Seminar Komplexität und Kryptographie

Kryptographische Protokolle

Prof. Johannes Köbler Sebastian Kuhnert

Wintersemester 2008/09

Mittwoch 13:15–14:45, RUD 25, 4.112

Kryptographische Protokolle schaffen Vertrauen in ungeschützten Umgebungen: Sie ermöglichen sichere Kommunikation über unsichere Kanäle und können verhindern, dass sich ein Kommunikationspartner unfair verhält.

In unsicheren Umgebungen wie dem Internet können sie die aus direkter Interaktion gewohnte Sicherheit herstellen. Und auch die Interaktion in sicheren Umgebungen wird um Möglichkeiten erweitert, die ohne Kryptographie nicht denkbar wären.

In diesem Seminar werden wir uns mit kryptographischen Protokollen beschäftigen, mit denen Informationen in unterschiedlichen Situationen geschützt werden können.

Themen für Referate

1. **Bit-Commitment:** Wie kann man jemanden davon überzeugen, dass man seine Meinung nicht ändern wird, ohne dass man seine Meinung sofort verraten muss?

   Inhalt: Was genau wird unter Bit-Commitment verstanden? Welche Anwendungen gibt es dafür? Wie lässt sich Bit-Commitment mithilfe eines Pseudozufallsgenerators realisieren?

   Literatur: [BSW99, Kapitel 2.6, 3.8], [Nao91]

2. **Oblivious Transfer:** Wie kann man einer anderen Person eine von zwei Informationen übermitteln, ohne dass diese die andere Information erfährt und ohne dass man weiß, welche der beiden Informationen gewählt wurde?

   Inhalt: Welche Varianten von Oblivious Transfer gibt es? Wozu lassen sich diese verwenden? Warum sind die unterschiedlichen Definitionen äquivalent?

   Literatur: [BSW99, Kapitel 7.3], [Cré88]

3. **Schlüsselvereinbarung:** Wie können zwei Personen einen kryptographischen Schlüssel über einen Kanal vereinbaren, der abgehört oder sogar manipuliert werden kann?

   Inhalt: In welchen Szenarien müssen Schlüssel über einen unsicheren Kanal vereinbart werden? Wie kann das realisiert werden? Warum sind die vorgestellten Verfahren sicher?

   Literatur: [BSW99, Kapitel 3.4], [Sti06, Kapitel 10.1, 11.1-2]

4. **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 man unehrlichen Teilnehmern begegnen?

   Literatur: [BSW99, Kapitel 5.1], [Sha79], [TW89]

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

   Inhalt: Was sind interaktive Beweissysteme? Wann haben diese die Zero-Knowledge-Eigenschaft? Wie und warum funktioniert das Zero-Knowledge-Protokoll für Graph-Isomorphie? Warum existiert für alle NP-Sprachen ein Zero-Knowledge-Beweis?

   Literatur: [BSW99, Kapitel 4.1-4.3], [Gol01, Kapitel 4.3], [Gol07, Kapitel 9.2]

Ablauf

- 15.10.: Vorstellung und Vergabe der Referatsthemen
- Im Lauf des Semesters: **Referate**
  - Einerseits anschaulich: Einführung und Einordnung des Themas
  - Andererseits präzise: Definitionen und Beweise
  - Zeitlicher Rahmen: Jeweils 90 Minuten, Zeit für Rückfragen einplanen
- **Vorbereitung** des eigenen Referats:
  - In das Thema einarbeiten, Literatur lesen
  - Vortrag vorbereiten: [Tan07, Abschnitt 5] lesen – das lohnt sich auch, wenn nicht LaTeX verwendet wird
  - Eine Woche vor dem Referat: Sprechstunde nutzen, letzte Verständnisfragen stellen, Ablauf des Referats durchsprechen
- **Anwesenheit**: Auch von den Referaten der anderen lernen
  - Nicht mehr als einmal unentschuldigt fehlen
  - Ihr wollt euer Referat auch nicht vor einem leeren Raum halten
- Nach dem Referat: Schriftliche **Ausarbeitung**
  - Ziel: Unser im Seminar gesammeltes Wissen zusammenfassen
  - Können auf der Website veröffentlicht werden
  - Umfang: ca. 10-20 Seiten

Literatur

[BSW99] Albrecht Beutelspacher, Jörg Schwenk und Klaus-Dieter Wolfenstetter. *Moderne Verfahren der Kryptographie. Von RSA zu Zero-Knowledge.* 3. Aufl. Wiesbaden: Vieweg, 1999. ISBN: 3-528-26590-6.

[Cré88] Claude Crépeau. 'Equivalence Between Two Flavours of Oblivious Transfers'. In: *Advances in Cryptology. Proceedings of CRYPTO '87.* Lecture Notes in Computer Science 293. Berlin et al.: Springer, 1988. Pp. 350–354. ISBN: 978-3-540-18796-7. DOI: 10.1007/3-540-48184-2_30.

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

[Gol07] Oded E. Goldreich. *Complexity Theory. A Conceptual Perspective.* Draft of [Gol08]. Rehovot, Israel: Weizmann Institute, 2007. URL: http://www.wisdom.weizmann.ac.il/~oded/cc-drafts.html (visited on Aug. 8, 2008).

[Gol08] Oded E. Goldreich. *Computational Complexity. A Conceptual Perspective.* New York: Cambridge University Press, 2008. ISBN: 978-0-521-88473-0.

[Nao91] Moni Naor. 'Bit commitment using pseudorandomness'. In: *Journal of Cryptology* 4.2 (Jan. 1991). Pp. 151–158. ISSN: 0933-2790. DOI: 10.1007/BF00196774.

[Sha79] Adi Shamir. 'How to share a secret'. In: *Communications of the ACM* 22.11 (Nov. 1979). Pp. 612–613. ISSN: 001-0782. DOI: 10.1145/359168.359176.

[Sti06] Douglas Robert Stinson. *Cryptography. Theory and Practice.* 3rd ed. Boca Raton, Florida: Chapman & Hall/CRC, 2006. ISBN: 978-1-58488-508-4.

[Tan07] Till Tantau. *The* BEAMER *class.* Version 3.07. 2007. URL: http://mirror.ctan.org/macros/latex/contrib/beamer/doc/beameruserguide.pdf (visited on Aug. 12, 2008).

[TW89] Martin Tompa and Heather Woll. 'How to share a secret with cheaters'. In: *Journal of Cryptology* 1.3 (Oct. 1989). Pp. 133–138. ISSN: 0933-2790. DOI: 10.1007/BF02252871.