Topics for cryptoseminar in fall 2017

Jan Willemsen
janwil@cyber.ee

05.09.2017
Tamarin Prover

- There are several proof assistants for cryptographic protocols
  - ProVerif works in symbolic model and can generate attacks, but the output is not human-readable
  - EasyCrypt works in computational model, cannot generate attacks itself and is rather unstable
- There is a recent alternative – Tamarin Prover
  http://tamarin-prover.github.io/
- The task is to get to know this tool, test it out and write a report
- Level: MSc or PhD student, experience with some other prover is a bonus
Practical implementations of quantum-resistant cryptography

- There are many PQ crypto algorithm proposals
  - NTRU, New Hope, McEliece, Niederriter, McBits, XMSS, SPHINKS, Rainbow, BLISS, SIDH, ...
- They are mostly on paper, but some implementations are available, too
- The task is to get an overview of the existing implementations
  - Which algorithms are supported?
  - How well do they integrate with existing frameworks, say, TLS?
    - Which algorithms are drop-in replacements for existing ones?
    - How much will the sizes of cryptograms, signatures, etc. Increase?
  - What is known about the potential side channels?
  - How thoroughly have the implementations been scrutinised?

The level is BSc or MSc student; experience with crypto libraries and system programming is a bonus