Master-Seminar über Komplexität und Kryptologie SoSe 23

Prof. Dr. Jörg Rothe und Roman Zorn

https://ilias.hhu.de/goto.php?target=crs_1432374

Vorbesprechung – 06. April 2023

Scheinvoraussetzungen

1. Anmeldung im LSF bis einschließlich 06. April 2023
2. schriftliche Ausarbeitung zum Seminarthema (5–10 Seiten)
   - WICHTIG: Eigenleistung; reine Übersetzung nicht ausreichend
   - wenn möglich LaTeX verwenden
   - ALLE Quellen angeben
3. Peer-Review zu einer Ausarbeitung
   - vorgegebene Kriterien: Struktur, technische Qualität, etc.
   - objektive, konstruktive Kritik, double blind
4. 18- bis 20-minütiger Vortrag (LaTeX sehr praktisch) und anschließende Fragen- und Diskussionsrunde
5. Teilnahme an allen anderen Vorträgen

Bewertungskriterien

Siehe PDF auf der Seminarwebsite:

`https://ccc.cs.uni-duesseldorf.de/~rothe/masterseminar-kryptokomp`

Allgemeine Infos

- Seminartermine: Do 12:30 bis 14:00 Uhr in Hörsaal 5M
  - → nicht jede Woche!
  - → stattdessen Sprechstunden möglich (mit Voranmeldung)
- Fragen an Roman Zorn senden: roman.zorn@hhu.de

Ablauf

Themenvergabe

- Ab heute bis Mittwoch 12.04., 12:00 Uhr (mittags!) Präferenzen zu Themen im ILIAS abgeben
- Literatur erhalten
- Ausarbeitung/Folien anfangen!

Ablauf

Themenvergabe

- Ab heute bis Mittwoch 12.04., 12:00 Uhr (mittags!) Präferenzen zu Themen im ILIAS abgeben
- Literatur erhalten
- Ausarbeitung/Folien anfangen!

Seminartermine (12:30 bis 14:00 in 5M)

- Heute: Einführung
- Am 20.04.: Wie schreibe ich eine Ausarbeitung?
- Am 25.05.: Wie bereite ich einen Vortrag vor?
- Am 29.06., 06.07. und 13.07.: Vorträge

Ablauf

Themenvergabe

- Ab heute bis Mittwoch 12.04., 12:00 Uhr (mittags!) Präferenzen zu Themen im ILIAS abgeben
- Literatur erhalten
- Ausarbeitung/Folien anfangen!

Seminartermine (12:30 bis 14:00 in 5M)

- Heute: Einführung
- Am 20.04.: Wie schreibe ich eine Ausarbeitung?
- Am 25.05.: Wie bereite ich einen Vortrag vor?
- Am 29.06., 06.07. und 13.07.: Vorträge

Abgaben (per Ilias)

- bis Do 11.05., 12:00 Abgabe der Ausarbeitung
  - → zeitnah erhalten Sie eine Ausarbeitung zur Begutachtung
- bis Do, 25.05., 12:00 Abgabe des Reviews
  - → zeitnah erhalten Sie Ihr Review und ein kurzes Feedback der Seminarleitung
- bis Do, 22.06., 12:00 Abgabe Folien und überarbeitete Ausarbeitung
  - → zeitnah erhalten Sie ein kurzes Feedback der Seminarleitung
- bis Do 29.06., 12:00 Evtl. Abgabe der überarbeiteten Folien

Themen

- Jeder erhält eine wissenschaftliche Arbeit zu einem Thema
- Ziele:
  - Definitionen und Kernaussagen herausfiltern
  - sinnvoll strukturieren (Ausarbeitung $\neq$ Vortrag)
  - in eigenen Worten wiedergeben
  - an Beispielen veranschaulichen
  - Eventuell einen interessanten Beweis anschaulich darstellen.
  - Quellen angemessen zitieren (~~Wikipedia~~, *ok zum Nachgucken oder für Bilderquellen*)
  - gegenseitig beurteilen, hinterfragen (keine negative Auswirkung; konstruktive Tipps für euch)

Themenübersicht

Complexity Theory:

- **Thema 1:** Stable Marriage and Roommate Problems
- **Thema 2:** Electing Successive Comittees
- **Thema 3:** Shift Bribery in Iterative Elections
- **Thema 4:** Magic: The Gathering is Turing-Complete

Cryptology:

- **Thema 5:** The RSA Protocol
- **Thema 6:** Protocol for the Millionaires' Problem
- **Thema 7:** How to Time-Stamp a Digital Document
- **Thema 8:** How To Share a Secret with Cheaters

Complexity Theory:

- **Thema 9:** Allocations with Connectivity Constraints

Thema 1: Stable Marriage and Roommate Problems

- Ermitteln die Komplexität der Überprüfung der Existenz von Matchings mit bestimmten Stabilitätskriterien.
- Fokus auf individuellen Stabilitätskriterien.
- Erweitern einige der Beweise auf andere Gebiete, wie z. B. hedonische Spiele.

Haris Aziz. Stable marriage and roommate problems with individual-based stability. In *Proceedings of the 12th International Conference on Autonomous Agents and Multiagent Systems*, pages 287–294. IFAAMAS, 2013

Thema 2: Electing Successive Comittees

- Betrachten *sukzessive Komitee-Wahlen* mit dem Ziel, eine "bestmögliche" Folge von Komitees zu bestimmen.
- So sollen "Machtkartelle" verhindert und die sozialen Kosten, Komitees zu überladen, klein gehalten werden. Gleichzeitig sollen zu häufige Wahlen vermieden werden.
- Zeigen scharfe Komplexitätsdichotomie zwischen Komiteegröße 2 (meist in P) und 3 (meist NP-schwer).

Robert Bredereck, Andrzej Kaczmarczyk, and Rolf Niedermeier. Electing successive committees. In *Proceedings of the 34th AAAI Conference on Artificial Intelligence*, pages 1846–1853. AAAI Press, 2020

Thema 3: Shift Bribery in Iterative Elections

- *"Shift bribery"*: Bestecher verschiebt Lieblingskandidaten in den Wählerstimmen nach oben (zu bestimmten Kosten), ohne sein Budget zu überschreiten.
  Gewinnt Lieblingskandidat?
- Dieses Problem wird für iterative Wahlsysteme untersucht, die in jeder Runde "schwächste" Kandidaten eliminieren.
- Zeigen NP-Vollständigkeit in allen Fällen.

Cynthia Maushagen, Marc Neveling, Jörg Rothe, and Ann-Kathrin Selker. Complexity of shift bribery in iterative elections. In *Proceedings of the 17th International Conference on Autonomous Agents and Multiagent Systems*, pages 1567–1575. IFAAMAS, 2018

Thema 4: Magic: The Gathering is Turing-Complete

- Zeigen, dass optimales Spielen in *Magic: The Gathering* mindestens so schwer ist wie das Halteproblem und somit unentscheidbar.
- Simulieren dazu eine Turingmaschine in einer Partie *Magic*.
- Kenntnis des Spiels nützlich, aber nicht erforderlich.

Alex Churchill, Stella Biderman, and Austin Herrick. Magic: The Gathering Is Turing Complete. In *Proceedings of the 10th International Conference on Fun with Algorithms (FUN 2021)*, pages 9:1–9:19. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2021

Thema 5: The RSA Protocol

- Führen die nach den Autoren dieser Arbeit benannte RSA-Methode zur Verschlüsselung ein.
- Erklären, wie man mit der Methode ver- und entschlüsselt.
- Sicherheit basiert auf der Schwierigkeit, große Zahlen in ihre Primfaktoren zu zerlegen.

Ronald L Rivest, Adi Shamir, and Leonard Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978

Thema 6: Protocol for the Millionaires' Problem

- Zwei Millionäre wollen wissen, wer von ihnen reicher ist. Sie wollen also bestimmen, welche von zwei Zahlen größer ist, ohne sich die Zahlen zu verraten.
- Führen ein Protokoll ein, um dieses Problem praktisch zu lösen.
- Vergleichen ihr Modell experimentell mit anderen Methoden.

Ioannis Ioannidis and Ananth Grama. An efficient protocol for Yao's millionaires' problem. In *Proceedings of the 36th Annual Hawaii International Conference on System Sciences*. IEEE, 2003

Thema 7: How to Time-Stamp a Digital Document

- Time-Stamps können nützlich sein für Urheberrechte oder zur Kontrolle von Manipulation an einem Dokument.
- Erklären, wie ein Time-Stamp-Service (TSS) unter bestimmten Bedingungen funktionieren kann.
- Vergleichen zwei Methoden, um das Vertrauen in einen TSS zu verbessern.

Stuart Haber and W Scott Stornetta. How to time-stamp a digital document. *Journal of Cryptology*, 3:99–111, 1991

Thema 8: How To Share a Secret with Cheaters

- Shamirs Protokoll: Eine geheime Nachricht soll so auf n Spieler 'aufgeteilt' werden, dass k Spieler nötig (und ausreichend) sind, um die geheime Nachricht zu rekonstruieren.
- Es wird eine Variante von Shamirs Protokoll vorgestellt, die immun gegen Betrug ist.
- Betrug bedeutet dabei: $k - 1$ Spieler tun sich zusammen, um einem k-ten Spieler eine falsche Nachricht weiszumachen.

Martin Tompa and Heather Woll. How to share a secret with cheaters. *Journal of Cryptology*, 1(3):133–138, 1989

Thema 9: Allocations with Connectivity Constraints

- Aufteilung von nicht-teilbaren Gütern auf Agenten mit additiven Bewertungsfunktionen.
- Graph, der Beziehungen zwischen Gütern darstellt.
  - → Es werden nur zusammenhängende Güter zugeteilt.
- Suche nach Pareto-optimalen Aufteilungen.
- Betrachten insbesondere Wege und Sterne.
- Komplexitätsanalyse.

Ayumi Igarashi and Dominik Peters. Pareto-optimal allocation of indivisible goods with connectivity constraints. In *Proceedings of the 33rd AAAI Conference on Artificial Intelligence*, pages 2045–2052. AAAI Press, 2019

Abschließende Hinweise

- Fangen Sie rechtzeitig an!
- Sie können sich bei Fragen gerne bei uns melden.
- Einen detaillierten Seminarplan finden Sie auf der Seminarwebseite:

`https://ccc.cs.uni-duesseldorf.de/~rothe/masterseminar-kryptokomp`

Viel Erfolg!