

LACS Research Days II

Schedule

Day 1: Tuesday, March 2nd

Location: Salle des Conseils

13:00-13:05 Opening remarks

Session 1, 13:05-14:05

13:05-13:25 Wojtek Jamroga

Reasoning about Strategic Properties of Multi-Agent Programs

13:25-13:45 Tim Muller

Trust Algebra

13:45-14:05 Baptiste Alcalde

TBA

14:05-14:20 *Coffee break*

Session 2, 14:20-15:30

14:20-14:40 Bin Zhang

Analysis of SNOW 3G⁺ Resynchronization Mechanism

14:40-15:00 Ivica Nikolić

Automatic Search of Differentials in Byte-Oriented Ciphers

15:00-15:30 Jean-François Gallais, Ilya Kizhvatov

Cache-Based Power Analysis of AES

15:30-16:00 *Coffee break*

Session 3, 16:00-17:00

16:00-16:20 Naipeng Dong

TBA

16:20-16:40 Ton van Deursen

Privacy of RFID Protocols

16:40-17:00 Saša Radomirović

Security Protocols

Day 2: Wednesday, March 3rd

Location: Salle des Conseils

Session 4, 13:00-14:00

13:00-13:20 David Galindo

Some Results on Public-Key Encryption

13:20-13:40 Avradip Mandal

Indifferentiability

13:40-14:00 Jean-Sébastien Coron

Deterministic Hashing into Elliptic Curves and Applications

14:00-14:20 *Coffee break*

Session 5, 14:20-15:30

14:20-14:40 Hugo Jonker

TBA

14:40-15:10 Barbara Kordy, Patrick Schweitzer

Attack-Defense Trees

15:10-15:30 Matthijs Melissen

A Game Theoretical Semantics for Attack-Defense Trees

15:30-16:00 *Coffee break*

Session 6, 16:00-17:00

16:00-16:20 Johann Großschädl

Constructing a Highly Leak-Resistant Stream Cipher from a Leaking Block Cipher

16:20-16:40 Dmitry Khovratovich

Rotational Cryptanalysis

16:40-17:00 Ralf-Philipp Weinmann

TBA
