

Elliptische Kurven Kryptographie

Kevin Kappelman, Lukas Stevens

Technische Universität München

29. Mai 2016

Einleitung

Sicherheitsniveau	RSA/Diffie-Hellman	Elliptische-Kurven
≤ 80	1024	160-223
112	2048	224-255
128	3072	256-383
192	7680	384-511
256	15360	512+

Tabelle: Vergleich Schlüssellängen

Überblick

1 Einleitung

2 Grundbegriffe

- Affine Ebenen
- Projektive Ebenen

3 Elliptische Kurven

- Die unendlich ferne Gerade
- Weierstraß-Gleichung
- Affine Darstellung

4 Eine Gruppe über E

- Tangenten und Geraden
- Die Verknüpfung \oplus
- Die Gruppenoperation

5 Anwendungen

- Diskretes-Logarithmen-Problem
- Sicherheit
- Angriffe



Definition affiner Ebenen

Definition

Es sei \mathcal{A} eine Menge von Punkten und \mathcal{G} eine Menge von Geraden mit $\mathcal{G} \subseteq \text{Pot}(\mathcal{A})$. Bei $(\mathcal{A}, \mathcal{G})$ handelt es sich um eine affine Ebene, wenn folgende Bedingungen erfüllt sind:

- 1 Zu je zwei Elementen $a, b \in \mathcal{A}$ mit $a \neq b$ existiert genau ein $G \in \mathcal{G}$ mit $a, b \in G$.



Definition affiner Ebenen

Definition

Es sei \mathcal{A} eine Menge von Punkten und \mathcal{G} eine Menge von Geraden mit $\mathcal{G} \subseteq \text{Pot}(\mathcal{A})$. Bei $(\mathcal{A}, \mathcal{G})$ handelt es sich um eine affine Ebene, wenn folgende Bedingungen erfüllt sind:

- 1 Zu je zwei Elementen $a, b \in \mathcal{A}$ mit $a \neq b$ existiert genau ein $G \in \mathcal{G}$ mit $a, b \in G$.
- 2 Zu $G \in \mathcal{G}$ und $a \in \mathcal{A} \setminus G$ existiert genau ein $G' \in \mathcal{G}$ mit $a \in G'$ und $G \cap G' = \emptyset$.



Definition affiner Ebenen

Definition

Es sei \mathcal{A} eine Menge von Punkten und \mathcal{G} eine Menge von Geraden mit $\mathcal{G} \subseteq \text{Pot}(\mathcal{A})$. Bei $(\mathcal{A}, \mathcal{G})$ handelt es sich um eine affine Ebene, wenn folgende Bedingungen erfüllt sind:

- 1 Zu je zwei Elementen $a, b \in \mathcal{A}$ mit $a \neq b$ existiert genau ein $G \in \mathcal{G}$ mit $a, b \in G$.
- 2 Zu $G \in \mathcal{G}$ und $a \in \mathcal{A} \setminus G$ existiert genau ein $G' \in \mathcal{G}$ mit $a \in G'$ und $G \cap G' = \emptyset$.
- 3 Es existieren drei Elemente $a, b, c \in \mathcal{A}$ mit $c \notin \overline{a, b}$.



Definition projektiver Ebenen

Definition

Es sei \mathcal{A} eine Menge von Punkten und \mathcal{G} eine Menge von Geraden mit $\mathcal{G} \subseteq \text{Pot}(\mathcal{A})$. Bei $(\mathcal{A}, \mathcal{G})$ handelt es sich um eine projektive Ebene, wenn folgende Bedingungen erfüllt sind:

- 1 Zu je zwei Elementen $P, Q \in \mathcal{P}$ mit $P \neq Q$ existiert genau ein $G \in \mathcal{G}$ mit $P, Q \in G$.



Definition projektiver Ebenen

Definition

Es sei \mathcal{A} eine Menge von Punkten und \mathcal{G} eine Menge von Geraden mit $\mathcal{G} \subseteq \text{Pot}(\mathcal{A})$. Bei $(\mathcal{A}, \mathcal{G})$ handelt es sich um eine projektive Ebene, wenn folgende Bedingungen erfüllt sind:

- 1 Zu je zwei Elementen $P, Q \in \mathcal{P}$ mit $P \neq Q$ existiert genau ein $G \in \mathcal{G}$ mit $P, Q \in G$.
- 2 Für je zwei $G, H \in \mathcal{G}$ mit $G \neq H$ gilt $|G \cap H| = 1$.



Definition projektiver Ebenen

Definition

Es sei \mathcal{A} eine Menge von Punkten und \mathcal{G} eine Menge von Geraden mit $\mathcal{G} \subseteq \text{Pot}(\mathcal{A})$. Bei $(\mathcal{A}, \mathcal{G})$ handelt es sich um eine projektive Ebene, wenn folgende Bedingungen erfüllt sind:

- 1 Zu je zwei Elementen $P, Q \in \mathcal{P}$ mit $P \neq Q$ existiert genau ein $G \in \mathcal{G}$ mit $P, Q \in G$.
- 2 Für je zwei $G, H \in \mathcal{G}$ mit $G \neq H$ gilt $|G \cap H| = 1$.
- 3 Es existieren vier verschiedene Elemente in \mathcal{P} , sodass immer höchstens zwei davon in jedem beliebigen $G \in \mathcal{G}$ liegen.

$\text{PG}(2, \mathbb{F})$

Konstruktion affiner Ebenen aus projektiven Ebenen

Abbildung: Von der Fano-Ebene zur minimalen affinen Ebene

Konstruktion affiner Ebenen aus projektiven Ebenen

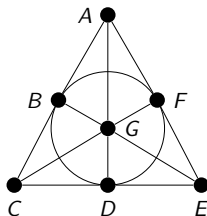


Abbildung: Von der Fano-Ebene zur minimalen affinen Ebene

Konstruktion affiner Ebenen aus projektiven Ebenen

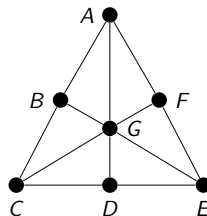
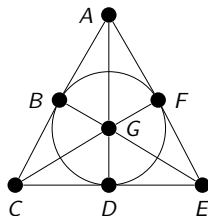


Abbildung: Von der Fano-Ebene zur minimalen affinen Ebene

Konstruktion affiner Ebenen aus projektiven Ebenen

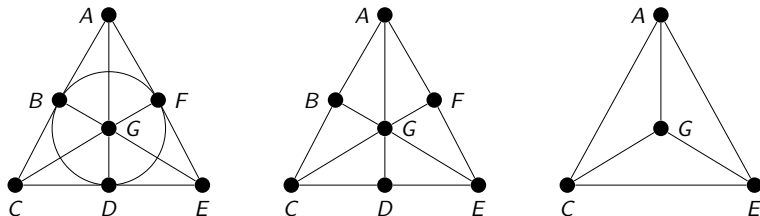


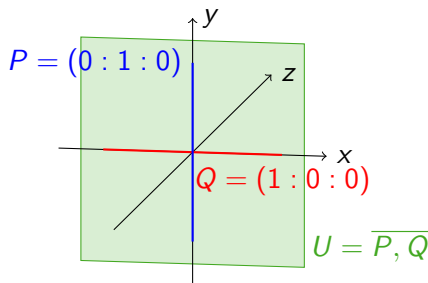
Abbildung: Von der Fano-Ebene zur minimalen affinen Ebene

Elliptische Kurven – Die unendlich ferne Gerade

- Wähle $U := \overline{P, Q}$ mit $P = (1 : 0 : 0)$, $Q = (0 : 1 : 0)$.

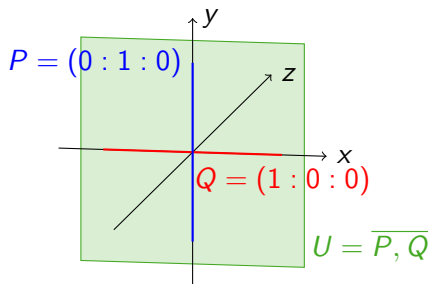
Elliptische Kurven – Die unendlich ferne Gerade

- Wähle $U := \overline{P, Q}$ mit $P = (1 : 0 : 0)$, $Q = (0 : 1 : 0)$.
- U ist im dreidimensionalen Raum genau die x, y -Ebene mit $z = 0$.



Elliptische Kurven – Die unendlich ferne Gerade

- Wähle $U := \overline{P, Q}$ mit $P = (1 : 0 : 0)$, $Q = (0 : 1 : 0)$.
- U ist im dreidimensionalen Raum genau die x, y -Ebene mit $z = 0$.



- Wir bezeichnen U als die **unendlich ferne Gerade**.

Elliptische Kurven – Die unendlich ferne Gerade

Lemma

Gegeben sei die projektive Ebene $(\mathcal{P}, \mathcal{G}) = PG(2, \mathbb{F})$ und die unendlich ferne Gerade U , dann ist die Abbildung

$$\phi : \mathbb{F}^2 \rightarrow \mathcal{P}_U, (a, b) \mapsto (a : b : 1)$$

bijektiv und bildet Geraden auf Geraden ab, d.h. ϕ ist ein Isomorphismus von affinen Ebenen.

Elliptische Kurven – Weierstraß-Gleichung

Erinnerung: Punktemenge von $\text{PG}(2, \mathbb{F})$

$$P = \{(x : y : z) \mid (x, y, z) \in \mathbb{F}^3 \setminus \{\mathbf{0}\}\}$$

Definition

Eine elliptische Kurve $E \subseteq P$ ist durch die Lösung der
Weierstraß-Gleichung

$$0 = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3$$

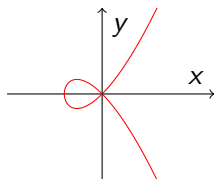
gegeben, wobei $a_i \in \mathbb{F}$ gilt und die Lösung keine Singularitäten besitzen darf.

Elliptische Kurven – Weierstraß-Gleichung

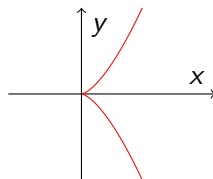
Definition

Eine Kurve E ist **singulär** in einem Punkt $P = (a : b : c) \in E$, wenn gilt:

$$\frac{\partial F}{\partial X}(P) = \frac{\partial F}{\partial Y}(P) = \frac{\partial F}{\partial Z}(P) = 0$$



(a) $y^2 = x^3 + x^2$



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

Abbildung: Kurven mit Singularitäten (Knoten und Spitze)

Elliptische Kurven – Weierstraß-Gleichung

- Wir schränken ein: Die *Charakteristik* des Körpers \mathbb{F} soll nicht 2 und nicht 3 sein: $\text{char } \mathbb{F} \neq 2, 3$.

Elliptische Kurven – Weierstraß-Gleichung

- Wir schränken ein: Die *Charakteristik* des Körpers \mathbb{F} soll nicht 2 und nicht 3 sein: $\text{char } \mathbb{F} \neq 2, 3$.
- Dies bedeutet, dass $1 + 1 \neq 0$ bzw. $1 + 1 + 1 \neq 0$, wobei 0, 1 die neutralen Elemente der Addition bzw. Multiplikation von \mathbb{F} sind.

Elliptische Kurven – Weierstraß-Gleichung

- Wir schränken ein: Die *Charakteristik* des Körpers \mathbb{F} soll nicht 2 und nicht 3 sein: $\text{char } \mathbb{F} \neq 2, 3$.
- Dies bedeutet, dass $1 + 1 \neq 0$ bzw. $1 + 1 + 1 \neq 0$, wobei 0, 1 die neutralen Elemente der Addition bzw. Multiplikation von \mathbb{F} sind.
- Unter diesen Voraussetzungen können wir die Weierstraß-Gleichung vereinfachen zu:

$$0 = Y^2Z - X^3 - aXZ^2 - bZ^3$$

Elliptische Kurven – Affine Darstellung

- Wir betrachten die elliptische Kurve

$$E = \{(X : Y : Z) \mid 0 = Y^2Z - X^3 - aXZ^2 - bZ^3\}$$

Elliptische Kurven – Affine Darstellung

- Wir betrachten die elliptische Kurve

$$E = \{(X : Y : Z) \mid 0 = Y^2Z - X^3 - aXZ^2 - bZ^3\}$$

- Wir erinnern uns an die unendlich fernen Gerade
 $U = \overline{(0 : 1 : 0), (1 : 0 : 0)}.$

Elliptische Kurven – Affine Darstellung

- Wir betrachten die elliptische Kurve

$$E = \{(X : Y : Z) \mid 0 = Y^2Z - X^3 - aXZ^2 - bZ^3\}$$

- Wir erinnern uns an die unendlich fernen Gerade
 $U = \overline{(0 : 1 : 0), (1 : 0 : 0)}$.
- Es gilt: $U \cap E = (0 : 1 : 0) =: \mathcal{O}$, d.h. es liegt nur \mathcal{O} auf unserer Kurve E .

Elliptische Kurven – Affine Darstellung

- Wir betrachten die elliptische Kurve

$$E = \{(X : Y : Z) \mid 0 = Y^2Z - X^3 - aXZ^2 - bZ^3\}$$

- Wir erinnern uns an die unendlich fernen Gerade
 $U = \overline{(0 : 1 : 0), (1 : 0 : 0)}$.
- Es gilt: $U \cap E = (0 : 1 : 0) =: \mathcal{O}$, d.h. es liegt nur \mathcal{O} auf unserer Kurve E .
- Wir bezeichnen \mathcal{O} als den **unendlich fernen Punkt**.

Elliptische Kurven – Affine Darstellung

- Für alle anderen Punkte $P \in E$ ist die z-Koordinate $\neq 0$, d.h. alle Punkte außer \mathcal{O} liegen im affinen Teil von E .

Elliptische Kurven – Affine Darstellung

- Für alle anderen Punkte $P \in E$ ist die z-Koordinate $\neq 0$, d.h. alle Punkte außer \mathcal{O} liegen im affinen Teil von E .
- Wir können also $P \in \{(x : y : 1) \mid x, y \in \mathbb{F}\}$ annehmen.

Elliptische Kurven – Affine Darstellung

- Für alle anderen Punkte $P \in E$ ist die z-Koordinate $\neq 0$, d.h. alle Punkte außer \mathcal{O} liegen im affinen Teil von E .
- Wir können also $P \in \{(x : y : 1) \mid x, y \in \mathbb{F}\}$ annehmen.
- Die Weierstraß-Gleichung für diese Punkte vereinfacht sich zu:

$$f(x, y) := y^2 - x^3 - ax - b$$

Elliptische Kurven – Affine Darstellung

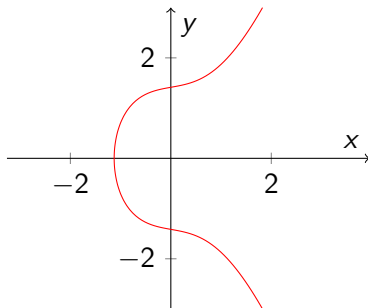
- Für alle anderen Punkte $P \in E$ ist die z-Koordinate $\neq 0$, d.h. alle Punkte außer \mathcal{O} liegen im affinen Teil von E .
- Wir können also $P \in \{(x : y : 1) \mid x, y \in \mathbb{F}\}$ annehmen.
- Die Weierstraß-Gleichung für diese Punkte vereinfacht sich zu:

$$f(x, y) := y^2 - x^3 - ax - b$$

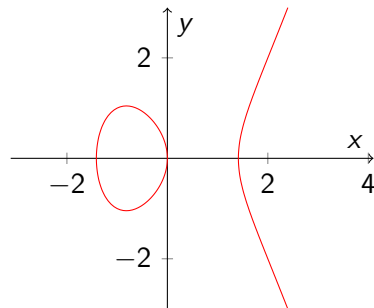
- Insgesamt gilt also:

$$E = \{(x : y : 1) \mid (x, y) \in \mathbb{F}^2 \wedge f(x, y) = 0\} \cup \{\mathcal{O}\}$$

Elliptische Kurven – Affine Darstellung



(a) $y^2 = x^3 + 0.5x + 2$



(b) $y^2 = x^3 - 2x$

Abbildung: Affine Darstellung elliptischer Kurven

Elliptische Kurven – Affine Darstellung

Lemma

Gegeben sei eine elliptische Kurve E , die durch die Lösungen der vereinfachten Weierstraß-Gleichung definiert ist:

$$E : Y^2Z = X^3 + aXZ^2 + bZ^3.$$

Dann gilt: Die Kurve E ist genau dann nicht-singulär, wenn das Polynom $f(x) = x^3 + ax + b$ keine mehrfachen Nullstellen besitzt.

Eine Gruppe über E – Voraussetzungen

- Es gelte $\text{char } \mathbb{F} \neq 2, 3$
- E sei nicht singulär.

Tangenten

Definition

Es sei P ein Punkt der elliptischen Kurve E . Wir definieren die Tangente an E im Punkt P :

$$T_P := \left\{ (u : v : w) \in \mathcal{P} \mid \frac{\partial F}{\partial X}(P)u + \frac{\partial F}{\partial Y}(P)v + \frac{\partial F}{\partial Z}(P)w = 0 \right\}$$

Geraden

1 Unendlich ferne Gerade U

Geraden

- 1 Unendlich ferne Gerade U
- 2 Affine Geraden: $y = kx + d$

Geraden

- 1 Unendlich ferne Gerade U
- 2 Affine Geraden: $y = kx + d$
- 3 Parallele zur y -Achse: $v + \lambda(0, 1)$ mit $v = (x, y)$ und $\lambda \in \mathbb{F}$

Eine Gruppe über E – Die Verknüpfung \oplus

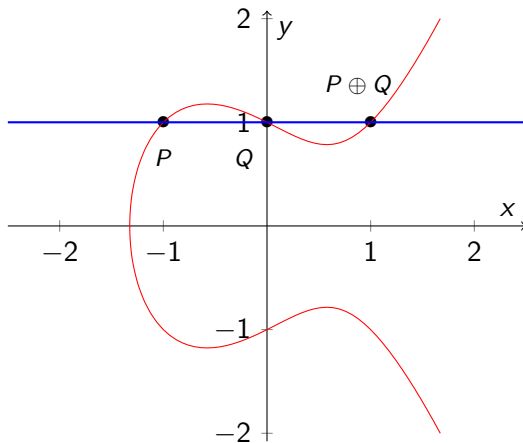
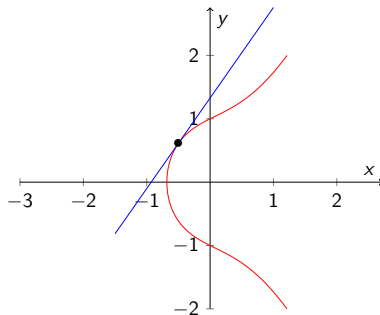


Abbildung: $P \oplus Q$

Vereinbarungen

Abbildung: Vereinbarungen(1)

Vereinbarungen



(a) $P \oplus P$

Abbildung: Vereinbarungen(1)

Vereinbarungen

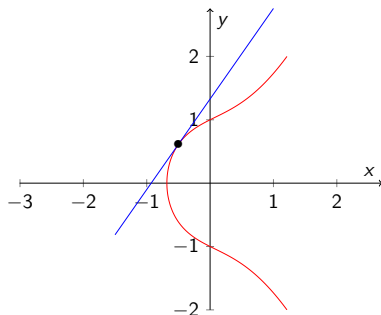
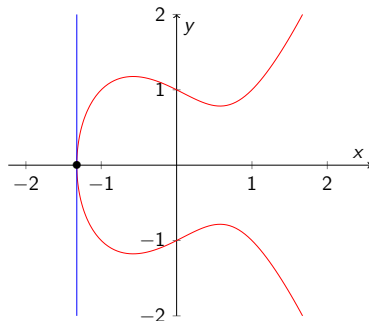
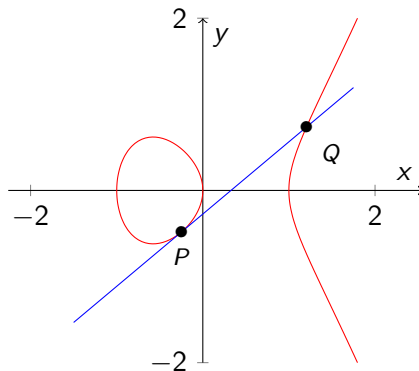
(a) $P \oplus P$ (b) $P \oplus P = P$

Abbildung: Vereinbarungen(1)

Vereinbarungen



$$(a) P \oplus Q = P$$

Abbildung: Vereinbarungen(2)

Kommutativität und Abgeschlossenheit

Fallunterscheidung für

$$P \oplus Q = R:$$

Kommutativität und Abgeschlossenheit

Fallunterscheidung für

$$P \oplus Q = R:$$

1 $P = Q = \mathcal{O}:$

$$\mathcal{O} \oplus \mathcal{O} = \mathcal{O}$$

Kommutativität und Abgeschlossenheit

Fallunterscheidung für

$$P \oplus Q = R:$$

1 $P = Q = \mathcal{O}:$

$$\mathcal{O} \oplus \mathcal{O} = \mathcal{O}$$

2 $P = \mathcal{O}:$

$$\mathcal{O} \oplus Q = -Q$$



Kommutativität und Abgeschlossenheit

Fallunterscheidung für

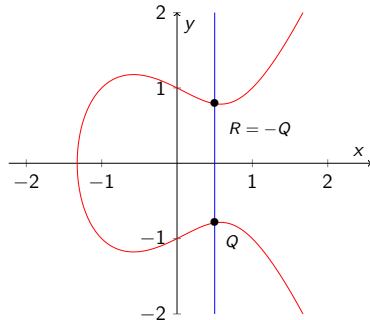
$$P \oplus Q = R:$$

1 $P = Q = \mathcal{O}:$

$$\mathcal{O} \oplus \mathcal{O} = \mathcal{O}$$

2 $P = \mathcal{O}:$

$$\mathcal{O} \oplus Q = -Q$$



(a) $\mathcal{O} \oplus Q = -Q$



Kommutativität und Abgeschlossenheit

Fallunterscheidung für

$$P \oplus Q = R:$$

1 $P = Q = \mathcal{O}:$

$$\mathcal{O} \oplus \mathcal{O} = \mathcal{O}$$

2 $P = \mathcal{O}:$

$$\mathcal{O} \oplus Q = -Q$$

3 $P = -Q:$

$$P \oplus (-P) = \mathcal{O}$$



Kommutativität und Abgeschlossenheit

Fallunterscheidung für

$$P \oplus Q = R:$$

1 $P = Q = \mathcal{O}:$

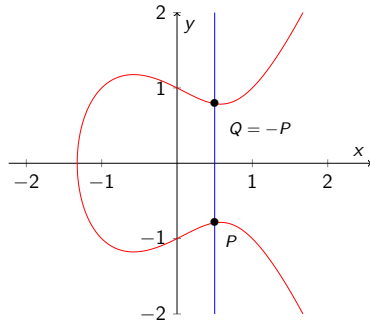
$$\mathcal{O} \oplus \mathcal{O} = \mathcal{O}$$

2 $P = \mathcal{O}:$

$$\mathcal{O} \oplus Q = -Q$$

3 $P = -Q:$

$$P \oplus (-P) = \mathcal{O}$$



(b) $P \oplus (-P) = \mathcal{O}$



Kommutativität und Abgeschlossenheit

Fallunterscheidung für

$$P \oplus Q = R:$$

1 $P = Q = \mathcal{O}:$

$$\mathcal{O} \oplus \mathcal{O} = \mathcal{O}$$

2 $P = \mathcal{O}:$

$$\mathcal{O} \oplus Q = -Q$$

3 $P = -Q:$

$$P \oplus (-P) = \mathcal{O}$$

4 $P \neq \pm Q:$

$$P \oplus Q = R$$



Kommutativität und Abgeschlossenheit

Fallunterscheidung für

$$P \oplus Q = R:$$

1 $P = Q = \mathcal{O}:$

$$\mathcal{O} \oplus \mathcal{O} = \mathcal{O}$$

2 $P = \mathcal{O}:$

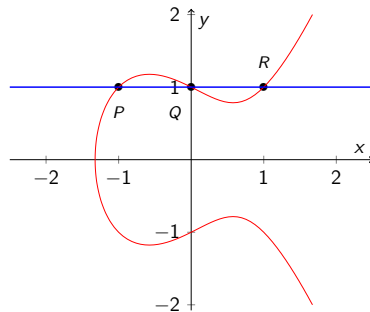
$$\mathcal{O} \oplus Q = -Q$$

3 $P = -Q:$

$$P \oplus (-P) = \mathcal{O}$$

4 $P \neq \pm Q:$

$$P \oplus Q = R$$



(c) $P \oplus Q = R$



Kommutativität und Abgeschlossenheit

Fallunterscheidung für

$$P \oplus Q = R:$$

1 $P = Q = \mathcal{O}:$

$$\mathcal{O} \oplus \mathcal{O} = \mathcal{O}$$

2 $P = \mathcal{O}:$

$$\mathcal{O} \oplus Q = -Q$$

3 $P = -Q:$

$$P \oplus (-P) = \mathcal{O}$$

4 $P \neq \pm Q:$

$$P \oplus Q = R$$

5 $P = Q \neq -P:$

$$P \oplus P = R$$



Kommutativität und Abgeschlossenheit

Fallunterscheidung für

$$P \oplus Q = R:$$

1 $P = Q = \mathcal{O}:$

$$\mathcal{O} \oplus \mathcal{O} = \mathcal{O}$$

2 $P = \mathcal{O}:$

$$\mathcal{O} \oplus Q = -Q$$

3 $P = -Q:$

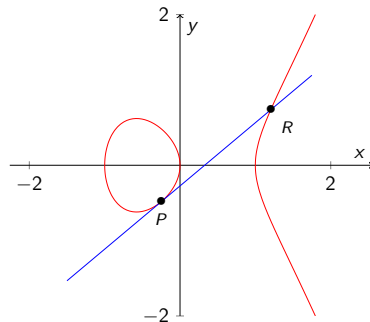
$$P \oplus (-P) = \mathcal{O}$$

4 $P \neq \pm Q:$

$$P \oplus Q = R$$

5 $P = Q \neq -P:$

$$P \oplus P = R$$



(d) $P \oplus P = R$



Mathematische Beschreibung der \oplus -Verknüpfung

Satz

Es sei $P = (x, y), Q = (u, v) \in E \setminus \{\mathcal{O}\}$. Dann gilt:

$$\mathcal{O} \oplus \mathcal{O} = \mathcal{O}, \quad \mathcal{O} \oplus P = (x, -y) =: -P \quad \text{und}$$

$$P \oplus Q = \begin{cases} \mathcal{O}, & \text{falls } P = -Q \\ (w, k(w - x) + y), & \text{sonst} \end{cases}$$

wobei

$$w = k^2 - x - u \quad \text{und} \quad k = \begin{cases} \frac{v-y}{u-x}, & \text{falls } P \neq \pm Q \\ \frac{3x^2+a}{2y}, & \text{falls } P = Q \neq -P \end{cases}$$

Eine Gruppe über E – Die Gruppenoperation

Wir definieren die Verknüpfung $+$ für $P, Q \in E$ folgendermaßen:

$$P + Q := \mathcal{O} \oplus (P \oplus Q) = -(P \oplus Q).$$

Satz

$(E, +)$ ist eine abelsche Gruppe mit neutralem Element \mathcal{O} .

Eine Gruppe über E – Die Gruppenoperation

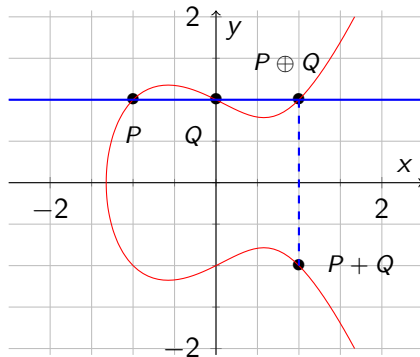


Abbildung: Grafische Addition in $(E, +)$

Anwendungen – Diskretes-Logarithmen-Problem

Definition

Sei G eine Gruppe und seien $x, y \in G$. Das Finden von $m \in \mathbb{N}$, so dass gilt

$$x^m = y,$$

wird **Diskretes-Logarithmen-Problem** (kurz DLP) genannt.

Anwendungen – Diskretes-Logarithmen-Problem

Definition

Sei G eine Gruppe und seien $x, y \in G$. Das Finden von $m \in \mathbb{N}$, so dass gilt

$$x^m = y,$$

wird **Diskretes-Logarithmen-Problem** (kurz DLP) genannt.

Über elliptische Kurven:

- Wähle $P, Q \in E$ und ein $m \in \mathbb{N}$. Das DLP ist dann die Lösung der Gleichung $mP = Q$, wobei P und Q bekannt sind.

Anwendungen – Diskretes-Logarithmen-Problem

Definition

Sei G eine Gruppe und seien $x, y \in G$. Das Finden von $m \in \mathbb{N}$, so dass gilt

$$x^m = y,$$

wird **Diskretes-Logarithmen-Problem** (kurz DLP) genannt.

Über elliptische Kurven:

- Wähle $P, Q \in E$ und ein $m \in \mathbb{N}$. Das DLP ist dann die Lösung der Gleichung $mP = Q$, wobei P und Q bekannt sind.
- Die skalare Multiplikation des Punktes P wird durch wiederholtes Addieren des Punktes mit sich selbst dargestellt.

Anwendungen – Sicherheit

- Naives Probieren: $O(|E|)$.

Anwendungen – Sicherheit

- Naives Probieren: $O(|E|)$.

Wir erinnern uns:

- DLP beispielsweise mit Babystep-Giantstep in $O(\sqrt{|E|})$ lösbar.

Anwendungen – Sicherheit

- Naives Probieren: $O(|E|)$.

Wir erinnern uns:

- DLP beispielsweise mit Babystep-Giantstep in $O(\sqrt{|E|})$ lösbar.
- DLP mit Hilfe von Primzahlen mit Index-Calculus-Algorithmen subexponentiell lösbar.

Anwendungen – Sicherheit

- Naives Probieren: $O(|E|)$.

Wir erinnern uns:

- DLP beispielsweise mit Babystep-Giantstep in $O(\sqrt{|E|})$ lösbar.
 - DLP mit Hilfe von Primzahlen mit Index-Calculus-Algorithmen subexponentiell lösbar.
- Aber:** Elliptische Kurven besitzen keine “Primzahlen”.

Anwendungen – Angriffe

Beispiel: Wir wollen $13P$ berechnen:

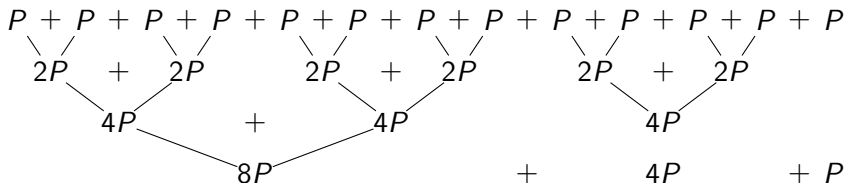


Abbildung: Effiziente Skalarmultiplikation mit Additionsbaum

Anwendungen – Angriffe

Beispiel: Wir wollen $13P$ berechnen:

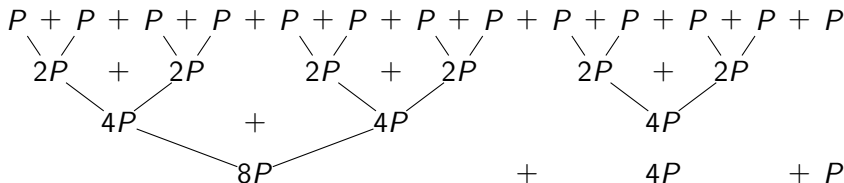


Abbildung: Effiziente Skalarmultiplikation mit Additionsbaum

- Fallunterscheidungen bei Addition notwendig.

Anwendungen – Angriffe

Beispiel: Wir wollen $13P$ berechnen:

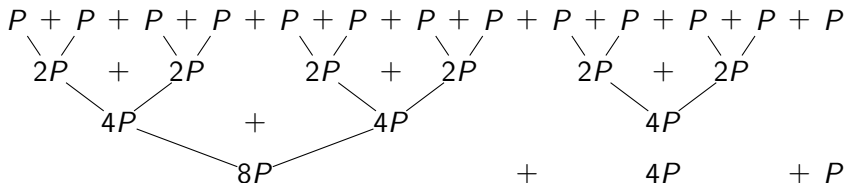


Abbildung: Effiziente Skalarmultiplikation mit Additionsbaum

- Fallunterscheidungen bei Addition notwendig.

⇒ Rückschlüsse über Schlüssel mit Seitenkanalangriff möglich.

The End

Zusammengefasst: Elliptische Kurven sind einfach super.