Proseminar Moderne Kryptoverfahren

Prof. Johannes Köbler Sebastian Kuhnert

Sommersemester 2009

Die rasante Ausbreitung des Internet und der mobilen Kommunikation hat dazu geführt, dass immer mehr Informationen digital erfasst und ausgetauscht werden. Daraus ergeben sich immer mehr Einschränkungen für die Privatsphäre. In diesem Proseminar werden wir uns mit kryptographischen Verfahren beschäftigen, die dem Schutz von Vertraulichkeit und anderen Sicherheitszielen dienen. Mit modernen Verfahren können dabei sogar Ziele erreicht werden, die in der analogen Welt unerreicht bleiben.

Für eine Einführung siehe [Lys08].

Themen für Referate

1. **Symmetrische Blockchiffren:** Wie können zwei Parteien geheime Nachrichten über einen abgehörten Kanal austauschen, indem sie zuvor einen Schlüssel austauschen?
   Inhalt: Wie funktioniert der DES? Welche Betriebsarten von Blockchiffren gibt es, und was sind deren Vor- und Nachteile?
   Literatur: [Wät08, Kapitel 4]
2. **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]
3. **Kryptographische Hashfunktionen:** Wie können lange Nachrichten so zu einem kompakten Hashwert zusammengefasst werden, dass sich nur sehr schwer Nachrichten mit gleichem Hashwert finden lassen?
   Inhalt: Welche Sicherheitsanforderungen werden an Hashfunktionen gestellt? Wie funktioniert der Geburtstagsangriff? Wie kann man aus einer Hashfunktion für konstant lange Eingaben eine für beliebig lange Eingaben konstruieren?
   Literatur: [Wät08, Kapitel 6]
4. **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]; ergänzend: [Sch06, Kapitel 5.3 und 6.4]
5. **Pseudozufallsgeneratoren:** Wie kann man aus wenigen zufälligen Bits viele zufällig aussehende Bits erzeugen?
   Inhalt: Welche Anforderungen werden an kryptographische Pseudozufallsgeneratoren gestellt? Wie können sie auf der Grundlage von Ununterscheidbarkeit definiert werden? Warum ist dies äquivalent zur Definition auf Grundlage von Unvorhersagbarkeit?
   Literatur: [Sti06, Kapitel 8.1 und 8.2]
6. **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? Wofür können diese verwendet werden?
   Literatur: [Wät08, Kapitel 10.2]
7. **Interaktive Beweissysteme:** 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?
   Literatur: [Gol01, Kapitel 4.2]; ergänzend: [BSW06, Kapitel 4.1]
8. **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]
9. **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] und [NS95]
10. **Identifikationsverfahren:** Wie kann man in elektronischer Kommunikation seine Identität nachweisen, ohne Identitätsdiebstahl zu ermöglichen?
    Inhalt: Wie können die Sicherheitsanforderung an Identifikationsverfahren formalisiert werden? Wie kann ein Identifikationsverfahren auf Grundlage von Zero Knowledge Proofs aussehen? Wie und warum funktioniert das Schnorr-Verfahren?
    Literatur: [Wät08, Kapitel 14]

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.
- In der zweiten Woche geben wir euch eine **Einführung** in kryptographische Grundbegriffe und modulare Arithmetik.
- Im Lauf des Semesters haltet ihr **Referate** in Zweiergruppen
  - 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 und setzt nicht mehr voraus, als sie schon wissen. Beispiele und Bilder helfen beim Verständnis.
  - Andererseits sollen eure Referate auch *präzise* sein: Ihr verwendet klare Definitionen und geht auch auf die Details von Konstruktionen und Algorithmen ein.
  - Für euer Referat stehen euch 90 Minuten zur Verfügung, also ca. 45 Minuten pro Person. 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 [Tan07, 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 5 Seiten umfassen.
  - Hinweise zum wissenschaftlichen Schreiben findet ihr unter [Böt06] und [Mit07].

Literatur

[BSW06] Albrecht Beutelspacher, Jörg Schwenk und Klaus-Dieter Wolfenstetter. *Moderne Verfahren der Kryptographie. Von RSA zu Zero-Knowledge.* 6. Aufl. Wiesbaden: Vieweg, 2006. ISBN: 3-8348-0083-X.

[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 30. März 2009).

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

[Lys08] Anna Lysyanskaya. 'How to Keep Your Secrets Safe'. In: *Scientific American Magazine* (Sept. 2008). URL: http://www.sciam.com/article.cfm?id=cryptography-how-to-keep-your-secrets-safe (visited on Mar. 30, 2009).

[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 30. März 2009).

[NS95] Moni Naor and Adi Shamir. 'Visual cryptography'. In: *Advances in Cryptology – EUROCRYPT'94.* Lecture Notes in Computer Science 950. Berlin et al.: Springer, 1995, pp. 1–12. ISBN: 978-3-540-60176-0. DOI: 10.1007/BFb0053419. URL: http://www.wisdom.weizmann.ac.il/~naor/PAPERS/vis.ps (visited on Nov. 5, 2008).

[Sch06] Bruce Schneier. *Angewandte Kryptographie. Protokolle, Algorithmen und Sourcecode in C.* Aus dem Englischen übers. von Katja Karsunke und Thomas Merz. München u. a.: 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.

[Tan07] Till Tantau. *The* BEAMER *class.* Version 3.07. 2007. URL: http://mirror.ctan.org/macros/latex/contrib/beamer/doc/beameruserguide.pdf (visited on Mar. 30, 2009).

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