

WP- & SP-Module im Bachelor & Master Informatik

Komplexitätstheorie & Kryptologie

Computational Social Choice

Algorithmische Spieltheorie

Dozent: Prof. Dr. J. Rothe



Unser Team im SS 2012



Prof. Dr. Jörg Rothe



Dorothea Baumeister



Magnus Roos



Lena Schend



Anja Rey



Trung Thanh Nguyen

Modul: Kryptokomplexität I (Bachelor)

- **Einführung in die Kryptologie**

Aufgaben und Ziele der Kryptologie

Einige klassische Kryptosysteme und
ihre Kryptoanalyse

Perfekte Geheimhaltung

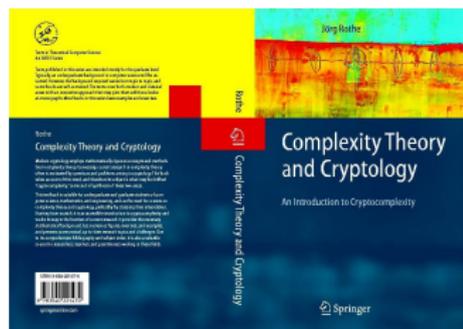
RSA

- **Primzahltests**

- **Einführung in die Komplexitätstheorie**

Grundlagen

Zwischen L und PSPACE



Modul: Kryptokomplexität II (Master)

- **Vertiefung der Kryptologie**

Diffie-Hellman und diskrete Logarithmen

Die Protokolle von ElGamal

Rabins Public-Key Kryptosystem

Arthur-Merlin-Spiele und Zero-Knowledge

Das Kryptosystem von Merkle und Hellman

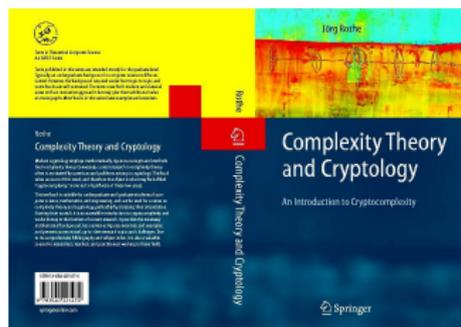
- **Randomisierte Algorithmen**

- **Vertiefung der Komplexitätstheorie**

Die Boolesche Hierarchie über NP

Die Polynomialzeit-Hierarchie

Alternierende Turingmaschinen



Halbmodule: Primzahltests & Randomisierung (Master)

- **Halbmodul: Primzahltests und das Faktorisierungsproblem**

Einige zahlentheoretische Grundlagen

Primalitätstests

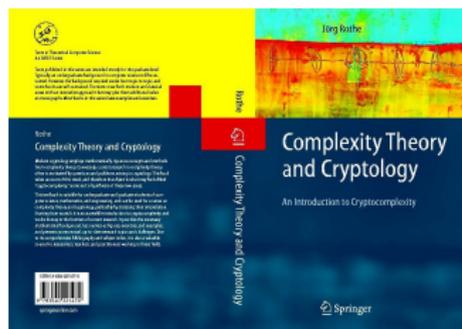
Das Faktorisierungsproblem

- **Halbmodul: Randomisierte Algorithmen und Komplexitätsklassen**

Randomisierte SAT-Algorithmen

Probabilistische Polynomialzeitklassen

Quantoren und Arthur-Merlin-Spiele



Computational Social Choice? Wahlen? Piraten?



Computational Social Choice? Wahlen? Piraten?



Halbmodul: Algorithmische Eigenschaften von Wahlsystemen I (Bachelor)

- **Grundlagen der Social-Choice-Theorie**

Wahlsysteme und einige ihrer Eigenschaften

Einige weitere Wahl-Paradoxa

Einige Unmöglichkeitssätze

- **Manipulation**

Konstruktive Manipulation

Destruktive Manipulation

- **Wahlkontrolle**

Immunität, Verletzbarkeit und Resistenz

Kontrollkomplexität

Buchtitel: 175 x 225 mm · Abstand: 6 mm

J. Rothe D. Baumeister C. Lindner I. Rothe

Einführung in Computational Social Choice

Individuelle Strategien und kollektive
Entscheidungen beim Spielen, Wählen und Teilen



ISBN von DGB
2570 St. Nr. 14, 01.9.2013 7:20
ISBN von DGB
2570 St. Nr. 14, 01.9.2013 7:20
ISBN von DGB
2570 St. Nr. 14, 01.9.2013 7:20

Buchtitel:
Bibliografie: Autor/Sprache:
Bibliografie:
ISBN von DGB
2570 St. Nr. 14, 01.9.2013 7:20

ISBN von DGB
2570 St. Nr. 14, 01.9.2013 7:20
ISBN von DGB
2570 St. Nr. 14, 01.9.2013 7:20

Halbmodul: Cake-cutting Algorithms (Master)

- **Grundlagen**

- **Bewertungskriterien**

Fairness & Effizienz

Manipulation & Laufzeit

- **Cake-cutting-Protokolle**

Proportionale Protokolle

Neidfreie Protokolle

Aufteilung in ungleiche Anteile

Dirty-Work-Protokolle

Minimierung der Schnittanzahl

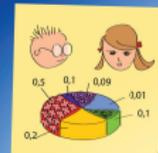
Grad der garantierten Neidfreiheit

Buchtitel 195 x 220 mm · Abstand 6 mm

J. Rothe D. Baumeister C. Lindner I. Rothe

Einführung in Computational Social Choice

Individuelle Strategien und kollektive
Entscheidungen beim Spielen, Wählen und Teilen



Spektrum
LEHRBÜCHER

ISBN von 978-3-7089-2310-1
2019, 16. Aufl., 31.9.2019
Permanenter digitaler Ausdruck
978-3-7089-2310-1
design@spektrum.de 20190316a

Buchreihe
Wissenschaftlicher Fachbereich
Bücherei
Anmeldung gegenüber Universitätsbibliothek

1. Auflage
1. Auflage
1. Auflage
1. Auflage
1. Auflage

