Eindhoven Institute for the Protection of Systems and Information

Cryptography Working Group

Friday, September 30, 2011

Trianon Zalencentrum (http://www.trianon-zalen.nl/)
Oudegracht 252, Utrecht

Program

10.45 – 11.30 hrs. **Michael Naehrig** (*TU/e*),
Can homomorphic encryption be practical?

11.30 - 11.45 hrs. *Coffee / tea break*

11.45 - 12.30 hrs. **Ilze Eichhorn** (*Intrinsic-ID*),
Hardware Intrinsic Security

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

14.00 - 14.45 hrs. **Roel Verdult** (*RU Nijmegen*),
Exposing iClass Key Diversification

14.45 - 15.00 hrs. *Coffee / tea break*

15.00 - 15.45 hrs. **Joop van de Pol** (*TU/e*),
Lattice-based Cryptography

Seminar dates 2011:
September 30
December 2

EIDMA, P.O. Box 513, 5600 MB Eindhoven, The Netherlands
Telephone: +31 40 247 2254, , E-mail: seccc@tue.nl, http://www.win.tue.nl/eipsi/seminars.html