KU LEUVEN

Summer School

on Design and security of cryptographic algorithms and devices for real-world applications

Šibenik, Croatia, June 1-7, 2014

http://summerschool-croatia14.cs.ru.nl

Summer school: facts

- 2 previous editions took place in Albena, Bulgaria
  - 2011: ECRYPT2 NoE summer school
  - 2013: Design and Security of Cryptographic Functions, Algorithms and Devices
- This edition is co-organized by: RU Nijmegen, KU Leuven, University of Zagreb and TU Denmark

Location: Šibenik, Croatia

KU LEUVEN

Summer school: topics

- Block ciphers and Hash functions
- Differential and linear cryptanalysis
- Implementation attacks
- Fault injection attacks
- Countermeasures for physical attacks
- Secure Hardware
- Lightweight cryptography
- Real-world embedded security protocols

Confirmed speakers

- Andrey Bogdanov, DTU
- Anne Canteaut, Inria
- Srdjan Capkun, ETH
- Joan Daemen, ST Microelectronics
- Orr Dunkelman, Haifa
- Lars Knudsen, DTU
- Marcel Medwed, NXP
- María Naya-Plasencia, Inria
- Christian Rechberger, DTU
- Kenny Paterson, RHUL
- Svetla Nikova, KUL
- Bart Preneel, KUL
- Lejla Batina, RUN
- Viktor Fischer, St. Etienne
- Michael Hutter, TUG
- Konstantinos Markantonakis, RHUL
- Nele Mentens, KUL
- Francesco Regazzoni, Alari
- Peter Schwabe, RU
- Nikolas Sklavos, Patras
- Ingrid Verbauwhede, KUL
- Gregor Leander, RUB
- Florian Mendel, TUG
- Elena Andreeva, KU Leuven

KU LEUVEN