Eindhoven Institute for the Protection of Systems and Information

Cryptography Working Group

Friday, March 24, 2017

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

Program

10.45 – 11.30 hrs. **Joost Rijneveld** *(RU Nijmegen)*,
MQDSS signatures – construction

11.30 - 11.45 hrs. *Coffee / tea break*

11.45 - 12.30 hrs. **Simona Samardjiska** *(RU Nijmegen)*,
MQDSS signatures - security

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

14.00 - 14.45 hrs. **Andreas Hülsing** *(TU/e)*,
Semantic Security and Indistinguishability in the Quantum World

14.45 - 15.00 hrs. *Coffee / tea break*

15.00 - 15.45 hrs. **Christine van Vredendaal** *(TU/e)*,
Short generators without quantum computers: the case of multiquadratics

---

Dates CWG 2017: March 24, June 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