Seminar »Komplexität und Kryptologie«

Moderne Hashfunktionen

Prof. Johannes Köbler Sebastian Kuhnert

Sommersemester 2012

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 liegt der Schwerpunkt auf kryptographischen Hashfunktionen.

Die Kryptographie ist ein hoch dynamisches Feld: Die eingesetzten Verfahren werden beständig weiterentwickelt, um ihre Sicherheit und ihren Ressourcenverbrauch zu verbessern. Diese Entwicklung wird nicht zuletzt durch immer bessere Angriffe erforderlich – und auch stimuliert. In den letzten Jahren wurden Schwächen von MD5, SHA-1 und SHA-2 bekannt, die heute teilweise eine praktische Bedrohung darstellen. Als Reaktion hierauf sucht das NIST in einem öffentlichen Verfahren nach einer sicheren Hashfunktion, die den Namen SHA-3 tragen wird. Von 64 Vorschlägen haben es 5 in die derzeit laufende Endrunde geschafft. In diesem Seminar werden wir uns mit Hashfunktionen im allgemeinen und den verbliebenen SHA-3-Kandidaten im besonderen beschäftigen.

Vorkenntnisse aus der Kryptographie sind zum Besuch dieses Seminars nützlich, jedoch nicht notwendig.

Themen für Referate

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

1. **Hashfunktionen aus Blockchiffren**
   Neben direkten Konstruktionen können Hashfunktionen auch auf Basis von anderen kryptographischen Grundbausteinen definiert werden.

   Inhalt: Wie kann aus einer Blockchiffre eine Hashfunktion konstruiert werden? Welche Sicherheitseigenschaften lassen sich für diese Konstruktionen nachweisen?

   Literatur: http://eprint.iacr.org/2010/519

2. **Der SHA-3-Kandidat BLAKE**

   Inhalt: Wie arbeitet BLAKE? Worauf stützt sich seine Sicherheit?

   Literatur: Siehe http://ehash.iaik.tugraz.at/wiki/The_SHA-3_Zoo

3. **Der SHA-3-Kandidat Grøstl**

   Inhalt: Wie arbeitet Grøstl? Worauf stützt sich seine Sicherheit?

   Literatur: Siehe http://ehash.iaik.tugraz.at/wiki/The_SHA-3_Zoo

4. **Der SHA-3-Kandidat JH**

   Inhalt: Wie arbeitet JH? Worauf stützt sich seine Sicherheit?

   Literatur: Siehe http://ehash.iaik.tugraz.at/wiki/The_SHA-3_Zoo

5. **Der SHA-3-Kandidat Skein**

   Inhalt: Wie arbeitet Skein? Worauf stützt sich seine Sicherheit?

   Literatur: Siehe http://ehash.iaik.tugraz.at/wiki/The_SHA-3_Zoo

6. **Angriffe auf MD5 und SHA-1**
   Diese weit verbreiteten Hashfunktionen haben sich als unsicher herausgestellt.

   Inhalt: Wie funktionieren die besten bekannten Angriffe auf diese Hashfunktionen?

   Literatur: http://dx.doi.org/10.1007/11535218_26
   http://eprint.iacr.org/2006/105.pdf
   http://dx.doi.org/10.1007/11535218_2

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 hilfreiche 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 [TWM11, 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 eine Krankschreibung.
- 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.
  - 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].

Literatur

[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 20. März 2012).

[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 20. März 2012).

[TWM11] Till Tantau, Joseph Wright, and Vedran Miletić. *The* BEAMER *class.* Version 3.15. 2011. URL: http://mirror.ctan.org/macros/latex/contrib/beamer/doc/beameruserguide.pdf (visited on Mar. 20, 2012).