Eindhoven Institute for the Protection of Systems and Information

# Cryptography Working Group

---

## Friday, April 12, 2019

De Kargadoor (http://www.kargadoor.nl/utrecht/zaalverhuur.html)
Oudegracht 36, Utrecht

## Program

**10.45 – 11.30 hrs.** **Michael Meyer** (*Hochschule RheinMain*),
On Lions and Elligators: An efficient constant-time implementation of CSID

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

**11.45 - 12.30 hrs.** **Tobias Oder** (*Ruhr Univ. Bochum*),
Masking NewHope at Arbitrary Orders

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

**14.00 - 14.45 hrs.** **Thom Wiggers** (*RU Nijmegen*),
Solving LPN using Large Covering Codes

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

**15.00 - 15.45 hrs.** **Richard Petri** (*SIT Fraunhofer*),
Implementing Side-Channel Protections for ARX Ciphers

---

**Future dates CWG 2019: TBA**

*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*