Eindhoven Institute for the Protection of Systems and Information

# Cryptography Working Group

---

## Friday, February 7, 2020

Opleidingsruimte-Utrecht
(http://opleidingsruimte-utrecht.nl/Routebeschrijving-Mariaplaats-3.pdf)
Mariaplaats 3, Utrecht

## Program

**10.45 – 11.30 hrs.** **Aldo Gunsing** (*RU Nijmegen*)
Deck-Based Wide Block Cipher Modes and an Exposition of the Blinded Keyed Hashing Model

**11.30 - 11.45 hrs.** *Coffee / tea break*

**11.45 - 12.30 hrs.** **Douglas Stebila** (*Univ. of Waterloo, Canada*)
Exploring Post-Quantum Cryptography in Internet Protocols

**12.30 - 14.00 hrs.** *Lunch break (lunch not included)*

**14.00 - 14.45 hrs.** **Florian Hahn** (*Univ. of Twente*)
Secure Data Aggregation Grouped by Multiple Attributes

**14.45 - 15.00 hrs.** *Coffee / tea break*

**15.00 - 15.45 hrs.** **Tomer Ashur** (*TU Eindhoven*)
Design of Symmetric-Key Primitives for Advanced Cryptographic Protocols

---

**Dates CWG 2020: February 7**

*EiPSI, P.O. Box 513, 5600 MB Eindhoven, The Netherlands*
*Telephone: +31 (0)40 247 2254, E-mail: secdm@tue.nl, http://www.win.tue.nl/eipsi/seminars.html*