



Eindhoven Institute for
the Protection of Systems
and Information

Cryptography Working Group

Friday, September 25, 2015

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

Program

- 10.45 – 11.30 hrs.** **Fabian van den Broek** (*RU Nijmegen*),
Defeating IMSI catchers
- 11.30 - 11.45 hrs.** *Coffee / tea break*
- 11.45 - 12.30 hrs.** **Ko Stoffelen** (*RU Nijmegen*),
Intrinsic side-channel analysis resistance and efficient masking
- 12.30 - 14.00 hrs.** *Lunch break (lunch not included)*
- 14.00 - 14.45 hrs.** **Ruben Niederhagen** (*TU/e*),
Breaking ECC2-113 – joy and pain of hardware design
- 14.45 - 15.00 hrs.** *Coffee / tea break*
- 15.00 - 15.45 hrs.** **Thijs Laarhoven** (*TU/e*),
Speeding up lattice sieving with nearest neighbor techniques
-

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>