

Programm zum Seminar über Kryptographie und elliptische Kurven

Vortrag Nr.9 findet im M104, alle übrigen Vorträge im M103 statt

- 1) Mi. 18.04., 12ct **Singer Carmen**
Grundlegendes zur Kryptographie.
Grundlegende Aufgabenstellungen und einfache Verschlüsselungstechniken (Caesar-Verschlüsselung, Blockchiffrierung), Grundidee der Public-Key-Kryptographie und der digitalen Signatur, RSA-Verschlüsselung
([R] 1.1,1.2,1.6, [W] 1,1.1, vgl. auch [B])
- 2) Mi. 25.04., 12ct **Wilhelm Marika**
Elementare zahlentheoretische Algorithmen und deren Komplexität.
Schnelle zahlentheoretische Algorithmen (euklidischer Algorithmus, ggT, Potenzieren, wahrscheinliche Primzahlen), langsame Algorithmen (Primfaktorzerlegung, diskreter Logarithmus), Diffie-Hellman-Schlüsselaustausch
([R] 1.3-1.5)
- 3) Mi. 02.05., 12ct **Hetterich Kathrin**
Verschlüsselungsmethoden und Angriffe.
ElGamal-Verschlüsselung und ElGamal-Signatur, Algorithmen für das diskrete Logarithmus-Problem (naiv, baby-step-giant-step, Pohlig-Hellman-Verfahren, Pollard-Methoden, Index-Calculus)
([W] 1.2.2,1.2.3,4.1, [R] 5.7.1, Kap. 6)
- 4) Mi. 09.05., 12ct **Kandsperger Michael**
Affiner und projektiver Raum, affine Kurven.
Der affine Raum $\mathbb{A}^n(k)$ und der projektive Raum $\mathbb{P}^n(k)$ für einen Körper k , Zerlegung von $\mathbb{P}^n(k)$ in unendlich ferne Hyperebene und $\mathbb{A}^n(k)$, affine Kurven
([R] 2.1-2.3, [W] 2.1)
- 5) Mi. 16.05., 12ct **Karl Michaela**
Ebene projektive Kurven.
Ebene projektive Kurven, Geometrische Addition und Gruppenstruktur ebener Kubiken
([R] 2.4,3.1,3.2, [W] 2.2)
- 6) Mi. 23.05., 12ct **Dudenaite Virginija**
Elliptische Kurven.
Definition, Weierstraß-Gleichung, Normalform der Weierstraß-Gleichung, Diskriminante
([R] 4.1-4.3, [W] 2.3, [S] Kap. III)
- 7) Mi. 23.05., 18st **Wiener Amelie**
Elliptische Kurven über \mathbb{C} .
Gitter und doppelt-periodische meromorphe Funktionen, elliptische Kurven über \mathbb{C}
([R] 9.1, [S] Kap. VI)
- 8) Mi. 30.05., 12ct **Baranyi Lenuta**
Die j -Invariante und der Isomorphietyp.
Definition der j -Invariante, Beweis, dass diese den Isomorphietyp über dem algebraischen Abschluß von k festlegt, Isomorphieklassen für nicht algebraisch abgeschlossenes k
([R] 4.3-4.5, [S] Kap. III §1)
- 9) Mo. 04.06., 18st **Prester Johannes**
Der Endomorphismenring.
Bestimmung des Endomorphismenrings, Komplexe Multiplikation und supersinguläre elliptische Kurven
([R] 9.3, [S] Kap. III)
- 10) Mi. 06.06., 12ct **Melzer Sabine**
Punkte auf elliptischen Kurven über \mathbb{F}_q .
Das Legendre-Symbol, Quadratisches Reziprozitätsgesetz, Formel für Anzahl der Punkte von $E(\mathbb{F}_q)$, Satz von Hasse zitieren (ohne Beweis)
([R] 5.1-5.3)

- 11) Mi. 13.06., 12ct **Umirova Julia**
Der Frobenius-Endomorphismus.
 Frobenius-Endomorphismus für eine elliptische Kurve über \mathbb{F}_p , Tate-Modul, spezielle Aussagen für supersinguläre elliptische Kurven
 ([W] 3.1,3.2,3.4, [R] 9.4)
- 12) Mi. 13.06., 18st **Bannach Andreas**
Bestimmung von $\#E(\mathbb{F}_p)$ in speziellen Fällen.
 Bestimmung von $\#E(\mathbb{F}_p)$ für elliptische Kurven mit spezieller j -Invariante
 ([R] 9.5-9.7)
- 13) Mi. 20.06., 12ct **Schreiner Sabine**
Verschlüsselungsverfahren mit elliptischen Kurven I.
 Praktische Implementation von Verschlüsselungen mit elliptischen Kurven: Algorithmus zum Bestimmen eines Punktes, Einbetten von Text in elliptische Kurve, Hash-Funktionen und Verschlüsselungsverfahren PSEC-1
 ([R], 5.4-5.6, Kap. 7)
- 14) Mi. 27.06., 12ct **Lehmer Andrea**
Verschlüsselungsverfahren mit elliptischen Kurven II.
 Digitale Signaturen, elliptisches ElGamal-Verfahren, DSA und ECDSA
 ([R] Kap. 8, [W] 5.3)
- 15) Mi. 04.07., 12ct **Schweinfurter Michael**
Berechnung von $\#E(\mathbb{F}_p)$.
 Allgemeine Algorithmen, Algorithmus nach Schoof
 ([R], Kap. 10, [W] 3.3)
- 16) Mi. 11.07., 12ct **Märtl Florian**
Weil-Paarung und das MOV-Verfahren.
 Definition und Grundlegendes zur Weil-Paarung, das MOV-Verfahren zur effektiven Berechnung des diskreten Logarithmus auf supersingulären elliptischen Kurven
 ([W] 4.2.1, [R], 11.1)
- 17) Mi. 18.07., 12ct **Umirova Natalya**
Anomale Kurven und der SSSA-Algorithmus.
 anomale Kurven, der SSSA-Algorithmus zur Berechnung des diskreten Logarithmus auf anomalen Kurven
 ([W] 4.2.2, [R], 11.2)

Literatur

- [B] J. Buchmann, *Einführung in die Kryptographie*, Springer-Verlag, 1999
- [K] E. Kunz, *Einführung in die algebraische Geometrie*, vieweg-Verlag, 1997
- [R] W. Ruppert, *Elliptische Kurven und Kryptographie*, Vorlesungsskript Sommersemester 2003
 Universität Erlangen, kann unter <http://www.uni-erlangen.de/~ruppert/skripten/ekk.ps.gz> als
 gzipped-Postscript heruntergeladen werden.
- [S] J. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, 1986, Grad. Texts in Math. 106
- [W] A. Werner, *Elliptische Kurven in der Kryptographie*, Springer-Verlag, 2002