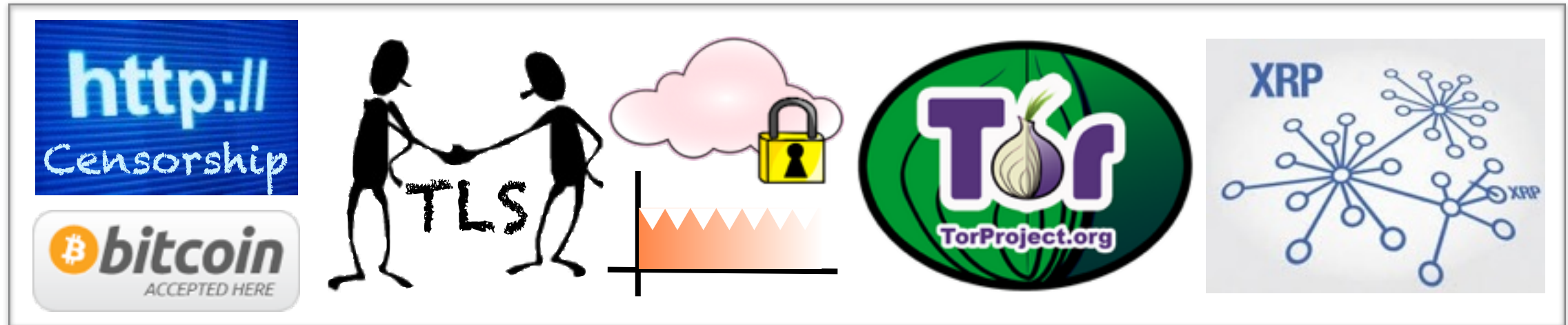


Organizational Meeting

Seminar: Practical Cryptographic Systems



Dr. Aniket Kate
Cryptographic Systems (CrypSys) Research Group
MMCI, Saarland University
<http://crypsys.mmci.uni-saarland.de>

Student Registration

- ✓ Checking with the Confirmed Students

Organizational Details

Organizational Details

Instructor: Dr. Aniket Kate

Teaching Assistant: Tim Ruffing

Time: Friday 10:15 to 12:00

Place: EI 7 Seminar Room 3.23

Webpage: <http://crypsys.mmci.uni-saarland.de/courses/pcs-seminar14/index.html>

Contact: pcs2014@mmci.uni-saarland.de

Credit Points: 7 CP [+ 6 CP]

Organizational Details

Instructor: Dr. Aniket Kate

Teaching Assistant: Tim Ruffing

Time: Friday 10:15 to 12:00

Place: EI 7 Seminar Room 3.23

Webpage: <http://crypsys.mmci.uni-saarland.de/courses/pcs-seminar14/index.html>

Contact: pcs2014@mmci.uni-saarland.de

Credit Points: 7 CP [+ 6 CP]



may change

Grading

Task	Percentage
Paper Presentation	40%
Paper Reviews	15%
Class Participation	10%
Course Project	35%

Grading: Paper Presentation

- ✓ Suggest four papers by Sunday night
- ✓ Give a 30-minute presentation for your selected paper
 - The schedule will be available early next week

Grading: Paper Reviews

- ✓ Write reviews for five pre-assigned papers
- ✓ Review = Summary + Critics
+ Future directions

Grading: Class Participation

- ✓ Actively participate in class discussions

Grading: Course Project

- ✓ A research/development project on some topic related to cryptographic systems
- ✓ Ideal group size: two, but adjustable
- ✓ Two steps:
 - Proposal presentation
 - Report Submission

Grading: Bonus Points

- ✓ Earn bonus points by performing better than expected in
 - class discussions,
 - your paper-reviews or
 - your project.

Course Basics

✓ Goal:

To study (and attack) the cryptographic systems used in our daily life

✓ Topics Considered:

- Crypto Currencies
- Social and Payment Networks
- Anonymity Networks and Censorship Evasion
- Digital Certificate Infrastructures
- Randomness
- Cloud Security
- Crypto Implementations

Course Topics



✓ Crypto-currencies:

- Bitcoin: A Peer-to-Peer Electronic Cash System
- A Fistful of Bitcoins: Characterizing Payments Among Men with No Names
- Zerocoin: Anonymous Distributed E-Cash from Bitcoin
- Secure Multiparty Computations on Bitcoin

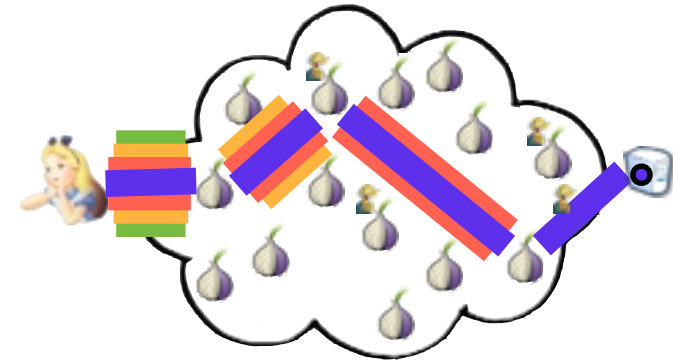
Course Topics



✓ Social and Payment Networks

- Social Networking with Friendegrity: Privacy and Integrity with an Untrusted Provider
- Bazaar: Strengthening User Reputations in Online Marketplaces

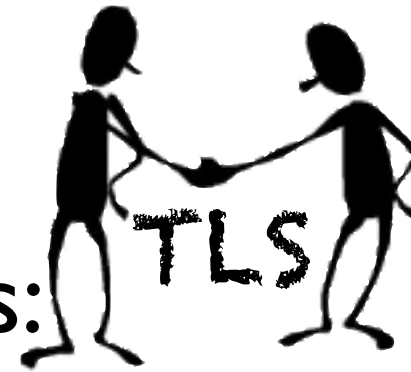
Course Topics



- ✓ Anonymity Networks and Censorship Evasion:
 - Trawling for Tor Hidden Services: Detection, Measurement, Deanonimization
 - Elligator: Elliptic-curve Points Indistinguishable from Uniform Random Strings
 - Protocol Misidentification Made Easy with Format-Transforming Encryption

Course Topics

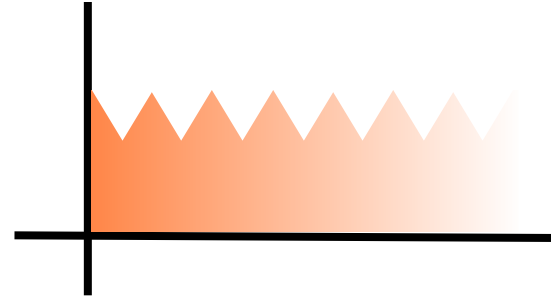
✓ Certificate Infrastructures:



DigiNotar
Internet Trust Services

- Web PKI: Closing the Gap between Guidelines and Practices
- SoK: SSL and HTTPS: Revisiting Past Challenges and Evaluating Certificate Trust Model Enhancements
- Certificate Transparency
- Enhanced Certificate Transparency and End-to-End Encrypted Mail
- Macaroons: Cookies with Contextual Caveats for Decentralized Authorization in the Cloud

Course Topics



✓ Randomness:

- Security Analysis of Pseudo-Random Number Generators with Input: `/dev/random` is not Robust
- Ensuring High-Quality Randomness in Cryptographic Key Generation

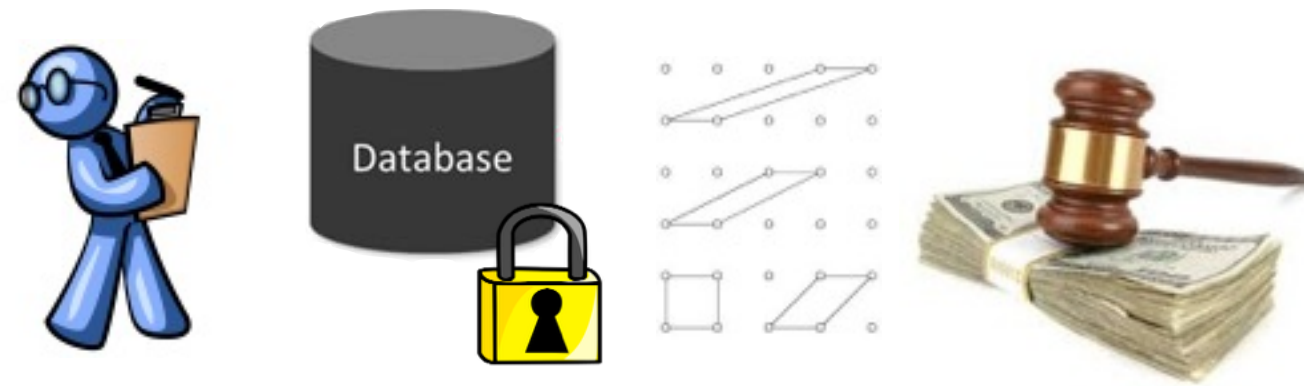
Course Topics



✓ Cloud Security:

- Pinocchio: Nearly Practical Verifiable Computation
- Blind Seer: A Scalable Private DBMS

Course Topics



✓ Cryptographic Implementations:

- CryptDB: Protecting Confidentiality with Encrypted Query Processing
- Verifiable Auctions for Online Ad Exchanges
- Lattice Cryptography for the Internet

Background Preparation

- ✓ Some background in cryptography, security, or privacy is expected
- ✓ Contact us early enough if you have not done background courses

Student Introductions

Thanks!

Aniket Kate

<http://crypsys.mmci.uni-saarland.de/>