Eindhoven Institute for the Protection of Systems and Information

Cryptography Working Group

Friday, November 17, 2017

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

Program

10.45 – 11.30 hrs. **Léon Groot Bruinderink** (*TU/e),*
Sliding right into disaster: Left-to-right sliding windows leak

11.30 - 11.45 hrs. *Coffee / tea break*

11.45 - 12.30 hrs. **Peter Pessl** (*TU Graz*),
Single-Trace Side-Channel Attacks on Masked Lattice-Based Encryption

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

14.00 - 14.45 hrs. **Robin Kwant** and **Kimberley Thissen** *(both TU/e),*
Lattice Klepto: Turning Post-Quantum Crypto Against Itself

14.45 - 15.00 hrs. *Coffee / tea break*

15.00 - 15.45 hrs. **Kai-Chun Ning** *(TU/el)*,
An Adaption of the Crossbred Algorithm for Solving Multivariate Quadratic Systems over F_2 on GPUs

---

Dates CWG 2017: March 24, June 16, September 8 and November 17

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