Z}_p$
G	Generatorpunkt auf der elliptischen Kurve
r	Ordnung des Punktes G, r muss prim sein

Schlüssel:

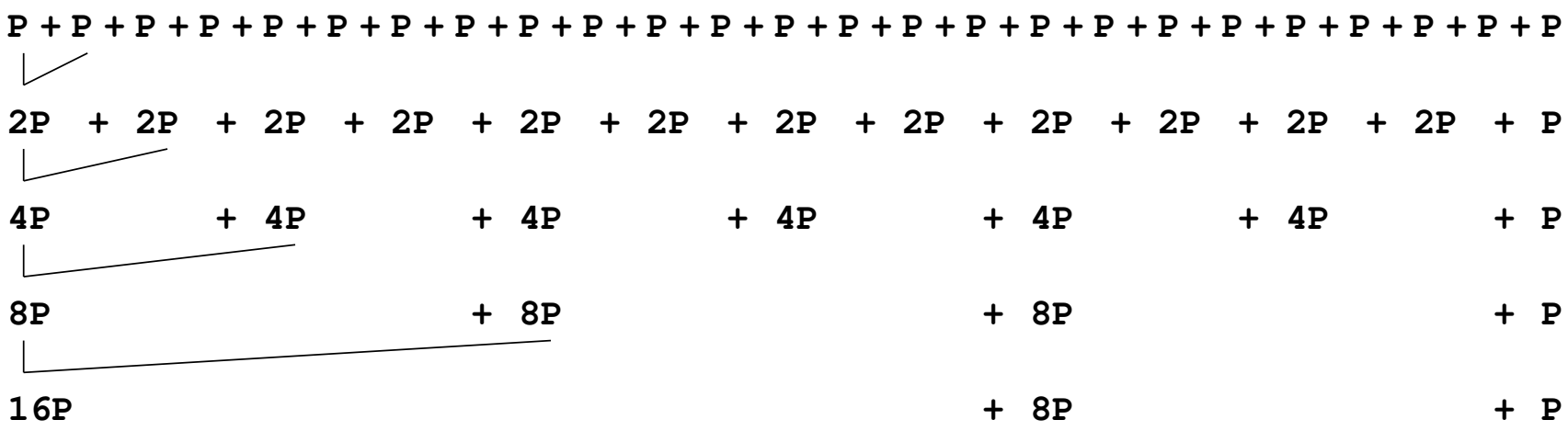
s	privat
W	öffentlich

erzeugt durch:

$$W = s \cdot G$$

Skalare Multiplikation von Punkten

Beispiel: $n = 25$



$$1 \cdot 16P + 1 \cdot 8P + 0 \cdot 4P + 0 \cdot 2P + 1 \cdot 1P = 25P$$

Skalare Multiplikation von Punkten

Für beliebiges n

- Binärdarstellung

$$\begin{aligned} n &= [b_z b_{z-1} \dots b_1 b_0] \\ \\ n \cdot P &= b_z \cdot [b_z 0 \dots 00]\, P \\ &+ b_{z-1} \cdot [0 b_{z-1} \dots 00]\, P \\ &+ \dots \\ &+ b_1 \cdot [00 \dots b_1 0]\, P \\ &+ b_0 \cdot [00 \dots 0 b_0]\, P \end{aligned}$$

- benötigte Operationen
  - z Additionen für $b_z \cdot [b_z 0 \dots 00]\, P$
  - z Additionen für den Rest
  - $2z$ Addition maximal für $n \approx 2^z$

Punktkompression

Problemstellung:

- Ein Punkt $P = (x, y)$ wird durch $2n$ Bits dargestellt
- Die öffentliche Parameter $(E_{ab}, q, G, sG) = (a, b, q, G, W)$ benötigen mehr als $6n$ Bits zur Repräsentation

Lösung:

- Punktkompression als Funktion

$$K : E \setminus \{0\} \to \mathbb{Z}_q \times \mathbb{Z}_2, \quad (x, y) \mapsto (x, y \mod 2)$$

- Für $E(\mathbb{Z}_p)$ mit $p > 3$ sind zwei elliptische Kurven isomorph, wenn gilt:

$$\exists u \in \mathbb{Z}_q \quad : \quad u \cdot \overline{a} = a \quad \text{und} \quad u^2 \cdot \overline{b} = b.$$

- Das Kryptosystem (a, b, q, G, W) benötigt ungefähr $3n$ Bits.

Homogene Weierstraß–Gleichung

Definition:

Sei K ein Körper und $F(X, Y, Z)$ ein homogenes Polynom der Form

$$\begin{aligned} F(X, Y, Z) &= Y^2Z + a_1XYZ + a_3YZ^2 \\ &\quad -X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3 \end{aligned}$$

mit $a_1, a_2, a_3, a_4, a_6 \in K$, dann bezeichnen wir die Gleichung

$$F(X, Y, Z) = 0$$

$$\iff Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

als homogene Weierstraß-Gleichung.

Singularität bei elliptischen Kurven

Definition:

Sei $F(X, Y, Z) = 0$ eine homogene Weierstraß–Gleichung über dem Körper K, dann heißt sie singulär, wenn an einem Punkt alle Ableitungen verschwinden.

Das heißt, wenn ein Punkt $P = (x, y, z) \in K^3$ existiert, bei dem gilt

$$\frac{\partial F}{\partial X}(x, y, z) = 0, \quad \frac{\partial F}{\partial Y}(x, y, z) = 0, \quad \frac{\partial F}{\partial Z}(x, y, z) = 0.$$

Punkt im Unendlichen:

Ist die Weierstraß-Gleichung nicht singulär, so folgt für $Z = 0$, daß die Lösungsmenge die Form $\overline{0} = (0, k, 0)$ für $k \in K$ hat. Diese Menge nennt man Punkt im Unendlichen.

Elliptische Kurve über K

Affine Weierstraß–Gleichung:

Eine Gleichung der Form

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

mit $a_1, a_2, a_3, a_4, a_6 \in K$, heißt affine Weierstraß–Gleichung.

Elliptische Kurve über dem Körper K:

Die Lösungsmenge $L(K) \subset K^2$ einer nicht singulären affinen Weierstraß–Gleichung bildet mit dem Punkt im Unendlichen eine elliptische Kurve:

$$E(K) = L(K) \cup \{\overline{0}\}$$

Äquivalenz der Definitionen

Elliptische Kurven über $\mathbb{Z}_{p^m}$ mit $p \neq 2$:

Die Funktion $\varphi : E(K) \to E(K)$ mit

$$(x, y) \mapsto \left(x, y - \frac{a_1}{2}x - \frac{a_3}{2}\right)$$

transformiert die affine Weierstraß–Gleichung in die Form

$$y^2 = x^3 + b_2x^2 + b_4x + b_6.$$

Elliptische Kurven über $\mathbb{Z}_{p^m}$ mit $p \neq 2, 3$:

Die Funktion $\psi : E(K) \to E(K)$ mit

$$(x, y) \mapsto \left(\frac{x - 3b_2}{2^2 \cdot 3^2}, \frac{y}{2^3 \cdot 3^3}\right)$$

transformiert die Gleichung von oben in die Form

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

Ordnung einer elliptischen Kurven

Satz von Hasse:

Sei E eine elliptische Kurve über $\mathbb{Z}_p$ (p Primzahl, $p > 3$) dann bezeichnet man als $\#E$ die Anzahl der Punkte auf E und es gilt:

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

Berechnung:

- Schoof-Algorithmus
  - Laufzeit von $O\left((\log p)^8\right)$.

Kryptoanalyse bei elliptischen Kurven

Klassische Verfahren:

- Brute-Force-Methode (Enumerationsverfahren)
- Babystep-Giantstep-Algorithmus
- Pollard-ρ-Methode
- Pollard-λ-Methode
- Pohling-Hellman-Verfahren

Spezielle Algorithmen:

- Supersinguläre Kurven (MOV-Algorithmus)
- Anomale Kurven (SSSA-Algorithmus)

$\Longrightarrow$ Index-Calculus-Algorithmus schlägt fehl

Parameter des Kryptosystems

Grundkörper:

- $\mathbb{Z}_p$ mit der Primzahl $p \in \mathbb{N}$
- $\mathbb{Z}_{2^m}$ mit der natürlichen Zahl $m \in \mathbb{N}$
- Härte des kryptographischen Systems
- Speicherbedarf

Elliptische Kurve:

- Parameter $a, b \in \mathbb{Z}_q$ bestimmen die elliptische Kurve.
- Generatorpunkt $G \in E(\mathbb{Z}_q)$

Schlüssel

- privater Schlüssel $s \in \mathbb{Z}_q$.
- öffentlicher Schlüssel $W = s \cdot G$.

Klassische Verfahren

- Brute Force:
  - privater Schlüssel s muß groß sein.
- Babystep-Giantstep-Methode:
  - Platzbedarf von $O(\sqrt{n})$
  - $n = ord(G) = min\{n \in \mathbb{N} : nG = 0\}$ muß groß sein.
- Pollard-ρ und Pollard-λ-Methode:
  - Laufzeit von $O(\sqrt{n})$
  - Algorithmus parallelisierbar
- Pohling-Hellman-Verfahren
  - Reduziert das Problem auf die Untergruppen von $< G >$
  - $n = ord(G)$ muß großen Primteiler haben.

MOV/Frey-Rück Methode

Algorithmus

Input: $P, Q \in E(\mathbb{Z}_q)$, der Ordnung r, so daß $Q = \lambda P$.

Output: Diskreter Logarithmus λ von Q zur Basis P.

1. Konstruiere einen Körper $\mathbb{Z}_{q^k}$, so daß $r|(q^k - 1)$.
2. Finde einen Punkt $S \in E(\mathbb{Z}_q)$, so daß $e(P, S) \neq 1$.
3. $\zeta_1 \leftarrow e(P, S)$.
4. $\zeta_2 \leftarrow e(Q, S)$.
5. Finde λ, so daß $\zeta_1^\lambda = \zeta_2$ in $\mathbb{Z}_{q^k}$.
6. Gebe λ aus.

Spezielle Methoden

- Menezes, Okamoto und Vanstone (MOV) Verfahren, bzw. Frey-Rück-Methode
  - Das ECDLP lässt sich auf DLP in $\mathbb{Z}_{q^k}$ zurückführen
  - $n \not| (q^k - 1)$ für alle $1 \leq k \leq \log(p)^2$
- Algebraisch-Geometrische Methode (Semaev/Rück)
- Zahlentheoretische Methode (Satoh/Araki/Smart)
  - $n = ord(G)$ darf nicht $p = char(\mathbb{Z}_q)$ teilen

Index Calculus Methode

- Verfügbar für $\mathbb{Z}_p$
- Benötigt eine Faktorbasis $\mathcal{B} = \{P_1, P_2, \ldots, P_B\}$
  - $B \in \mathbb{N}$ ist obere Schranke.
  - $P \in \mathcal{B}$ ist ein freier Erzeuger:

$$\forall x \in \mathbb{N} \ : \ xG = a_{1_x} P_1 + a_{2_x} P_2 + \cdots + a_{B_x} P_B$$

- Zwei Herangehensweisen:
  1. $(E, +)$ gehört zur Klasse der Gruppen über Funktionskörper
  2. Untersuchen der Gruppe $E(\mathbb{Q})$ und die Punkte in die Restklassen überführen $(x \ mod_q, y \ mod_q)$.
- Xedni Calculus Algorithmus von J. Silverman ist nicht praktisch anwendbar

Kryptographisch geeignete Kurven / Parameter

Zusammenfassung:

- Der private Schlüssel $s \in \mathbb{N}$ darf nicht klein sein.
- Die Anzahl der Punkte muß einen großen Primteiler haben.

$$\#E(Z_q) = \overline{n} \cdot d, \quad \overline{n} > 2^{160} \text{ ist Primzahl}$$

- $\#E(Z_q) = \overline{n} \cdot d, \quad \overline{n} \neq p$
- $q^k \not\equiv 1 \mod \overline{n}$ für $1 \leq k \leq \log(p)^2$
- Für $E(\mathbb{Z}_{p^m})$ mit $m > 1$ ist $a, b \notin \mathbb{Z}_p$
- Quantenrechner dürfen nicht verfügbar sein

Schlüssellänge ECC

Empfohlene Schlüssellänge der NIST:

Symm. Algorithmus	RSA und Diffie-Hellman	ECC	Faktor
80 Bits	1024 Bits	160 Bits	6
112 Bits	2048 Bits	224 Bits	9
128 Bits	3072 Bits	256 Bits	12
192 Bits	7680 Bits	348 Bits	22
256 Bits	15360 Bits	512 Bits	30

Benötigte Rechenzeit mit der Pollard-ρ Methode:

q	$\#E(\mathbb{Z}_q)$	MIPS Jahre
$\approx 2^{155}$	$\approx 2^{150}$	$3,8 \cdot 10^{10}$
$\approx 2^{210}$	$\approx 2^{205}$	$7,1 \cdot 10^{18}$
$\approx 2^{239}$	$\approx 2^{234}$	$1,6 \cdot 10^{28}$

Fazit

- Mit Hilfe elliptischer Kurven kann ein Public-Key-Kryptosystem gebildet werden.
- Asymmetrisches Verfahren
- Es ist schwer für zwei bekannte Punkte $G, W \in E(K)$ den Wert $s \in K$ zu berechnen, bei dem gilt

$$W = s \cdot G$$

- Überprüfen der gewählten Parameter
- Beste Attacke besitzt eine Laufzeit der Ordnung $O(\sqrt{n})$
- Geringe Schlüssellänge
  - Einsatz für Smartcards
  - Effizient für große Schlüssellänge

Quellen

- Elaine Barker, William Barker, William Burr, William Polk, and Miles Smid:
  Recommendation for Key Management Part 1: General
  National Institute of Standarts and Technologie (NIST), 2006
- Ian Blake, Gadiel Seroussi, Nigel Smart:
  Elliptic Curves in Cryptography.
  Cambridge University Press, 1999
- Ian Blake, Gadiel Seroussi, Nigel Smart:
  Advances in Elliptic Curve Cryptography.
  Cambridge University Press, 2005
- Certicom Corp.:
  Elliptic Curve Cryptography Tutorial.
  http://www.certicom.com, Stand: 25.01.2007
- Neal Koblitz:
  Algebraic Aspects of Cryptography.
  Springer-Verlag, 1998

- Thomas Laubrock:
  Krypto-Verfahren basierend auf elliptischen Kurven - HTML-Tutorial mit JavaTM-Applet
  Diplomarbeit an der Fachhochschule Dortmund,
  http://www.laubrock.de, 1999
- Alfred J. Menezes:
  Elliptic Curve Public Key Cryptosystems.
  3rd Edition, Kluwer Academic Publishers, 1996
- Joseph H. Silverman:
  The Arithmetic of Elliptic Curves.
  Springer-Verlag, 1986
- Douglas R. Stinson:
  Cryptography: Theory and Practice.
  2nd Edition, Chapman & Hall/CRC, 2002
- Dr. Anette Werner:
  Elliptische Kurven in der Kryptographie.
  Springer-Verlag, 2002
- Rainer Wilmink:
  Elliptic Curve Cryptosystems
  Diplomarbeit an der Universität Bielefeld,
  http://www.math.uni-bielefeld.de/~rwilmink/, 1999