Themes for Crypto Seminar

Sven Laur
swen@math.ut.ee

My Interests

- Systematisation of Cryptography
  - homological classification
  - generic constructions
- Practical Protocol Design
  - Efficient solutions for specific problems
  - tools for semi-automatic security analysis

Catch-22

To understand Cryptography, you have to work with the material. The best way for that is through seminar. Most of my seminar topics require basic understanding of Cryptography

Homological Classification of Zero-Knowledge

- It is a master thesis topic
- You have to read lot of articles from 80-ies
- You have to extract basic constructions
- You have to love math and reductions
- For the seminar, you just have to choose a good overview article and present it

Efficient Certified Computations

- It is a master thesis topic
- The main aim is to describe the notorious GMV compiler for protocols
- You must give a complete instantiation
  - Pedersen commitments
  - Proofs of knowedge (POK)
  - Conversion from POK to zero-knowledge

Verifiable Protocols for Arithmetic Operations

- At least master level research topic
- You must love linear algebra
- We need verifiable share computing over
- Protocols for multiplication and addition $\mathbb{Z}_{2^{32}}$
- For the seminar, a review about classical verrifiable protocols is enough

Share Multiplication Protocols over Rings

- A master level research topic
- You must love linear algebra and math
- You must give a general description of almost all share multiplication protocols
- Can be both experimental or theoretical
- For the seminar, you could just review classical results

Automatic Generation of Garbled Circuits

- This is a practical master level topic
- You must love C++ and compiler writing
- Essentially you must implement
  - parsing of logic and arithmetic expression
  - compilation into boolean circuits
  - circuit scrambling operations