Eindhoven Institute for the Protection of Systems and Information

Cryptography Working Group

Friday, December 16, 2016

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

Program

10.45 – 11.30 hrs. **Léon Groot Bruinderink** *(TU/e)*,
Flush, Gauss, and Reload - A Cache-attack on the BLISS Lattice-based Signature Scheme

11.30 - 11.45 hrs. *Coffee / tea break*

11.45 - 12.30 hrs. **Joost Renes** *(RU Nijmegen)*,
Efficient compression of SIDH public keys

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

14.00 - 14.45 hrs. **Dan Bernstein** *(Univ. of Illinois, Chicago / TU/e)*,
How to manipulate curve standards: a white paper for the black hat

14.45 - 15.00 hrs. *Coffee / tea break*

15.00 - 15.45 hrs. **Kostas Papagiannopoulos** *(RU Nijmegen)*,
Bitsliced Masking and ARM: Friends or Foes?

Dates CWG 2016: April 1, May 27, September 16, December 16

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