Eindhoven Institute for the Protection of Systems and Information

Cryptography Working Group

Friday, September 5, 2014

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

Program

10.45 – 11.30 hrs. **Björn Haase** (*E+H Conducta)*,
Integrating asymmetric crypto in process industry applications
Adapting arithmetics to the restrictions imposed by explosion protection and field bus systems

11.30 - 11.45 hrs. *Coffee / tea break*

11.45 - 12.30 hrs. **Christine van Vredendaal** (*TU/e*),
Kangaroos in Side Channel Attacks

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

14.00 - 14.45 hrs. **Kostas Papagiannopoulos** (*RU Nijmegen*),
Throughput in A slices: the case of PRESENT, PRINCE and KATAN64 ciphers

14.45 - 15.00 hrs. *Coffee / tea break*

15.00 - 15.45 hrs. **Tung Chou** (*TU/e*),
Faster binary-field multiplication and faster binary-field MACs

---

Dates CWG 2014: February 28, May 23, September 5, December 5

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