Seminar »Kryptographie und Komplexität«

Prof. Johannes Köbler Sebastian Kuhnert

Wintersemester 2010/2011

In diesem Seminar werden aktuelle Themen der Theoretischen Informatik, insbesondere der Komplexitätstheorie und der Kryptologie behandelt. Hierbei gehen wir auch gern auf Teilnehmerwünsche ein.

In diesem Semester wollen wir uns schwerpunktmäßig den Themen Pseudozufallsgeneratoren und Derandomisierung widmen. Die Erzeugung von Bitfolgen mit »zufälligen« Eigenschaften besitzt zahlreiche Anwendungen in der Kryptografie. Darüber hinaus sind Pseudozufallsgeneratoren ein zentrales Konzept der modernen Komplexitätstheorie, welches u. a. für die Derandomisierung probabilistischer Komplexitätsklassen genutzt werden kann.

Vorkenntnisse aus der Kryptographie und/oder Komplexitätstheorie sind zum Besuch dieses Seminars nützlich, jedoch nicht unabdingbar.

Themen für Referate

Im Seminar sind Vorträge einführenden und vertiefenden Charakters zu folgenden Themenbereichen geplant:

1. **Äquivalenz der Existenz von schwachen und starken Einwegfunktionen.** Schwache Einwegfunktionen sind manchmal schwer zu invertieren, starke Einwegfunktionen fast immer.

   Inhalt: Wie sind Einwegfunktionen genau definiert? Wie kann aus einer schwachen Einwegfunktion eine starke konstruiert werden?

   Literatur: [AB09, Kapitel 9], [Gol01, Kapitel 2]

2. **Pseudozufallsgeneratoren: Ununterscheidbarkeit und Unvorhersagbarkeit.** Ein Pseudozufallsgenerator ist eine Funktion, die aus einer kurzen, zufällig zu wählenden Eingabe eine längere, zufällig aussehende Ausgabe berechnet.

   Inhalt: Wie können Pseudozufallsgeneratoren durch Ununterscheidbarkeit und Unvorhersagbarkeit definiert werden? Warum sind beide Definitionen äquivalent?

   Literatur: [AB09, Kapitel 9]

3. **Äquivalenz der Existenz von Einwegfunktionen und Pseudozufallsgeneratoren.**

   Inhalt: Warum gibt es genau dann Einwegfunktionen, wenn es Pseudozufallsgeneratoren gibt?

   Literatur: [AB09, Kapitel 9]

4. **Derandomisierung von probabilistischen Komplexitätsklassen.** Neben der Komplexitätsklasse P, die effiziente deterministische Berechenbarkeit charakterisiert, hat sich die Klasse BPP zur Beschreibung von effizienten probabilistischen Berechnungen etabliert.

   Inhalt: Wie ist BPP genau definiert? Unter welchen Voraussetzungen kann $\mathsf{BPP} = \mathsf{P}$ gezeigt werden?

   Literatur: [AB09, Kapitel 7 und 20]

5. **Extraktoren** können selbst aus nur schwach zufälligen Quellen brauchbare Zufallszahlen erzeugen.

   Inhalt: Wie lassen sich Extraktoren genau definieren? Wie können sie konstruiert werden? Wie können sie zur Derandomisierung verwendet werden?

   Literatur: [AB09, Kapitel 20]

6. **Elektronisches Geld.**

   Inhalt: Wie kann durch kryptographische Methoden beim Bezahlen im Internet die von Bargeld gewohnte Anonymität hergestellt werden, ohne dass digitale »Münzen« beliebig kopiert werden können?

   Literatur: [Mol02, Kapitel 7], [TW05, Kapitel 11]

Ablauf

- In der ersten Woche stellen wir euch die Referatsthemen vor und ihr wählt euer Thema aus. Außerdem geben wir euch Hinweise zur Gestaltung von Referaten und Ausarbeitungen.
- Im Lauf des Semesters haltet ihr **Referate**
  - Die Referate haben das Ziel, dass ihr (a) euch ein Thema erarbeitet, (b) euer Thema den anderen vermittelt, (c) von den Referaten der anderen lernt und (d) Vortragspraxis sammelt.
  - Einerseits sollen eure Referate *anschaulich* sein: Ihr führt die anderen in euer Thema ein. Bitte setzt dabei nicht mehr voraus, als sie schon wissen. Mit Beispielen und Bildern könnt ihr euren Zuhörern das Verstehen erleichtern. Eine gute Richtschnur für gute Erklärungen ist die Frage »Was hat mir selbst geholfen, das zu verstehen?«
  - Andererseits sollen eure Referate auch *präzise* sein: Klare Definitionen und die Details von Konstruktionen und Algorithmen gehören auch dazu.
  - Für euer Referat stehen euch ca. 90 Minuten zur Verfügung. Bitte plant Zeit für Rückfragen ein!
- **Vorbereitung** des eigenen Referats:
  - Ihr arbeitet euch in das Thema ein, indem ihr die angegebene (und ggf. weitere) Literatur lest. Literatur, die es nicht in der Bibliothek oder im Netz gibt, kann bei uns kopiert werden.
  - Vor der Vorbereitung des Vortrags lest ihr am besten [TWM10, Abschnitt 5] – das lohnt sich auch dann, wenn ihr nicht LaTeX verwendet.
  - Eine Woche vor dem Referat kommt ihr in unsere Sprechstunde, um letzte Verständnisfragen zu stellen und den Ablauf des Referats durchzusprechen.
- Es ist ein zentrales Element eines Seminars, auch von den Referaten der anderen zu lernen. Deshalb solltet ihr möglichst immer **anwesend sein**. Wenn ihr mehr als einmal fehlt, zeigt uns bitte unaufgefordert ein Attest.
- Nach dem Referat fertigt ihr noch eine schriftliche **Ausarbeitung** zu eurem Thema an.
  - Die Ausarbeitungen haben das Ziel, (a) das im Seminar gesammelte Wissen zusammenzufassen, (b) Interessierten einen Einstieg in euer Thema zu ermöglichen und (c) euch die Gelegenheit zu geben, wissenschaftliches Schreiben zu üben (Vorbereitung auf Studien- und Diplomarbeit).
  - Wir werden eure Ausarbeitungen auf der Webseite des Seminars veröffentlichen, wenn ihr damit einverstanden seid.
  - Eure Ausarbeitung sollte ungefähr 10-20 Seiten umfassen.
  - Hinweise zum wissenschaftlichen Schreiben findet ihr unter [Böt06] und [Mit07].

Literatur

[AB08] Sanjeev Arora and Boaz Barak. *Computational complexity. A modern approach.* Web draft of [AB09]. Princeton University, 2008. URL: http://www.cs.princeton.edu/theory/index.php/Compbook/Draft (visited on Sept. 3, 2010).

[AB09] Sanjeev Arora and Boaz Barak. *Computational complexity. A modern approach.* Cambridge University Press, 2009. ISBN: 978-0-521-42426-4. Web draft: [AB08].

[Böt06] Martin Böttcher. *Einführung in das wissenschaftliche Arbeiten.* Universität Leipzig. 2006. URL: http://bis.informatik.uni-leipzig.de/de/Lehre/0506/SS/SemASKE/files?get=einfuehrung_in_das_wiss_arbeiten.pdf (besucht am 3. Sep. 2010).

[Gol01] Oded Goldreich. *Foundations of cryptography.* Vol. 1: Basic Tools. Cambridge University Press, 2001. ISBN: 0-521-79172-3.

[Mit07] Roland Mittermair. *Hinweise für korrektes Zitieren.* Institut für Informatik-Systeme, Universität Klagenfurt. 2007. URL: http://www.uni-klu.ac.at/tewi/downloads/Zitierhinweise.pdf (besucht am 3. Sep. 2010).

[Mol02] Richard A. Mollin. *RSA and public key cryptography.* Boca Raton, Florida: Chapman & Hall/CRC, 2002. ISBN: 1-58488-338-3.

[TW05] Wade Trappe and Lawrence C. Washington. *Introduction to cryptography with coding theory.* 2nd ed. Pearson Prentice Hall, 2005. ISBN: 0-13-198199-4.

[TWM10] Till Tantau, Joseph Wright, and Vedran Miletić. *The* BEAMER *class.* Version 3.10. 2010. URL: http://mirror.ctan.org/macros/latex/contrib/beamer/doc/beameruserguide.pdf (visited on Sept. 3, 2010).