Elliptische Kurven und ihre Anwendung in der Kryptographie

Carsten Baum

Institut für Informatik
Universität Potsdam

17. Juni 2009

Inhaltsverzeichnis

Charakteristik

Es sei $(K, +, \cdot)$ ein Körper.

Die Charakteristik des Körpers ist die Ordnung des neutralen Elements der Multiplikation bezüglich der Addition.

$$\underbrace{1 + 1 + \cdots + 1}_{n-mal} = 0$$

Gibt es kein solches n, so setzt man die Charakteristik 0.

Gibt es ein solches n, so ist es eine Primzahl.

Endliche Körper

Sei $(K, +, \cdot)$ ein Körper.

Der Körper heißt endlich, wenn $|K|$ endlich ist.

Jeder endliche Körper hat eine Charakteristik $p \neq 0$.

Zu jeder Primzahl p existiert ein Körper $(\mathbb{Z}_p, +, \cdot)$ der Ordnung p.

Galois Field

Es gelten die folgenden Aussagen:

1. Sei k die Ordnung eines Körpers, so ist $k = p^n$, wobei p prim ist (Primzahlpotenz).
2. Für eine Primzahl p und ein $n \in \mathbb{N}$ lässt sich ein Körper der Ordnung p^n konstruieren.
3. Seien K_1 und K_2 endliche Körper mit gleicher Ordnung p^n. Es existiert eine Abbildung $\phi : K_1 \rightarrow K_2$, die mit den Körperoperationen verträglich ist. Zwei Körper gleicher Ordnung sind also isomorph.

   Einen Körper der Ordnung p^n bezeichnet man als $GF(p^n)$ bzw. Galois Field. Für $n = 1$ spricht man von einem Primkörper nach einer Primzahl p.

Quadratischer Rest

Es sei $p \geq 3$ eine Primzahl und $a \in \mathbb{N}$. a heißt quadratischer Rest wenn $a \neq 0 \mod p$ und $\exists y \in \mathbb{Z}_p : y^2 \equiv a \mod p$.

Eulersches Kriterium

Es sei $p \geq 3$ eine Primzahl.

a ist ein quadratischer Rest mod $p \Leftrightarrow a^{\frac{p-1}{2}} \equiv 1 \mod p$.

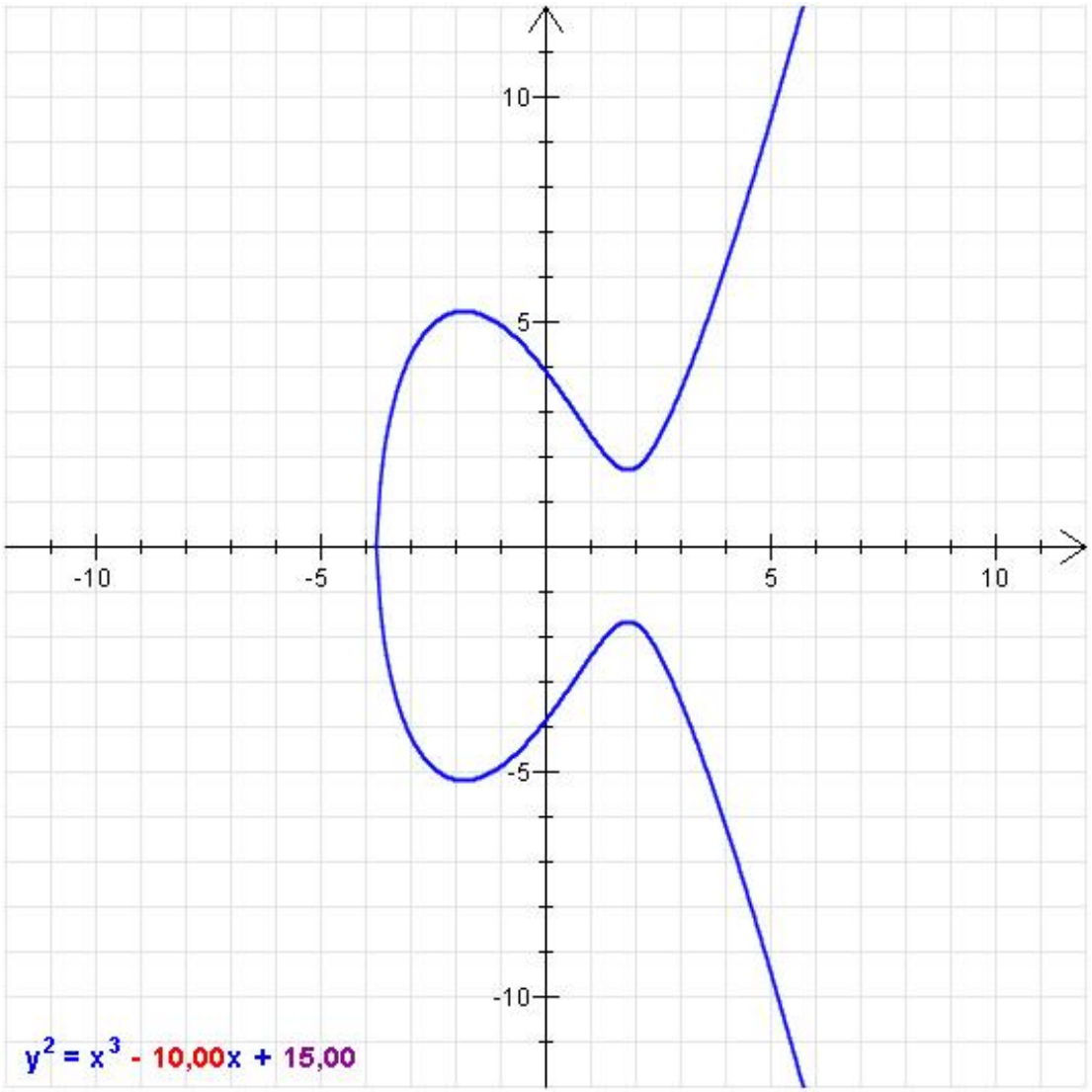
Definition

Es seien $a, b \in \mathbb{R}$ sowie $4a^3 + 27b^2 \neq 0$.

Eine Elliptische Kurve ist eine Menge E von Lösungen $(x, y) \in \mathbb{R}^2$ der Gleichung
$y^2 = x^3 + ax + b$
vereinigt mit dem Punkt in der Unendlichkeit O.

Die Gleichung $y^2 = x^3 + ax + b$ heißt **Weierstrass-Gleichung**.

Elliptische Kurve in $\mathbb{R}^2$



Herleitung der Addition über E

- Es sei E die Punktmenge einer Elliptischen Kurve sowie $P = (x_1, y_1), Q = (x_2, y_2) \in E$ mit $x_1 \neq x_2$.
- Man definiert die Addition $+$ der Gruppe $(E, +)$ wie folgt:

1. Es sei L die Gerade, die P und Q in E schneidet.
2. L schneidet E in einem weiteren Punkt, den man R' nennt. Spiegelt man R' an der x-Achse, so erhält man den Punkt R. Man definiert $R = P + Q$.

3. Die Gerade L sei $L = \lambda x + \nu$.
4. Der Anstieg λ ist $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$.
5. Der Summand ν ist $\nu = y_1 - \lambda x_1 = y_2 - \lambda x_2$.

Herleitung der Addition über E

6. Man berechnet nun $E \cap L$, um den Punkt R' zu finden.
7. $y = \lambda x + \nu \Rightarrow (\lambda x + \nu)^2 = x^3 + ax + b$
8. Man kann dies umformen zu
   $x^3 - \lambda^2 x^2 + (a - 2\lambda\nu)x + b - \nu^2 = 0$
9. Die Lösungen dieser Gleichung sind die x-Koordinaten von $E \cap L$.
10. Zwei der Lösungen sind mit x_1 und x_2 bereits bekannt.
11. Da x_1 und x_2 reelle Zahlen sind, muss auch x_3 reell sein.
12. Es gilt: $x_3 = \lambda^2 - x_1 - x_2$.
13. x_3 ist die x-Koordinate des Punktes R'.

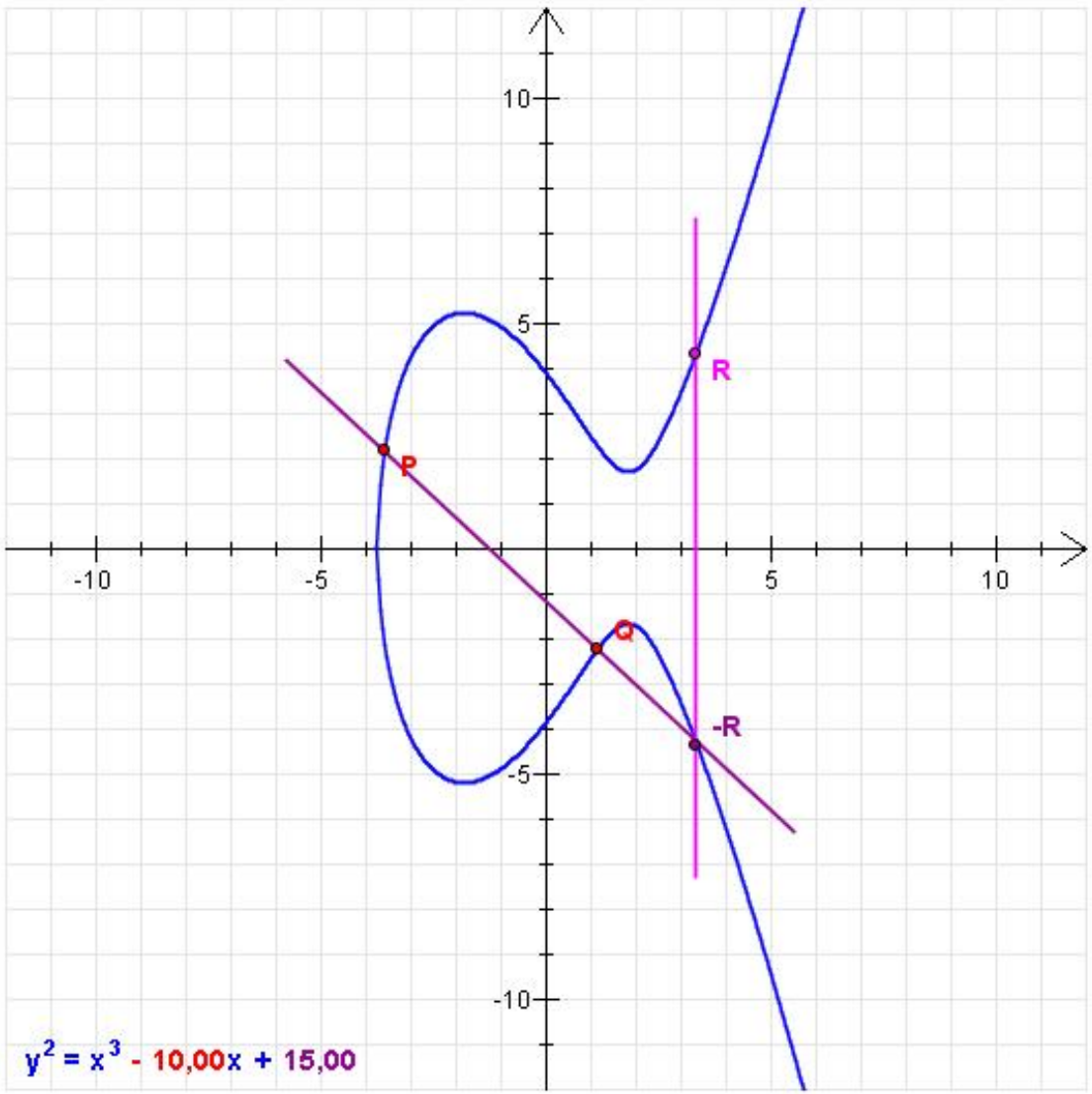
Herleitung der Addition über E

14 Es sei $-y_3$ die y-Koordinate von R' und damit y_3 die y-Koordinate von R.

15 Es gilt $\lambda = \frac{-y_3 - y_1}{x_3 - x_1}$ und damit $y_3 = \lambda(x_1 - x_3) - y_1$.

16 Damit ist $+$ auf E definiert.

Addition auf einer Elliptischen Kurve in $\mathbb{R}^2$



Regeln in $\mathbb{Z}_p$

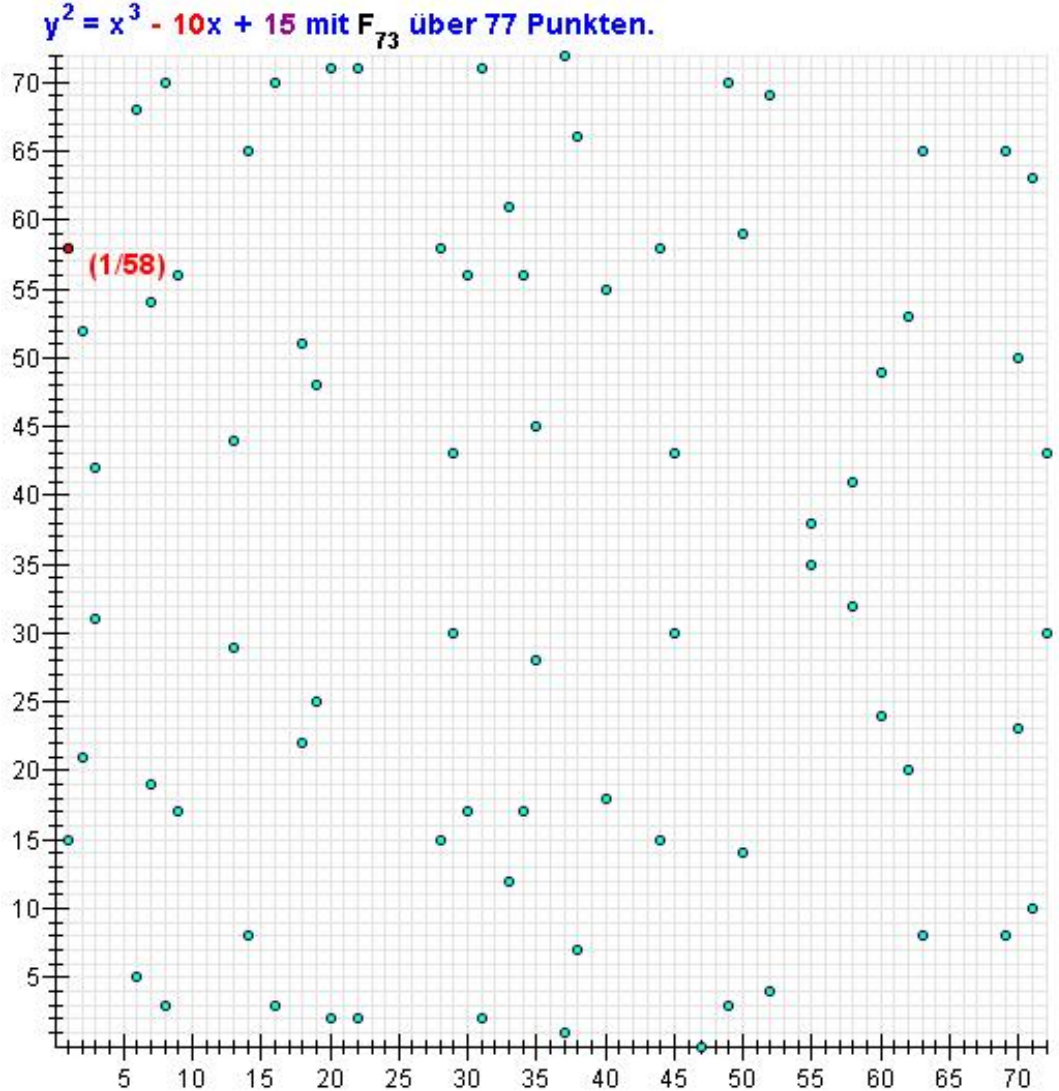
Es sei $GF(p)$ ein Körper mit $p > 3$.

Die Elliptische Kurve hat die Gleichung $y^2 = x^3 + ax + b$ mit $4a^3 + 27b^2 \neq 0$.

Es gelten die folgenden Rechenregeln:

1. $O + P = P + O = P$ für alle $P \in E$.
2. $P = (x, y)$ und $Q = (x, -y) \Rightarrow P + Q = O$.
3. Es seien $P = (x_1, y_1), Q = (x_2, y_2)$, $P, Q \neq O$ und $P + Q \neq O$.
   Dann ist $P + Q = (x_3, y_3)$ mit $x_3 = \lambda^2 - x_1 - x_2$, $y_3 = \lambda(x_1 - x_3) - y_1$.
   $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ für $P \neq Q$.
   $\lambda = \frac{3x_1^2 + a}{2y_1}$ für $P = Q$
4. Wenn $P = (x, y) \in E$, dann ist $-P = (x, -y) \in E$.

Elliptische Kurve in $\mathbb{Z}_{73}$



Regeln in $\mathbb{Z}_{2^n}$

Es sei $GF(2^n)$ ein Körper.

Die Elliptische Kurve hat die Gleichung $y^2 + xy = x^3 + ax^2 + b$ mit $b \neq 0$.

Es gelten die folgenden Rechenregeln:

1. $O + P = P + O = P$ für alle $P \in E$.
2. $P = (x, y)$ und $Q = (x, x + y) \Rightarrow P + Q = O$.
3. Es seien $P = (x_1, y_1), Q = (x_2, y_2)$, $P, Q \neq O$ und $P + Q \neq O$.
   Dann ist $P + Q = (x_3, y_3)$ mit $x_3 = \lambda^2 + \lambda - x_1 + x_2 + a$, $y_3 = \lambda(x_1 + x_3) + y_1 + x_3$.
   $\lambda = \frac{y_2 + y_1}{x_2 + x_1}$ für $P \neq Q$.
   $\lambda = x_1 + \frac{y_1}{x_1}$ für $P = Q$.
4. Wenn $P = (x, y) \in E$, dann ist $-P = (x, x + y) \in E$.

Satz von Hasse

Man kann die Anzahl n der Elemente in $E(\mathbb{Z}_p)$ nur schwer berechnen, aber mit dem Satz von Hasse abschätzen:

Es gilt $p + 1 - 2\sqrt{p} \leq n \leq p + 1 + 2\sqrt{p}$.

Die genaue Anzahl der Elemente kann man mit **Schoof's Algorithmus** berechnen.

Aussagen

Es sei $E(\mathbb{Z}_p)$ eine Elliptische Kurve mit $p > 3$, p ist prim.

1. Dann gibt es $n_1, n_2 \in \mathbb{N}$ so dass $(E, +)$ zu $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$ isomorph ist.
2. Weiterhin gilt $n_2 | n_1$ und $n_2 | (p-1)$.
3. Es gilt $n_2 = 1$, wenn E zyklisch ist.
4. Es gibt eine zyklische Untergruppe $(\langle G \rangle, +)$ der Ordnung n_1, die zu $(\mathbb{Z}_{n_1}, +)$ isomorph ist.

Das ECDLP

Voraussetzungen:

Es sei E die Punktmenge einer gegebenen Elliptischen Kurve über einem endlichen Körper K.

Es sei $G \in E$ ein Punkt der Ordnung n und $P \in \langle G \rangle$.

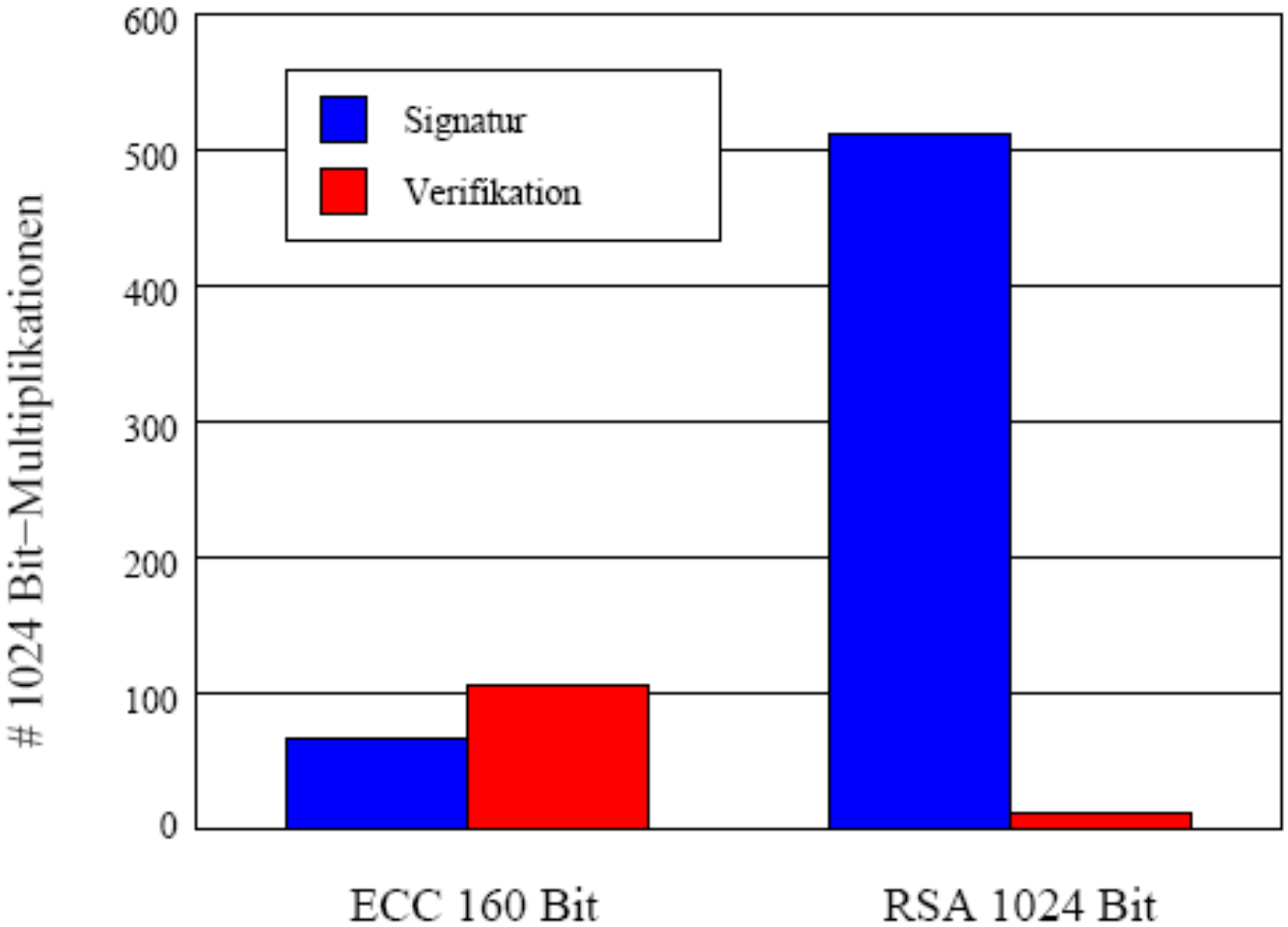
Problem:

Gesucht ist $k \in [0, n-1]$ mit $P = [k]G$.

Aus informatischer Sicht

- Sichere Schlüssellängen sind deutlich kürzer als bei RSA ($\approx$ 224 Bit).
- Erstellung von Signaturen ist mit geringerem Aufwand möglich als bei RSA (Verifikation nicht).
- Aufgrund der kürzeren Schlüssellängen kann das Verfahren auf Smartcards eingesetzt werden.

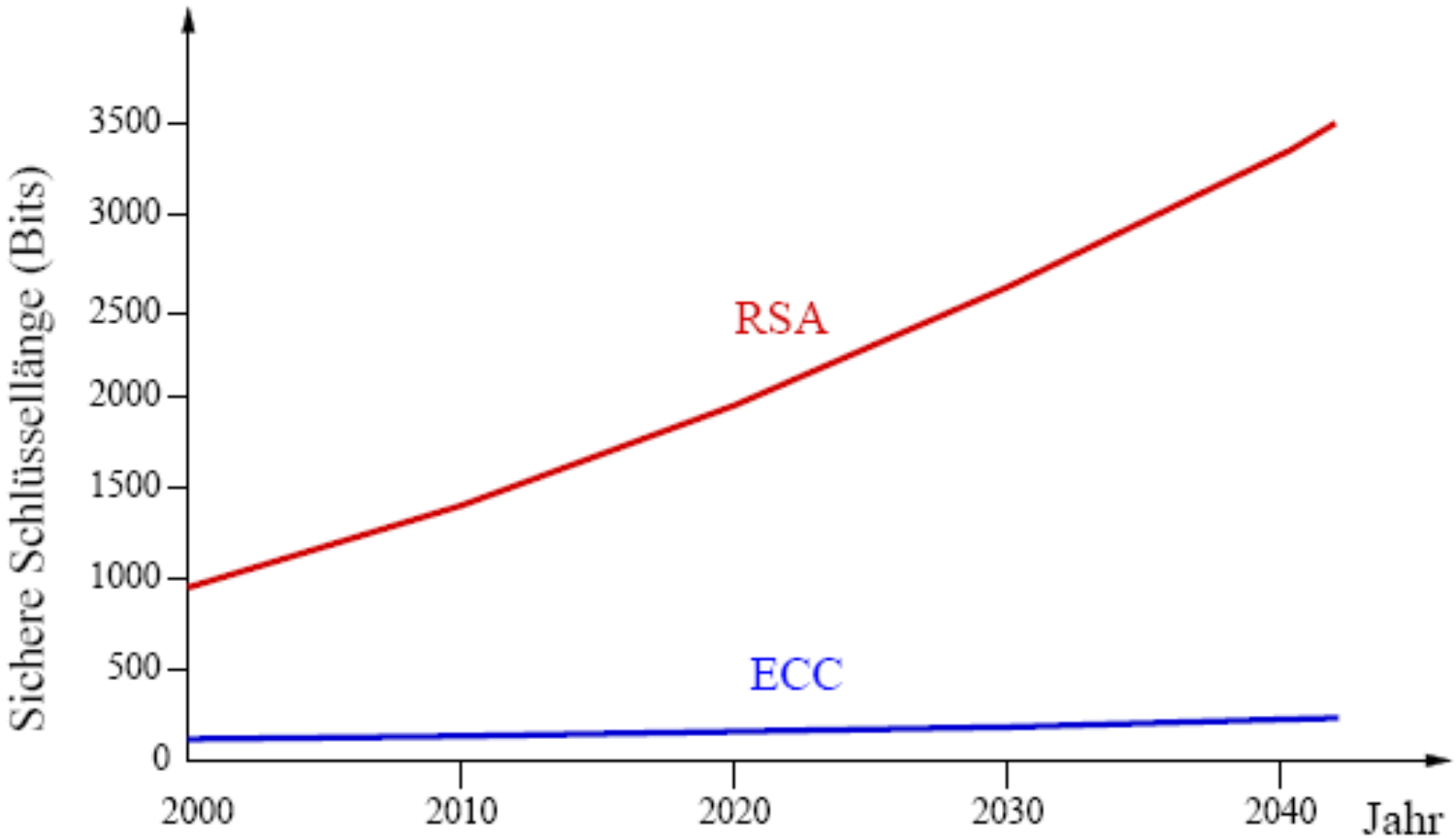
Anzahl der Multiplikationen



Aus kryptographischer Sicht

- Shanks Algorithmus, Pollard-ρ und Pohlig-Hellman lassen sich auch zum Lösen des ECDLP adaptieren.
- Der Aufwand für diese Verfahren steigt mit der Ordnung des Körpers exponentiell.
- Es gibt für Elliptische Kurven keine Verfahren, die ähnlich effizient sind wie Index-Calculus und Zahlkörpersieb für das DLP und die Faktorisierung.

Sichere Schlüssellängen



Sichere Kurven

Empfehlungen des BSI zu Kurven in Z_p

1. Die Ordnung des Punktes G muss eine Primzahl und mindestens 224 Bit groß sein.
2. Die Ordnungen des Punktes G und des zugrunde liegenden Körpers müssen verschieden sein.
3. p sollte so gewählt werden, dass $p^r \neq 1 \bmod n$ $\forall r \in [1, 10000]$

Definition

Parameter	**Bemerkungen**
p	Primzahl des zugrundeliegenden Körpers $\mathbb{Z}_p$
a	Erster Parameter der Weierstrass-Gleichung
b	Zweiter Parameter der Weierstrass-Gleichung
G	Generator einer Untergruppe in $E(\mathbb{Z}_p)$
n	Ordnung von G in $E(\mathbb{Z}_p)$
h	$\frac{\#(E(\mathbb{Z}_p))}{n}$

ECKA-Diffie-Hellman

1. Alice und Bob haben sich auf (p, a, b, G, n, h) geeinigt. Sie berechnen $l = h^{-1} \bmod n$.
2. Alice wählt zufällig ein $d_A \in \{1, \cdots, n-1\}$ und berechnet $P_A = [d_A]G$.

   Bob wählt zufällig ein $d_B \in \{1, \cdots, n-1\}$ und berechnet $P_B = [d_B]G$.
3. Alice und Bob tauschen P_A und P_B aus.
4. Alice berechnet $Q_A = [h]P_B$ und $S_A = [d_A \cdot l \bmod n]Q_A$.

   Bob berechnet $Q_B = [h]P_A$ und $S_B = [d_B \cdot l \bmod n]Q_B$.
5. Es ist $S_A = S_B$.

Definition

Parameter	**Bemerkungen**
p	Primzahl des zugrundeliegenden Körpers $\mathbb{Z}_p$
a	Erster Parameter der Weierstrass-Gleichung
b	Zweiter Parameter der Weierstrass-Gleichung
G	Generator einer Untergruppe in $E(\mathbb{Z}_p)$
n	Ordnung von G in $E(\mathbb{Z}_p)$
h	$\frac{\#(E(\mathbb{Z}_p))}{n}$

Punktkompression und -dekompression

Kompression

Berechne $PC : E\backslash\{O\} \to \mathbb{Z}_p \times \mathbb{Z}_2$ mit $PC(P) = (x, y \bmod 2)$ für $P = (x, y) \in E$.

Dekompression

Berechne $DC : \mathbb{Z}_p \times \mathbb{Z}_2 \to E\backslash\{O\}$

Es sei (x, i) gegeben.

1 $z \leftarrow x^3 + ax + b \bmod p$.

2a Ist z kein Quadratischer Rest, dann terminiere.

2b $y \leftarrow \sqrt{z} \bmod p$.

3 Wenn $y \equiv i \bmod 2$ dann ist y berechnet, ansonsten $y \leftarrow p - y$.

ECIES

Es sei E die Punktmenge einer Elliptischen Kurve über $\mathbb{Z}_p$ mit $G \in E$.

Es sei $H = \langle G \rangle$ eine zyklische Untergruppe mit der primen Ordnung n.

Der öffentliche Schlüssel ist (E, Q, G, n) mit $Q = [m]G$, $m \in \mathbb{Z}_p^*$.

Verschlüsseln:

Man wähle die geheime Nachricht $x \in \mathbb{Z}_p^*$ und die Zufallszahl $k \in \mathbb{Z}_n^*$.

Man berechnet $y_1 = PC([k]G)$ sowie $[k]Q = (x_0, y_0)$ und daraus $y_2 = xx_0 \mod p$.

Es ergibt sich der Schlüsseltext (y_1, y_2).

Entschlüsseln:

Man berechnet $(x_0, y_0) = [m]PD(y_1)$ und damit $x = y_2(x_0)^{-1} \mod p$.

Literatur

1. *Cryptography - Theory and Practice*, Stinson, 3. Auflage, Chapman & Hall
2. *CrypTool-Skript*, Esslinger et al., 9. Auflage, www.cryptool.org
3. *Elementary Number Theory, Cryptography and Codes*, Baldoni et al., 1. Auflage, Springer Science
4. *Technical Guideline TR-03111: Elliptic Curve Cryptography*, BSI, Version 1.11, www.bsi.bund.de