

Program: COINS - Winter School, FINSE, May 6-11, 2018

Sunday, May 6

21:00 Welcome Dinner

Monday, May 7

08:00 – 09:00 Breakfast

09:00 – 10:15 Gunnar Alendal, NTNU, Harddisk encryption

10:45 – 12:30 Dennis Andriessse, VU Amsterdam, Binary analysis techniques and Introduction to Pin

12:30 – 14:00 Lunch

17:00 – 19:00 Gunnar Alendal, NTNU, Android: security and challenges

19:00 – 20:30 Dinner

Tuesday, May 8

08:00 – 09:00 Breakfast

09:00 – 10:30 Dennis Andriessse, VU Amsterdam, Binary analysis techniques 2

11:00 – 12:30 Colin Boyd, NTNU, Cryptocurrencies and blockchain

12:30 – 14:00 Lunch

17:00 – 18:30 Presentations by the participants (I)

Navid Ghaedi Bardeh: Yoyo game on AES

Andrea Tenti: Probabilistic analysis on the rank of Macaulay Matrices over finite fields

Jens-Petter Sandvik: IoT Forensics

Each presentation 30 min., incl. questions

19:00 – 20:30 Dinner

Wednesday, May 9

08:00 – 09:00 Breakfast

09:00 – 10:30 Colin Boyd, NTNU, Cryptocurrencies and blockchain

*11:00 – 12:30 Martin Pirker, UAS (University of Applied Sciences) St. Pölten, Austria
Trusted computing I*

12:30 – 14:00 Lunch

17:00 – 18:30 Presentations by the participants (II)

Irene Villa: Optimal boolean functions

Albin Severinson: Coding for distributed computing

Enio Marku: Shielding Network Function on a Multi-Operator System using SGX

Each presentation 30 min., incl. questions

19:00 – 20:30 Dinner

Thursday, May 10

08:00 – 09:00 Breakfast

09:00 – 10:30 Martin Pirker, UAS (University of Applied Sciences) St. Pölten, Austria

Trusted computing 2

11:00 – 12:30 Nils Gruschka, UiO, PKI and Certificate Security 1

12:30 – 14:00 Lunch

17:00 – 19:00 Nils Gruschka, UiO, PKI and Certificate Security 2

19:00 – 20:30 Dinner

Friday, May 11

08:00 – 9:00 Breakfast

09:00 – 10:00 Qian Guo, UiB, Attacks on QC-MDPC based post-quantum cryptography

Checkout etc.

10:30 – 12:30 Audun Jøsang, UiO, Threat of quantum computing against current crypto solutions, and possible mitigations

12:30 – 14:00 Lunch

Departure