Eindhoven Institute for the Protection of Systems and Information

Cryptography Working Group

Friday, May 22, 2015

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

Program

10.45 – 11.30 hrs. **Peter van Emde Boas** (*ILLC / FNWI / UvA / Bronstee.com Software & Services B.V. Heemstede)*,
The use of Information and Spycraft in Ancient Chinese Warfare

11.30 - 11.45 hrs. *Coffee / tea break*

11.45 - 12.30 hrs. **Leo Ducas** (*CWI*),
Recovering Short Generators of Principal Ideals in Cyclotomic Rings
(joint work with Ronald Cramer, Chris Peikert and Oded Regev)

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

14.00 - 14.45 hrs. **Moritz Neikes** (*RU Nijmegen*),
Fingerprint scheduling for dining-cryptographer networks

14.45 - 15.00 hrs. *Coffee / tea break*

15.00 - 15.45 hrs. **Andreas Hülsing & Peter Schwabe** (*TU/e & RU Nijmegen*),
SPHINCS: practical stateless hash-based signatures

Dates CWG 2015: February 27, May 22, 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