Eindhoven Institute for the Protection of Systems and Information

Cryptography Working Group

Friday, April 1, 2016

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

Program

10.45 – 11.30 hrs. **Tung Chou** (*TU/e*),
QcBits: constant-time small-key code-based cryptography

11.30 - 11.45 hrs. *Coffee / tea break*

11.45 - 12.30 hrs. **Boris Škorić** (*TU/e*),
4x2=8: Unclonable Encryption revisited

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

14.00 - 14.45 hrs. **Joost Renes** (*RU Nijmegen*),
Complete Addition Formulas for Prime Order Elliptic Curves

14.45 - 15.00 hrs. *Coffee / tea break*

15.00 - 15.45 hrs. **Peter Schwabe** (*RU Nijmegen*),
Post-quantum key exchange -- a new hope

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