Prof. Dr. W. Bley 08.10.2021

Seminar zur Kryptographie (WS 21/22)

Vorkenntnisse: Lineare Algebra, eventuell Algebra, Grundkenntnisse zum Quanten-Computing wie in meiner Vorlesung vom SS 2021.

Das Seminar findet jeweils am Donnerstag, 16:15 - 17:45 Uhr, im Raum B 252 statt.

Erster Vortrag am 28.10.2021

Programm / Vorträge

- 1. Vortrag: noch frei
  Das quadratische Sieb
  Literatur: [3, Kapitel 20] und [5, Ch. 10.4].
- 2. Vortrag: Willberger
  Diskreter Logarithmus, Diffie-Hellman-Schlüsselaustausch und ElGamal-Verschlüsselungsverfahren
  Literatur: [3, Kapitel 21] und [4, Kap. 7.5 und 7.6].
- 3. Vortrag: Bley
  Shors Algorithmus und Anwendung auf das DL-Problem und Faktorisierung
  Literatur: [1, Kap. 5.4].
- 4. Vortrag: Bley
  Hidden Subgroup Problem
  Literatur: [1, Kap. 5.4] und [2, Quantum Computing by Hallgren/Vollmer].
- 5. und 6. Vortrag: Albrecht, Neumaier
  Quadratische Zahlkörper, Klassengruppe und Fundamentaleinheit, elementare Algorithmen zur Bestimmung von Klassengruppe und Fundamentaleinheit
  Literatur: [3, Kapitel 24 und 28]
- 7. Vortrag: Bley
  Buchmanns Sub-exponentieller Algorithmus
  Literatur: [5, Kap. 5.5 und 5.9].
- 8. und 9.Vortrag: Brenner
  Polynomielle Quantum-Algorithmen zur Berechnung von Klassengruppe und Fundamentaleinheit
  Literatur: [5].
- 11. und 12. Vortrag: Griesser
  Lattice-based Cryptography und Multivariate Public Key Cryptography
  Literatur: entsprechende Kapitel in [2].

Literatur:

1 Chuang/Nielsen, Quantum Computation and Quantum Information

2 Bernstein/Buchmann/Dahmen, Post-Quantum Cryptography

3 Forster, Algorithmische Zahlentheorie

4 Buchmann, Einführung in die Kryptographie

5 Cohen, A course in computational algebraic number theory

6 Sean Hallgren, Polynomial-Time Quantum Algorithms for Pells Equation and the Principal Ideal Problem