Seminar "Verschlüsselungs- und Codierungstheorie" 2018

PD Dr. T. Timmermann

1. (09./11.4.) *Theresa Kranz/Fenna Harms*

Der Chinesische Restsatz erweiterter euklidischer Algorithmus; Rechnen mit Restklassen; prime Restklassengruppe und Eulersche ϕ-Funktion; chinesischer Restsatz über simultane Kongruenzen; evt. Anwendung auf Carmichael-Zahlen [Buc16, §1.6, §2.8, §2.15, §7.3]

2. (16./18.4.) *Marcel Schoppmeier/Nicole Becker*

Der kleine Satz von Fermat und das RSA-Verfahren Ordnung von Gruppenelementen; der kleine Satz von Fermat; Prinzip der Public-Key Verschlüsselung; das RSA-Verfahren: Ver- und Entschlüsselung; evt. schnelle Exponentiation; evt. Bemerkungen zur Sicherheit [Buc16, 2.8–2.12, §8.3], [Wil08, S. 76–78]

3. (23./25.4.) *Niklas Pieper/Jonah Samson*

Verschlüsselung mittels diskreter Logarithmen diskrete Logarithmen, Diffie-Hellman-Schlüsselaustausch, Diffie-Hellman-Problem; ElGamal-Verfahren; Pohlig-Hellman-Algorithmus [Buc16, §8.6–8.7, §10.5], [Wil08, S. 78–80, §16]

4. (30.4./02.5.) *Johanna Döller/Eileen Bartl*

Verschlüsselung mittels elliptischer Kurven Was ist eine elliptische Kurve; Gruppenstruktur: geometrische und algebraische Beschreibung; Satz von Hasse ohne Beweis [Buc16, §13.2], [Wil08, §15]

5. (07./09.5.) *Oliver Lappenküper/Sarah Pinkhaus*

Der Chinesische Restsatz für Ringe Produkte von Ringen; Ringhomomorphismen; Zerlegung des Restklassenringes; Ideale, Hauptideale und Quotientenringe; der allgemeine chinesische Restsatz [Buc16, §2.16], [Bos13, §2.3]

6. (14./16.5.) *Ekaterini Karanassiou/Julia Cleven*

Endliche Körper Charakteristik, Primkörper und Anzahl der Elemente eines endlichen Körpers; Polynomdivision mit Rest; irreduzible Polynome und Zerfällungskörper; multiplikative Gruppe eines endlichen Körpers ist zyklisch [Buc16, §2.19, 2.20], [Man17, §5.1], [Wil08, §22]

7. (28./30.5.) *Monika Schäfter/Felix Schmidt*

Grundbegriffe der Codierungstheorie Grundproblem der Codierung; Block-Codes und Hamming-Metrik; Parameter eines Block-Codes; Hamming-Schranke; evt. Singleton-Schranke; Beispiele (Paritätscheck, ISIN-Code, EAN-Code, ISBN-Code) [Wil08, §1]; siehe auch [Man17, §1]

8. (04./06.6.) *Theresa Roßkamp/Lisa Rensing*
Lineare Codes Lineare Codes, Minimalgewicht, Rate; Erzeuger- und Kontrollmatrix; Beispiele; erweiterter und dualer Code; Hamming- und Simplex-Code [Man17, §2.2, 2.3, 3.1], [Wil08, S. 15–17]

9. (11./13.6.) *Aurelia Bröskamp/Menuja Jeyalavathas*
Kodierung und Dekodierung linearer Codes Systematische Kodierung; Syndrom-Dekodierung; Hamming-Dekodierung [Man17, 2.4, 2.5, 3.2, 3.3.2–3.3.4], [Wil08, S. 18–19]

10. (18./20.6.) *Jonathan Wille/Alexander Westhölter*
Beispiele linearer Codes binäre Golay-Codes; Plotkin-Konstruktion und binäre Reed-Muller-Codes [Man17, 3.3, 3.4, 4.1, evt. 4.2], [Wil08, S. 21–23]

11. (25./27.6.) *Johanna Hartmann/Tabea Emans*
Zyklische Codes Zyklische Codes; Erzeuger- und Kontroll-Polynom; Erzeuger- und Kontrollmatrizen; einfache Beispiele zyklischer Codes [Buc16, §2.19], [Man17, §6.1], [Wil08, S. 47–50]

12. (02./04.7.) *Lena Flathmann/Leonie Lenders*
Reed-Solomon-Codes Konstruktion von endlichen Körpern als Restklassen bezüglich eines irreduziblen Polynoms; Reed-Solomon-Codes; Beispiele und Anwendungen [Buc16, §2.20], [Man17, §5.1.2, §5.2, §5.3], [Wil08, S. 20]

13. (09./11.7.) *Simon Pehle/Mona Knab*
Mehr über zyklischer Codes ODER Faltungscodes Kodierung und CRC-Kodierung; zyklische Reed-Solomon-Codes; BCH-Schranke [Man17, §6.3.1, 6.3.3, 6.5.3, 7.1], [Wil08, S. 49–52], [Buc16, §2.21]

Literatur

[Bos13] Siegfried Bosch. *Algebra.* Berlin: Springer, 8th corrected ed. edition, 2013. `http://link.springer.com/book/10.1007/978-3-662-05648-6`.

[Buc16] Johannes Buchmann. *Einführung in die Kryptographie.* Heidelberg: Springer Spektrum, 6th revised edition edition, 2016. `http://link.springer.com/book/10.1007/978-3-642-39775-2`.

[Man17] Olaf Manz. *Fehlerkorrigierende Codes. Konstruieren, Anwenden, Decodieren.* Wiesbaden: Springer Vieweg, 2017. `http://link.springer.com/book/10.1007/978-3-658-14652-8`.

[Wil08] Wolfgang Willems. *Codierungstheorie und Kryptographie.* Basel: Birkhäuser, 2008. `http://link.springer.com/book/10.1007/978-3-7643-8612-2`.