Privatdozent Dr. Claus Diem
Prof. Dr. Andreas Maletti

SEMINAR
ZERO-KNOWLEDGE

Topics for the talks

1. One-way functions (C.D.)
2. Pseudorandom generators (FOC, Chapter 3; my lecture from the winter semester) (Song Tian)
3. Models of security and constructions for cryptographic systems (my lecture from the winter semester) (Sergei Stoliarchuk & Vadim Osipov)
4. Interactive proof systems (FOC, 4.1, 4.2; MCPPPR, 2.2) (Nicole Timme)
5. IP = PSPACE (A.M.)
6. Is NP = PSPACE?
7. Zero-knowledge proofs: definition and a first example (FOC, 4.3; GB, 12.2) (Denis Olefirenko)
8. Zero-knowledge proofs for NP (FOC, 4.4; GB, 12.2) (Nikita Kolesninov)
9. Negative results (FOC 4.5., in particular 4.5.4.2) (Robert Schädlich)
10. Zero-knowledge proofs and cuncurrent communication (Dennis Kreusel, 31.5.)
11. Proofs of knowledge (FOC, 4.7.1-4.7.4; Wikipedia article) (Felix Hillmann, 7.6.)
12. Proofs of identity (FOC, 4.7.5; Wikipedia article) (Frauke Beccard, 14.6.)
13. Non-interactive zero-knowledge proofs / proofs of knowledge and Fiat-Shamit heuristic (FOC, 4,10; Wikipedia articles) (Jannis Holliger, 21.6.)
14. Non-interactive zero-knowldege proofs / proofs of knowledge from pairings, maybe SNARKs (Wikipedia article on non-interactive zero-knowledge proofs and in there [10], maybe [5]) (Charlotte Tiede, 28.6.)
15. STARKs (Fabian Sauer, 5.7.)

Literature

FOC. O. Goldreich, Foundations of Cryptography, in der Bibliothek

GB. S. Goldwasser & M. Bellare, Lecture Notes on Cryptography,
http://cseweb.ucsd.edu/∼mihir/papers/gb.pdf

MCPPPR. O. Goldreich, Modern Cryptography, Probabilistic Proofs and Pseudo-Randomness, in der Bibliotheik

Vorgaben

Ein Vortrag hat 60 - 75 Minuten (nach Absprache länger).

Spätenstens eine Woche vor dem Vortrag muss eine schriftliche Ausarbeitung abgegeben werden. Ich gebe dann Rückmeldung und Sie können (sollten) die Ausarbeitung verbessern.

Die Note setzt sich zusammen aus:

- 2/3 der Vortrag
- 1/3 die Ausarbeitung

Es wird auf Noten mit Tendenz gerundet.

Der Vortrag darf sowohl mit Folien als auch an der Tafel gehalten werden.

Besonders wichtig: Alle neuen verwendeten Begriffe müssen eingeführt werden.

Auch wichtig: Schon die Höflichkeit gegenüber den Vortragenden gebietet es, dass Sie auch regelmäßig teilnehmen. Ich erwarte von Ihnen, dass Sie mir vorab mitteilen, wenn Sie mehr als einmal mit teilnehmen können.