Crypto Seminar Topics

Dominique Unruh

University of Tartu

Rules of the game

- Literature review:
  - Read a paper (new stuff, 2013/14)
  - Understand the paper
  - Summarize the paper
  - Present the paper

- Clarity of presentation / understanding

Indistinguishability Obfuscation

[Garg, Gentry, Halevi]

- Obfuscation: Can transform a program such that it becomes unreadable (leaks **no** information)?

- Task: present paper on “indistinguishability obfuscation” **or** give a survey of recent results based on indistinguishability obfuscation

PhD

Quantum position verification

[Unruh]

- A device wants to prove it's position in space (based on speed of light)
- Impossible classically
- Can be done by sending quantum states (that's the result of the paper)

MSc

PhD