Seminar Komplexität und Kryptologie

Prof. Johannes Köbler Dr. Sebastian Kuhnert

Sommersemester 2016

Montag 15:15–16:45, RUD 26, 1'307

In diesem Seminar werden aktuelle Forschungsthemen der Gebiete Komplexitätstheorie und Kryptografie vorgestellt und diskutiert. Hierbei gehen wir auch gern auf Teilnehmerwünsche ein. Vorkenntnisse aus dem Bereich Komplexitätstheorie und Graphalgorithmen sind hilfreich, aber nicht notwendig. Das Seminar eignet sich gut zur Vorbereitung auf Abschlussarbeiten.

In diesem Semester liegt der Schwerpunkt auf *Kryptographie*.

Themen für Referate

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

1. **Diffie-Hellman und der Logjam-Angriff:**

   Inhalt: Wie kann ein Schlüssel über einen unsicheren Kanal sicher vereinbart werden? Wie funktioniert der Logjam-Angriff und wie kann er verhindert werden?

   Literatur: [Wät08, Kapitel 8.1], [ABD+15]

2. **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]

3. **Diskrete Logarithmen:** Modulare Exponentiation gilt als guter Kandidat für eine kryptographische Einwegfunktion, da für die Umkehrfunktion – den diskreten Logarithmus – keine effizienten Algorithmen bekannt sind. Darauf basiert die Sicherheit z.B. des ElGamal-Kryptosystems.

   Inhalt: Wie ist der diskrete Logarithmus definiert? Was sind die derzeit effizientesten Ansätze, diskrete Logarithmen zu berechnen?

   Literatur: [Sti06, Kapitel 6.2]

4. **Faktorisierung:** Auch die Multiplikation großer Primzahlen gilt als guter Kandidat einer kryptographischen Einwegfunktion, auf der die Sicherheit z.B. des RSA-Kryptosystems beruht.

   Inhalt: Wie arbeitet das RSA-Verfahren? Was sind die derzeit effizientesten Ansätze, große Zahlen zu faktorisieren?

   Literatur: [Sti06, Kapitel 5.3 und 5.6]

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

   Inhalt: Was sind blinde Signaturen und wie kann mit diesen elektronisches Geld realisiert werden? Welche Sicherheitseigenschaften sind für elektronisches Geld wünschenswert? Wie funktioniert Brands' Schema für elektronisches Geld?

   Literatur: [Mol02, Kapitel7.3]; [TW05, Kapitel 11]; [Wät08, Kapitel 10.5]

6. **Bitcoin:**

   Inhalt: Wie funktioniert Bitcoin und die zugrundeliegende Blockchain?

   Literatur: [Oku15], [RH13]

7. **Sichere Wahlen:** Wie kann bei einer freien und geheimen Wahl sichergestellt werden, dass das Ergebnis beim Auszählen nicht manipuliert wird?

   Inhalt: Welche Sicherheitsanforderungen sollte man an Wahlen stellen? Wie funktionieren blinde Signaturen? Wie können anonyme Kanäle durch Mixe realisiert werden?

   Literatur: [Sch06, Kaptiel 6.1], [Wät08, Kapitel 10.6], [MN07], [Cha94], [JCJ02]

8. **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], [Gol08, Kapitel 9.2]

Ablauf

- In der ersten Vorlesungswoche stellen wir euch die Referatsthemen vor und ihr wählt euer Thema aus.
- 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

[ABD+15] David Adrian, Karthikeyan Bhargavan, Zakir Durumeric, et al. 'Imperfect forward secrecy: How Diffie-Hellman fails in practice'. In: *Proc. 22th CCS*. Oct. 2015. DOI: 10.1145/2810103.2813707.

[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 9. Okt. 2014).

[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.

[Cha94] David L. Chaum. 'Secret-ballot receipts: True voter-verifiable elections'. In: *IEEE Security and Privacy* 2.1 (Jan. 1994), pp. 38–47. DOI: 10.1109/MSECP.2004.1264852.

[Gol07] Oded Goldreich. *Computational complexity. A conceptual perspective*. Rehovot, Israel: Weizmann Institute, 2007. URL: http://www.wisdom.weizmann.ac.il/~oded/cc-drafts.html (visited on Apr. 2, 2009). Draft of [Gol08].

[Gol08] Oded Goldreich. *Computational complexity. A conceptual perspective*. New York: Cambridge University Press, 2008. ISBN: 978-0-521-88473-0. Draft available online as [Gol07].

[JCJ02] Ari Juels, Dario Catalano, and Markus Jakobsson. *Coercion-resistant electronic elections*. Cryptology ePrint Archive. 2002. URL: http://eprint.iacr.org/2002/165. Report 2002/165.

[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 9. Okt. 2014).

[MN07] Tal Moran and Moni Naor. 'Split-ballot voting: everlasting privacy with distributed trust'. In: *Proceedings of the 14th ACM conference on Computer and communications security*. New York: ACM, 2007, pp. 246–255. DOI: 10.1145/1315245.1315277.

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

[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 (visited on Apr. 5, 2013).

[Oku15] Krzysztof Okupski. *Bitcoin Developer Reference*. Dec. 17, 2015.
URL: http://enetium.com/resources/Bitcoin.pdf.

[RH13] Fergal Reid and Martin Harrigan.
'An Analysis of Anonymity in the Bitcoin System'.
In: *Security and Privacy in Social Networks*. New York: Springer, 2013, pp. 197–223. DOI: 10.1007/978-1-4614-4139-7_10.

[Sch06] Bruce Schneier.
Angewandte Kryptographie. Protokolle, Algorithmen und Sourcecode in C.
Aus dem Englischen übers. von Katja Karsunke und Thomas Merz.
München: Pearson Studium, 2006. ISBN: 3-8273-7228-3.

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

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

[TWM13] Till Tantau, Joseph Wright, and Vedran Miletić. *The* BEAMER *class*.
Version 3.27. June 18, 2013. URL: http://mirror.ctan.org/macros/latex/contrib/beamer/doc/beameruserguide.pdf (visited on Oct. 1, 2013).

[Wät08] Dietmar Wätjen. *Kryptographie. Grundlagen, Algorithmen, Protokolle*.
2. Aufl. Heidelberg: Spektrum Akademischer Verlag, 2008.
ISBN: 978-3-8274-1916-3.