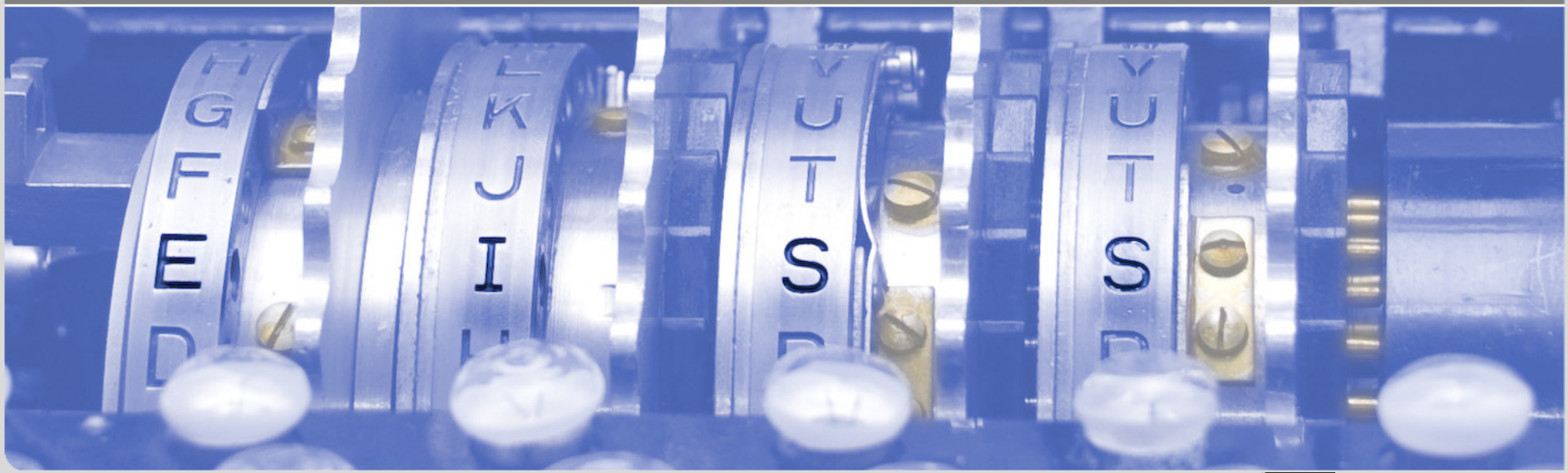
Karlsruher Institut für Technologie

Seminar – Fortgeschrittene Themen der Beweisbaren Sicherheit – SS 2016

KIT-Fakultät für Informatik – Institut für Theoretische Informatik – Forschungsgruppe für Kryptographie und Sicherheit



Inhalt

- Ziele
- Regeln
  - Grundsätzliches
  - Ausarbeitung und Präsentation
  - Aufbau der Ausarbeitung
- Termine
- EasyChair „KITATPS2016“
- Themenvorstellung
- Themenzuweisung

Ziele

- Hinreichendes Verständnis des Themas
- Schriftliche Ausarbeitung
  - In-sich-abgeschlossen, d.h. Hintergründe und Annahmen erklären
  - 12-16 Seiten Umfang
- Präsentation
  - Folienvortrag vor anderen Teilnehmern
  - 20 Minuten Dauer
  - Anschließende Diskussion, vorbereitet sein auf Fragen
- Selbständiges Arbeiten, insb. sind Termine mit Betreuer eigenverantwortlich zu vereinbaren

Regeln – Grundsätzliches

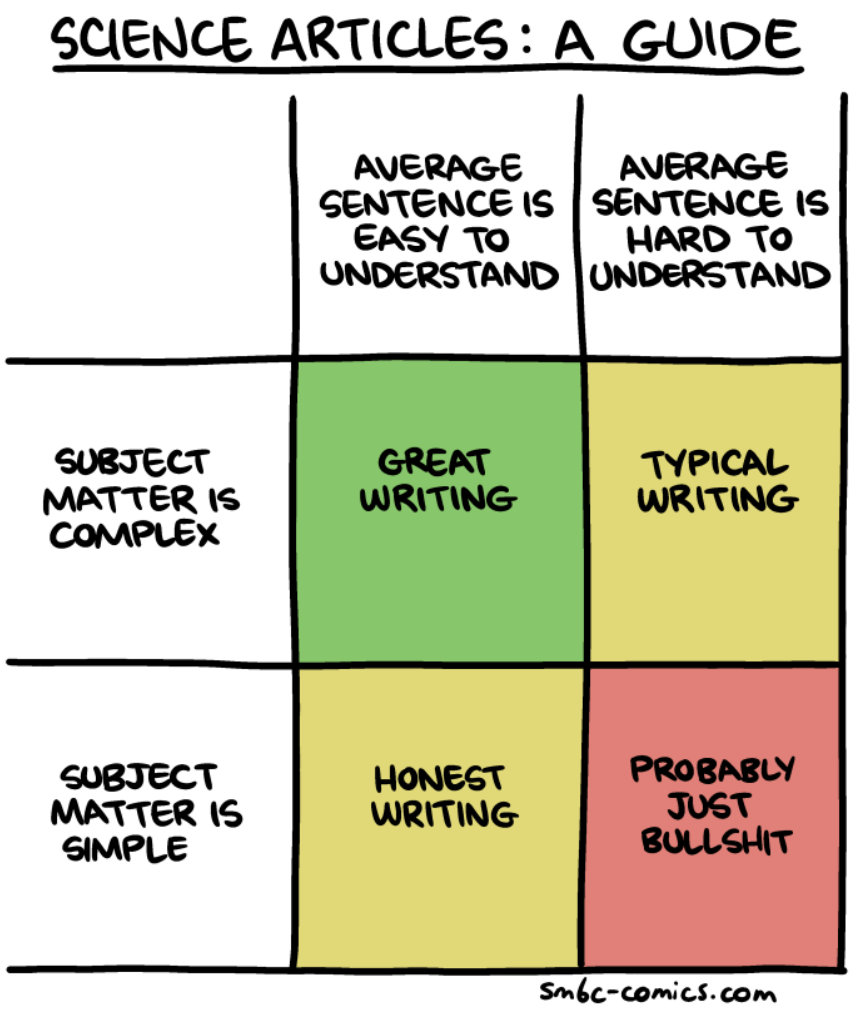
- Keine Plagiate, falls doch:
  - keine ECTS-Punkte
  - keine Teilnehmenbescheinung
  - in gravierenden Fällen: Meldung an den Prüfungsausschuss
- Termine sind verpflichtend
- Ernsthafte Teilnahme und ehrliches Bemühen
  - Die gesamte Mitarbeit am Seminar kann zur Notenfindung herangezogen werden
  - Die Review-fähige Zwischenabgabe ist Teil dieser Mitarbeit
  - Bei Schwierigkeiten: Rechtzeitig, nach Möglichkeit im Vorfeld Gespräch mit dem Betreuer suchen

Regeln – Ausarbeitung und Präsentation (I)

- Benutzung des vorgegeben Formats
  - LaTeX, PDF
  - Vorlage von Homepage
- Verwendung wissenschaftlicher Quellen
  - Quellen mit Peer-Review
  - nicht nur Wikipedia

Regeln – Ausarbeitung und Präsentation (II)

- Richtige Orthografie und Grammatik
- Niemals aufeinanderfolgende Überschriften ohne Text dazwischen
- Niemals nur eine Unterüberschrift
  (Merke: „Wer ‚Erstens' sagt, muss auch ‚Zweitens' sagen")
- Aussagekräftige Bildunterschriften



Regeln – Ausarbeitung und Präsentation (III)

- Drei Arten von Tatsachenbehauptungen
  - Allgemein bekannte Behauptungen
    (Bsp.: *„Nachts wird es draußen dunkel“*)
  - Eigene Behauptungen, die selbst belegt werden
    (Bsp.: *„Wir beweisen N = NP“*)
  - Fremde Behauptungen (Zitate, Paraphrasen, etc.)
    - Quelle muss eindeutig und auffindbar sein
    - Autor
    - Titel
    - Datum
    - Erscheinungsort, -art

Regeln – Aufbau der Ausarbeitung

1. Einleitung
    1. Motivation
    2. Ziel der Arbeit
    3. Aufbau der Arbeit
2. Voraussetzungen
3. Thema
4. Fazit
    1. Zusammenfassung
    2. Ausblick

Regeln – Abschlusspräsentation (I)

- 20 Minuten, mindestens 15, allerhöchstens 25
- 5-10 Minuten für Diskussion
- Anderer Fokus als in der Ausarbeitung
  - Wichtig sind Motivation und die Ergebnisse
  - Details nur als „Highlights“

Regeln – Abschlusspräsentation (II)

- LaTeX-Beamer oder Powerpoint oder OpenOffice
- Plane ca. 1 Minute pro Folie
- Weniger ist mehr
  - Wenige Stichworte, keine Sätze
  - Freiräume
  - Im Zweifel: Auf eine neue Folie!
- Verwende Grafiken
- Die Folien sollen den Vortrag unterstützen und ihn nicht ersetzen!
- Nicht vergessen: Inhaltsverzeichnis, Quellenverzeichnis, Foliennummern!

Regeln – Aufbau der Abschlusspräsentation

- Motivation, Kontext
- „Methode“: Was habe ich gemacht, was stelle ich vor?
- „Ergebnisse“: Konkret Ergebnisse vorstellen (aus der Vogelperspektive)
- Zusammenfassung, Schluss

Termine

- 18.04.2016: Allgemeine Einführungsveranstaltung
- 27.06.2016: Abgabe der vorläufigen, schriftlichen Ausarbeitung (Review-fähige Version) per EasyChair
- 11.07.2016: Abgabe der Reviews per EasyChair
- 25.07.2016: Abgabe der Vortragsfolien per E-Mail
- 01.08.2016/
  15.08.2016: Zwei Vortragsblöcke (genaues Datum wird „erdoodelt“)
- 15.08.2016: Abgabe der finalen, schriftlichen Ausarbeitung

EasyChair „KITUC2016“

- Konferenzmanagementsystem EasyChair
- Verwendung um
  - erste Review-fähige Ausarbeitung abzugeben (27.06.2016)
  - gegenseitige Reviews zu erstellen (11.07.2016)
  - finale Ausarbeitung abzugeben (15.08.2016)
- KITATPS2016: `https://easychair.org/conferences/?conf=kitatps2016`
- Bis 30.04.2016 eigenen Account erstellen, Name des Accounts an Matthias (<matthias.nagel@kit.edu>) senden

Themenvorstellung

Unconditionally Secure UC-Commitments from Physical Assumptions

- Inhalte:
  - Allgemeine Black-Box-Transformation von informationstheoretisch-sichereren Commitments in UC-Commitments
  - Instantiierung mit PUFs und mit zustandslosen, manipulationssicheren Hardware-Tokens
- Literatur:

[1] Ivan Damgård, Alessandra Scafuro 2013: „Unconditionally Secure and Universally Composable Commitments from Physical Assumptions“

An Algebraic Approach To Non-Malleability

- Inhalte:
  - Konstruktion eines Commitment-Schemas auf Basis von fehlerkorrigierenden Codes
  - Ziel ist ein Commitment-Schema das weniger als CCA-sicher ist, dafür aber nur eine konstante Anzahl an Runden benötigt und immer noch eine sinnvolle Definition von „Non-Malleability“ erfüllt
- Literatur:

[1] Vipul Goyal, Silas Richelson, Alon Rosen, Margarita Vald 2014: „An Algebraic Approach To Non-Malleability“

- Hinweis: Evtl. wird Literatur noch getauscht gegen „Nachfolge“-Paper, dass konzeptionell einfacher ist und auf Gittern basiert

Achieving UC without Trusted Setup

- Inhalte:
  - Viele, wichtige Krypto-Primitiven können nicht im „plain“ UC-Modell realisiert werden
  - Durch Einfügen von super-polynomiellen Orakel beim Simulator im idealen Experiment wird die Sicherheitsnotation relaxiert, sodass die Unmöglichkeitsresultate überwunden werden können ohne die Nachteile eines allgemeinen super-polynomiellen Simulators in Kauf nehmen zu müssen.
- Literatur:

[1] Manoj Prabhakaran and Amit Sahai 2004: „New Notions of Security: Achieving Universal Composability without Trusted Setup“

How to Use Indistinguishability Obfuscation

- Inhalte:
  - Allgemeine Black-Box Code-Obfuszierung von beliebigen Schaltkreisen ist unmöglich
  - Indistinguishability Obfuscation (iO) ist eine abgeschwächte Variante
  - Es werden die Anwendungsmöglichkeiten von iO wie CCA-sichere PKE, NIZK, injektive Falltürfunktionen, etc., … gezeigt
- Literatur:

[1] Amit Sahai, Brent Waters 2014: „How to Use Indistinguishability Obfuscation: Deniable Encryption, and More“

Lossy Trapdoor Functions and Their Applications

- Inhalte:
  - Lossy-Trapdoor-Funktionen (LTF) können in zwei ununterscheidbaren Betriebsmodi betrieben werden: lossy und injektiv
  - Konstruktion von LTFs
  - Anwendung von LTFs: CCA-sichere Verschlüsselung, kollisionsresistente Hash-Funktionen, OTs
- Literatur:

[1] Chris Peikert, Brent Waters 2008: „Lossy Trapdoor Functions and Their Applications“

Dual System Encryption

- Inhalte:
  - Neue Technik für Identity-Based Encryption z.B. auf Basis der Bilinear-Diffie-Hellman-Annahme
  - Je zwei, ununterscheidbare Arten von geheimen Schlüsseln und Chiffraten: normale und semi-funktionale
  - Neue Spiele für den Sicherheitsbeweis sind notwendig
- Literatur:

[1] Brent Waters 2009: „Dual System Encryption: Realizing Fully Secure IBE and HIBE under Simple Assumptions“

Functional Signatures and Pseudorandom Functions

- Literatur:

[1] Elette Boyle, Shafi Goldwasser, Ioana Ivan 2013: „Functional Signatures and Pseudorandom Functions“

Aggregate and Verifiably Encrypted Signatures from Multilinear Maps Without Random Oracles

- Literatur:

[1] Markus Rückert, Dominique Schröder 2013: „ Aggregate and Verifiably Encrypted Signatures from Multilinear Maps Without Random Oracles“

Sanitizable Signatures

- Literatur:

[1] Giuseppe Ateniese, Daniel H. Chou, Breno de Medeiros, Gene Tsudik 2005: „Sanitizable Signatures“

Themenvergabe

Themenvergabe

#	Titel	Betreuer
1	Uncond.' Secure UC-Commitments from Physical Assumptions	MN
2	An Algebraic Approach To Non-Malleability	MN
3	Achieving UC without Trusted Setup	MN
4	How to Use Indistinguishability Obfuscation	AR
5	Lossy Trapdoor Functions	AR
6	Dual System Encryption	AR
7	Functional Signatures and Pseudorandom Functions	JK
8	Aggregate and Verifiably Encrypted Signatures from Multilinear Maps Without Random Oracles	JK
9	Sanitizable Signatures	JK

Verbindliche, schriftliche Anmeldung mit KIT-Card