Eindhoven Institute for the Protection of Systems and Information

Cryptography Working Group

Friday, February 27, 2015

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

Program

10.45 – 11.30 hrs. **Dan Bernstein & Tanja Lange** (*TU/e*),
Batch NFS

11.30 - 11.45 hrs. *Coffee / tea break*

11.45 - 12.30 hrs. **Christiane Peters** (*ENCS*),
Weaknesses in Smart Metering Cryptography

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

14.00 - 14.45 hrs. **Chitchanok Chuengsatiansup** (*TU/e*),
New Diffie-Hellman Speed Records

14.45 - 15.00 hrs. *Coffee / tea break*

15.00 - 15.45 hrs. **Pedro Massolino** (*RU Nijmegen*),
Design and Evaluation of a Post-Quantum Cryptographic Co-Processor

---

Dates CWG 2015: February 27, May 8, September 25, December 11

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