Eindhoven Institute for the Protection of Systems and Information

Cryptography Working Group

Friday, May 25, 2018

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

Program

10.45 – 11.30 hrs. **Boris Škorić** (*TU/e*)
Quantum stuff with optical PUFs

11.30 - 11.45 hrs. *Coffee / tea break*

11.45 - 12.30 hrs. **Martijn Stam** (*Univ. of Bristol*),
Untagging Tor: A Formal Treatment of Onion Encryption
(joint work with Jean Paul Degabriele)

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

14.00 - 14.45 hrs. **Kit Smeets** (*UCL*),
Rounded Gaussians — Fast and Secure Constant-Time Sampling for Lattice-Based Crypto

14.45 - 15.00 hrs. *Coffee / tea break*

15.00 - 15.45 hrs. **Jason Donenfeld** *(Edge Security*),
Considerations in designing WireGuard

Dates CWG 2018: May 25, September 14

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