Eindhoven Institute for the Protection of Systems and Information

Cryptography Working Group

Friday, September 6, 2013

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

Program

10.45 – 11.30 hrs. **Tanja Lange** (*TU/e*),
Factoring RSA keys from certified smart cards: Coppersmith in the wild

11.30 - 11.45 hrs. *Coffee / tea break*

11.45 - 12.30 hrs. **Michael Feiri** (*Univ. Twente*),
The practical weakness of the S/KEY one-time-password system (RFC 1760 and 2289) against brute force attacks

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

14.00 - 14.45 hrs. **Mathias Morbitzer** (*RU Nijmegen*),
TCP Idle Scans in IPv6

14.45 - 15.00 hrs. *Coffee / tea break*

15.00 - 15.45 hrs. **Zekeriya Erkin** (*TU Delft*),
Privacy Preserving Online Services for Dynamic Settings

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