

Kurzes Inhaltsverzeichnis

Kryptologie:

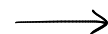
- K1: Einführung, Kryptologie, Enigma
- K2: Grundlagen aus der elementaren Zahlentheorie
- K3: Grundlegendes zu Gruppen
- K4: Public-Key-Kryptographie
- K5: El-Gamal-Verschlüsselung und -Signatur

Algorithmische Zahlentheorie:

- K6: Quadratische Reste und Kongruenzen
- K7: Primzahltests, Pseudo-Primzahlen
- K8: AKS- bzw. LP-Primzahltest
- K9: Faktorisierung mit Kettenbrüchen
- K10: Faktorisierung am Quantencomputer
- K11: DL-Problem am Quantencomputer
- K12: Grovers Algorithmus am QC

Elliptische Kurven-Arithmetik:

- K13: Grundlagen: Polynome und endliche Körper
- K14: Affine und projektive Ebene
- K15: Projektive Kurven
- K16: Der Satz von Bézout
- K17: Weierstraßform elliptischer Kurven
- K18: Das Diskriminantenkriterium
- K19: Die Gruppenstruktur elliptischer Kurven
- K20: Assoziativgesetz für elliptische Kurven
- K21: Schnelle Arithmetik auf elliptischen Kurven



Kryptographische Eignung elliptischer Kurven:

K22: Elliptische Kurven über \mathbb{Q} und \mathbb{C}

K23: Elliptische Kurven über endlichen Körpern

K24: Der Schoof-Algorithmus

K25: Sichere Kryptographie mit elliptischen Kurven

K26: El Gamal für elliptische Kurven, ECDSA

K27: Angriffe auf ECC