

Program: COINS - Winter School, FINSE, May 5-10, 2019

Sunday, May 5

21:00 Welcome Dinner

Monday, May 6

08:00 – 09:00 Breakfast

09:00 – 09:05 **Øyvind Ytrehus**, Simula UiB, Welcome

09:05 – 10:15 **Dietmar Bremser**, German Federal Office for Information Security (BSI)
Security Certification and Standardization Caught in the Act - A Briefing beyond the Lecture Book's Onepager

10:15 – 10:45 Coffee break

10:45 – 12:30 **Dietmar Bremser**, German Federal Office for Information Security (BSI)
POWERD - a Critical Discourse on the Economics of Security Standardization and Certification

12:30 – 14:00 Lunch

17:00 – 19:00 **László Erdódi**, University of Oslo, *Ethical hacking*

19:00 – 20:30 Dinner

Tuesday, May 7

08:00 – 09 :00 Breakfast

09:00 – 10:30 **Joan Daemen**, Radboud University in Nijmegen, *Symmetric cryptography 2.0*

10:30 – 11.00 Coffee break

11:00 – 12:30 **László Erdódi**, University of Oslo, *Ethical hacking*

12:30 – 14:00 Lunch

14:00 – 15:30 Visit to Rallarmuseet

17.00 – 18:40 Presentations by the participants (I)

- Jan William Johnsen, *"Digital Forensics Report for Dagens Næringsliv"*
- Mazaher Kianpour, *"Modeling and Simulating Information Security Economics for Business Decision Making"*
- Merve Bas Seyyar, *"Privacy by Design (PbD) in Large Scale Digital Forensics"*
- Benjamin J. Knox, *"Cyber Power Praxis: a study of ways to improve understanding and governance in the Cyber Domain"*
- Eivind Kristoffersen, *"Towards a Smart Circular Economy – how companies can use digital technologies to leverage the transformation to more data-driven and circular business models"*

19:00 – 20:30 Dinner

20:30 – 21:50 Presentations by the participants (II)

- Farzane Karami, *"Information-flow security"*
- Jin Zhang, *"Challenges in testing and verifying NN-based safety-critical control software"*
- Muhammad Mudassar Yamin, *"Detecting Windows Based Exploit Chains by Means of Event Correlation and Process Monitoring"*
- Ali Khodabakhsh, *"Automated Authentication of Audiovisual Contents: A Biometric Approach"*

Wednesday, May 8

08:00 – 09:00 *Breakfast*

09:00 – 10:30 **Joan Daemen**, Radboud University in Nijmegen, *Symmetric cryptography 2.0*

10:30 – 11:00 *Coffee break*

11:00 – 12:30 **Martijn Stam**, Simula UiB, *Differential Power Analysis with Key*

Ranking/Enumeration

12:30 – 14:00 *Lunch*

14:15 – 15:30 (*Coins steering committee meeting*)

17:00 – 18:40 *Presentations by the participants (III)*

- Shuang Wu, “*Hash Time Lock Contract Analysis*”
- Ávald Áslaugson Sommervoll, “*Genetic algorithm attack on the Enigmas plugboard*”
- Isaac Canales-Martinez, “*On the cryptanalysis of LFSR based stream ciphers*”
- Diana Davidova, “*Niho bent functions and o-equivalence*”
- Thor Tunge, “*Voting with Commitments*”

19:00 – 20:30 *Dinner*

20:30 – 21:50 *Presentations by the participants (IV)*

- Adam Szekeres, “*Human motivation and the security of Internet of Things*”
- Ahmed Amro, “*Communication and Cybersecurity of Autonomous Passenger Ferry*”
- Georgios Kavallieratos, “*Cyber-attacks against the autonomous ship*”
- Nektaria Kaloudi, “*Cybersecurity, safety, and resilience of smart cities*”

Thursday, May 9

08:00 – 09:00 *Breakfast*

09:00 – 11:00 **Adi Shamir**, Weizmann Institute of Science,

The Insecurity of Machine Learning: Problems and Solutions

11:00 – 11:30 *Coffee break*

11:30 – 12:30 **Bart Preneel**, University of Leuven,

Cryptocurrencies and Distributed Consensus

12:30 – 14:00 *Lunch*

17:00 – 19:00 **Bart Preneel**, University of Leuven, *IoT Security Challenges*

19:00 – 20:30 *Dinner*

Friday, May 10

08:00 – 9:00 Breakfast

*09:00 – 10:30 **Lilya Budaghyan**, University of Bergen,
On Optimal Cryptographic Functions*

10:30 – 11.00 Coffee break

*11:00 – 12:28 **Martijn Stam**, Simula UiB, Untagging Tor: Modelling Onion Encryption*

*12:28 – 12:30 **Øyvind Ytrehus**, Simula UiB, Conclusion/farewell*

12:30 – 14:00 Lunch

Departure