

Inhalt der Vorlesung

Elliptische Kurven und Kryptographie im SoSe 2015

PD Dr. K. Halupczok

Separat: Notationstabelle

§0 Motivation und Einführung

vorl.:  
1

§1 Allgemeines zu Kryptographieverfahren

§1.1 Grundlagen aus der elem. ZT und Gruppentheorie

1.1.1 Zahlen, Darstellung von Zahlen

2

1.1.2 Kongruenzrechnen und die "modulare Brille"

3

1.1.3 Gruppen, faires Münzwurfsketchen am Telefon

4

§1.2 Public-Key-Kryptographie

1.2.1 RSA-Verfahren

} 5

1.2.2 Diffie-Hellman-Verfahren

1.2.3 ElGamal-Verschlüsselung

§1.3 Digitale Unterschriften

1.3.1 ElGamal-/DSA-Signatur

} 6

§2 Elliptische Kurven

§2.1 Grundlagen aus der Algebra

2.1.1 Polynome

2.1.2 Endliche Körper

} 7

§2.2 Der affine Raum, affine Kurven und der <sup>zweidimensionale</sup> projektive Raum 8

2.2.1 Die affine und projektive Ebene

2.2.2 Affine Kurven

§2.3 Projektive Kurven

2.3.1 Homogene Polynome und projektive Kurven

9

2.3.2 Der Satz von Bézout

10

§2.4 Elliptische Kurven

2.4.1 Definition elliptischer Kurven und vereinfachte Weierstraßgleichungen

11

2.4.2 Das Diskriminantenkriterium

12

- PFINGSTPAUSE -

- 2.4.3 Die Gruppenstruktur elliptischer Kurven 13
- 2.4.4 Das Assoziativgesetz 14
- 2.4.5 Schnelle Arithmetik auf elliptischen Kurven 15

Einschub: Wiederholung, Beispiele, Vertiefung W1, W2

Vertretung am 17.6.: Franziska Jahnke; die ENIGMA und ihre Rolle im 2. WK

§ 3 Elliptische Kurven über verschiedenen Körpern

- § 3.1 Elliptische Kurven über  $\mathbb{Q}$  } 16
- § 3.2 Elliptische Kurven über  $\mathbb{C}$  } 16
- § 3.3 Elliptische Kurven über  $\mathbb{F}_p$  und  $\mathbb{F}_{p^r}$  } 17
  - 3.3.1 Punkte zählen, der Frobenius } 17
  - 3.3.2 Modularitätsmuster und der große Fermatsche Satz } 18
  - 3.3.3 Der Schoof-Algorithmus } 18

§ 4 Sichere Kryptographie mit elliptischen Kurven

- § 4.1 Bekannte Angriffe auf das DL-Problem: Überblick } 19
  - 4.1.1 BSGS und Silver-Pohlig-Hellman } 19
  - 4.1.2 Pollard- $\rho$  und Pollard- $\lambda$  } 19
  - 4.1.3 MOV und SSSA } 19
  - 4.1.4 Fazit: geeignete elliptische Kurven und Vergleich mit anderen Public-Key-Verfahren } 19
- § 4.2 ElGamal für elliptische Kurven } 20
- § 4.3 ECDSA-Signaturen } 20
- § 4.4 Patente, Standards, Schlussbemerkungen } 21
  - $\rightsquigarrow$  Plus: Wiederholung und Prüfungs Vorbereitung } 21