Research Seminar in Cryptography

Benson Muite

benson.muite@ut.ee
http://kodu.ut.ee/~benson

23 February 2018
Secure communication

- Design and build a secure and simple encrypted chat, voice or messaging system.
- Be sure to explain choice of protocols used, their software and hardware implementations.
- You may build on existing projects, but the final result should be as simple as possible.
- Level Msc, Bsc
Open source voting applications

There are a number of open source voting applications including:
- Nextcloud polls app https://github.com/nextcloud/polls
- Dudle https://github.com/kellerben/dudle
- Fedora voting https://github.com/ryanlerch/elections

Examine some of these applications.
Do they allow for anonymous voting, if so how good are the implementations?
How might they be improved?
Level Msc, Bsc
Sparse fast Fourier transform

- Perform a survey of algorithms for the sparse fast Fourier transform.
- Explain the main concepts.
- Possibly implement the sparse fast Fourier transform or use an implementation of the sparse fast Fourier transform in the creation of jpeg like files.
- Level Msc, PhD
Review the papers on Meltdown and Spectre.
Try to reproduce the vulnerability on a modern CPU.
Determine whether this impacts the Estonian ID card system.
References: https://meltdownattack.com/
Level Bsc, Msc, PhD