Seminar Komplexität und Kryptologie

Prof. Johannes Köbler Sebastian Kuhnert

Sommersemester 2013

In diesem Seminar werden aktuelle Forschungsthemen der Gebiete Komplexitätstheorie und Kryptografie vorgestellt und diskutiert. Hierbei gehen wir auch gern auf Teilnehmerwünsche ein. Das Seminar eignet sich sowohl zum Einstieg in das Gebiet als auch hervorragend zur Vorbereitung auf Diplom- oder Bachelorarbeit.

Themen für Referate

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

1. **Asymmetrische Kryptosysteme:** Wie können zwei Partien Nachrichten über einen abhörbaren und manipulierbaren Kanal sicher austauschen, ohne zuvor einen Schlüssel über einen abhörsicheren Kanal zu vereinbaren?

   Inhalt: Wie lassen sich mit asymmetrischen Kryptosystemen Verschlüsselung und Signatur realisieren? Wie funktioniert das RSA-System? Was ist über die Sicherheit von RSA bekannt?

   Literatur: [Wät08, Kapitel 5]

2. **Schlüsselaustausch und Zertifikate:** Um moderne Verschlüsselungsverfahren einsetzen zu können, müssen zuvor die zu verwendenden Schlüssel sicher ausgetauscht werden.

   Inhalt: Wie kann mit dem Diffie-Hellman-Verfahren ein symmetrischer Schlüssel über einen abgehörten (aber manipulationssicheren) Kanal vereinbart werden, sodass am Ende nur die beiden Kommunikationspartner ihn kennen? Wie kann dies durch den Einsatz von Zertifikaten auch über manipulierbare Kanäle erreicht werden?

   Literatur: [Wät08, Kapitel 8]

3. **Anonymes elektronisches Geld:** Wie kann ein elektronisches Bezahlsystem aussehen, in dem Falschgeld unmöglich ist und Käufer dennoch anonym bleiben?

   Inhalt: Was sind blinde Signaturen? Wie können diese verwendet werden, um anonymes elektronisches Geld zu realisieren?

   Literatur: [Wät08, Kapitel 10.5]

4. **Interaktive Beweissysteme 1:** Können mehr Aussagen bewiesen werden, wenn man Interaktion zwischen Beweiser und Überprüfer zulässt?

   Inhalt: Wie kann man interaktive Beweise formalisieren? Wie kann ein interaktives Beweissystem für Nichtisomorphie von Graphen aussehen? Warum spielt es keine Rolle, ob der Beweiser dem Überprüfer beim Würfeln zuschauen kann?

   Literatur: [AB09, Kapitel 8.1–8.2]

5. **Interaktive Beweissysteme 2:**

   Inhalt: Warum gilt $\mathsf{IP} = \mathsf{PSPACE}$?

   Literatur: [AB09, Kapitel 8.3]

6. **Zero Knowledge Proofs:** Wie kann man jemand anderes davon überzeugen, dass man über geheimes Wissen verfügt, ohne dieses zu offenbaren?

   Inhalt: Wann haben interaktive Beweissysteme die Zero-Knowledge-Eigenschaft? Wie funktioniert Bit-Commitment? Warum gibt es für jede Sprache in NP Zero Knowledge Proofs?

   Literatur: [Wät08, Kapitel 11]; ergänzend: [Gol01, Kapitel 4.3 und 4.4.2]

7. **Secret Sharing Schemes:** Wie kann man ein Geheimnis unter n Personen so aufteilen, dass mindestens k von ihnen zusammenkommen müssen, um es zu rekonstruieren?

   Inhalt: Wie lassen sich Secret Sharing Schemes formalisieren? Wie können sie implementiert werden? Wie kann durch Einsatz visueller Kryptographie die Rekonstruktion des Geheimnisses erleichtert werden?

   Literatur: [Wät08, Kapitel 15.1], [NS95]

8. **Platzeffiziente Algorithmen:** Wie leistungsfähig sind nichtdeterministische Turingmaschinen, die nur logarithmisch viel Platz auf dem Arbeitsband verwenden dürfen?

   Inhalt: Warum ist Reach (Erreichbarkeit in gerichteten Graphen) vollständig für NL? Warum ist 2Sat (Erfüllbarkeit von KNF-Formeln, in denen jede Klausel höchstens 2 Literale enthält) vollständig für NL?

   Literatur: [AB09, Kapitel 4.3], [Rot08, Kapitel 3.5.2]

9. **Boolesche Schaltkreise**

   Inhalt: Wie kann eine deterministische Turingmaschinen einen NC^1-Schaltkreis (logarithmische Tiefe, polynomielle Größe, nur 2 Eingänge pro Gatter) simulieren? Wie kann ein AC^1-Schaltkreis (logarithmische Tiefe, polynomielle Größe, beliebig viele Eingänge pro Gatter) eine nichtdeterministische Turingmaschine mit logarithmischer Platzschranke simulieren?

   Literatur: [Sav98, Kapitel 8.13 und 8.15]

10. **Untere Schranken:** Eine Möglichkeit um $\mathsf{P} \neq \mathsf{NP}$ zu zeigen, ist eine Sprache in NP anzugeben, die nicht durch Boolesche Schaltkreise polynomieller Größe entschieden werden kann. Bisher sind aber nur überraschend schwache untere Schranken für die Schaltkreisgröße von Funktionen bekannt.

    Inhalt: Warum kann die Paritätsfunktion nicht durch AC^0-Schaltkreise (konstante Tiefe, polynomielle Größe) entschieden werden?

    Literatur: [AB09, Kapitel 14.1]

Ablauf

- In der ersten Vorlesungswoche 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!
  - Nach jedem Referat gibt es eine Feedbackrunde.
- **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 [TWM13, 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 Abschlussarbeiten).
  - Der Umfang eurer Ausarbeitung soll dem Umfang eures Referats entsprechen. Erfahrungsgemäß ergibt das 10–20 Seiten.
  - Hinweise zum wissenschaftlichen Schreiben findet ihr unter [Böt06] und [Mit07].
  - Der **Abgabeschluss** für Ausarbeitungen ist der erste Tag der Vorlesungszeit im folgenden Semester.

Literatur

[AB09] Sanjeev Arora and Boaz Barak.
Computational complexity. A modern approach.
Cambridge University Press, 2009.

[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.

[BSW06] Albrecht Beutelspacher, Jörg Schwenk und Klaus-Dieter Wolfenstetter.
Moderne Verfahren der Kryptographie. Von RSA zu Zero-Knowledge.
6. Aufl. Wiesbaden: Vieweg, 2006.

[Gol01] Oded Goldreich. *Foundations of cryptography.* Vol. 1: Basic Tools.
Cambridge University Press, 2001.

[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.

[NS95] Moni Naor and Adi Shamir. 'Visual cryptography'.
In: *Advances in Cryptology – EUROCRYPT'94.* Berlin: Springer, 1995, pp. 1–12. DOI: 10.1007/BFb0053419.
URL: http://www.wisdom.weizmann.ac.il/~naor/PAPERS/vis.ps.

[Rot08] Jörg Rothe. *Komplexitätstheorie und Kryptologie. Eine Einführung in Kryptokomplexität.* Berlin: Springer, 2008.
DOI: 10.1007/978-3-540-79745-6.

[Sav98] John E. Savage.
Models of computation. Exploring the power of computing.
Reading, Mass.: Addison-Wesley, 1998.
URL: http://www.modelsofcomputation.org.

[TWM13] Till Tantau, Joseph Wright, and Vedran Miletić. *The* BEAMER *class.*
Version 3.26. 4, 2013. URL: http://mirror.ctan.org/macros/latex/contrib/beamer/doc/beameruserguide.pdf.

[Wät08] Dietmar Wätjen. *Kryptographie. Grundlagen, Algorithmen, Protokolle.*
2. Aufl. Heidelberg: Spektrum Akademischer Verlag, 2008.