

# Elliptische Kurven Kryptographie

Kevin Kappelman, Lukas Stevens

Technische Universität München

22. Mai 2016

# Überblick

## 1 Einleitung

## 2 Grundbegriffe

- Affine Ebenen

## 3 Elliptische Kurven

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

## 4 Eine Gruppe über $E$

- Tangenten
- Die Gruppenoperation

## 5 Anwendungen

- Diskretes-Logarithmen-Problem
- Sicherheit
- Angriffe

# Einleitung

Blubb Lukas



# Grundbegriffe – Affine Ebenen

Blubb2 Lukas



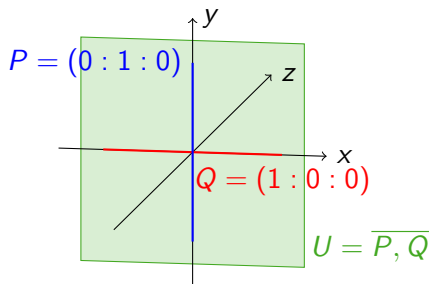
# Elliptische Kurven – Die unendlich ferne Gerade

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



# Elliptische Kurven – Die unendlich ferne Gerade

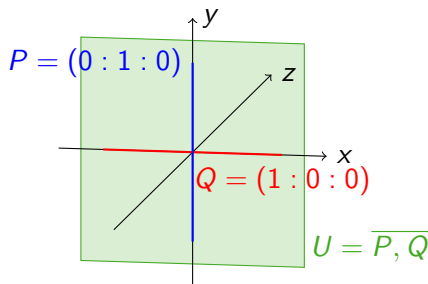
- Wähle  $U := \overline{P, Q}$  mit  $P = (1 : 0 : 0)$ ,  $Q = (0 : 1 : 0)$ .
- $U$  ist im dreidimensionalen Raum genau die  $x, y$ -Ebene mit  $z = 0$ .





# 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.  $\phi$  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**

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

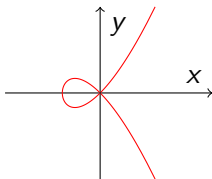
gegeben, wobei  $a_i \in \mathbb{F}$  gilt und die Lösung keine Singularitäten besitzen darf.

# Elliptische Kurven – Weierstraß-Gleichung

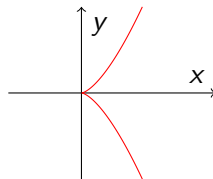
## Definition

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 Weierstraßgleichung für diese Punkte vereinfacht sich zu:

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



# Elliptische Kurven – Affine Darstellung

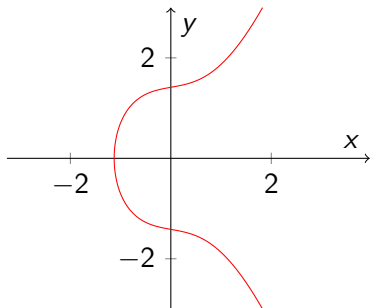
- Für alle anderen Punkte  $P \in E$  ist die z-Koordinate  $\neq 0$ , d.h. alle Punkte außer  $\mathcal{O}$  liegen im affinen Teil von  $E$ .
- Wir können also  $P \in \{(x : y : 1) \mid x, y \in \mathbb{F}\}$  annehmen.
- Die Weierstraßgleichung für diese Punkte vereinfacht sich zu:

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

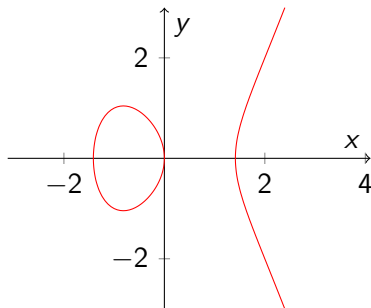
- Insgesamt gilt also:

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

# 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

Lukas Teil. Blub



# Eine Gruppe über $E$ – Tangenten

Blub



# 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

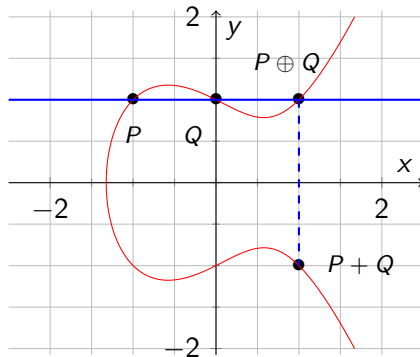


Abbildung: Grafische Addition in  $(E, +)$



# Blocks of Highlighted Text

## Block 1

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Integer lectus nisl, ultricies in feugiat rutrum, porttitor sit amet augue. Aliquam ut tortor mauris. Sed volutpat ante purus, quis accumsan dolor.

## Block 2

Pellentesque sed tellus purus. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos himenaeos. Vestibulum quis magna at risus dictum tempor eu vitae velit.



# 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** (kury 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** (kury 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** (kury 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:  $O(|E|)$ .

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.

# 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:

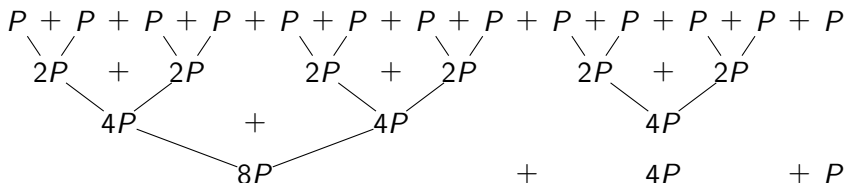
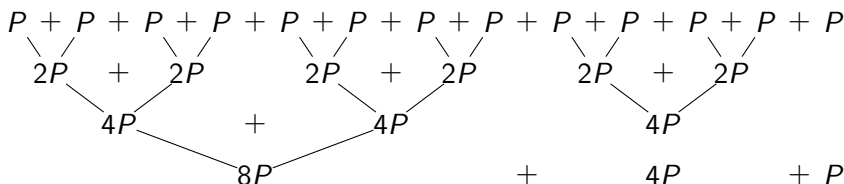


Abbildung: Effiziente Skalarmultiplikation mit Additionsbaum

# Anwendungen – Angriffe

Beispiel: Wir wollen  $13P$  berechnen:

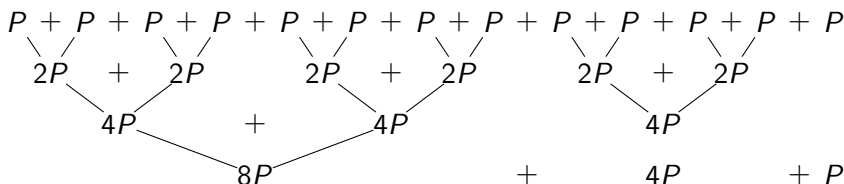


**Abbildung:** Effiziente Skalarmultiplikation mit Additionsbaum

- Fallunterscheidungen bei Addition notwendig.

# Anwendungen – Angriffe

Beispiel: Wir wollen  $13P$  berechnen:

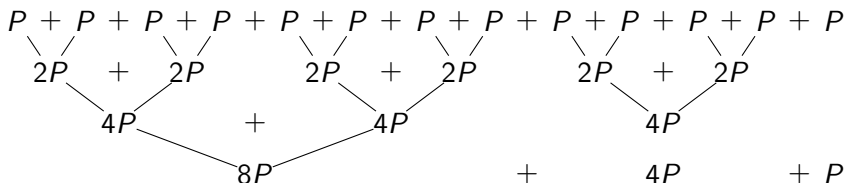


**Abbildung:** Effiziente Skalarmultiplikation mit Additionsbaum

- Fallunterscheidungen bei Addition notwendig.

# Anwendungen – Angriffe

Beispiel: Wir wollen  $13P$  berechnen:



**Abbildung:** Effiziente Skalarmultiplikation mit Additionsbaum

- Fallunterscheidungen bei Addition notwendig.  
 $\Rightarrow$  Rückschlüsse über Schlüssel mit Seitenkanalangriff möglich.

# References



John Smith (2012)

Title of the publication

*Journal Name* 12(3), 45 – 678.



# The End

Zusammengefasst: Elliptische Kurven sind einfach super.