Eindhoven Institute for the Protection of Systems and Information

Cryptography Working Group

Friday, December 11, 2015

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

Program

10.45 – 11.30 hrs. **Baris Ege** (*RU Nijmegen)*,
Near Collision Side Channel Attacks

11.30 - 11.45 hrs. *Coffee / tea break*

11.45 - 12.30 hrs. **Jon Solworth** (*Univ. of Illinois at Chicago)*,
Some thoughts on composition for security

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

14.00 - 14.45 hrs. **Isis Agora Lovecruft** (*Tor Project*),
Tor's Circuit Level Crypto, Hacks, and the
Proposed Change to an Authenticated Encryption Cipher

14.45 - 15.00 hrs. *Coffee / tea break*

15.00 - 15.45 hrs. **Louiza Papachristodoulou** (*RU Nijmegen*),
Online Template Attacks on ECC

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