Eindhoven Institute for the Protection of Systems and Information

Cryptography Working Group

Friday, June 14, 2013

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

Program

10.45 – 11.30 hrs. **Tony Chou** (*TU/e*),
McBits: fast constant-time code-based cryptography

11.30 - 11.45 hrs. *Coffee / tea break*

11.45 - 12.30 hrs. **Marc Stevens** (*CWI*),
Counter-cryptanalysis: analyzing Flame's new collision attack

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

14.00 - 14.45 hrs. **Ruud Pellikaan** (*TU/e*),
Error-correcting pairs and majority coset decoding in public-key crypto systems and secret sharing

14.45 - 15.00 hrs. *Coffee / tea break*

15.00 - 15.45 hrs. **Anna Krasnova** (*RU Nijmegen*),
Elligator: Elliptic curve points indistinguishable from uniform random strings

---

Dates CWG 2013: March 1, June 14, September 6, November 29

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