



Eindhoven Institute for
the Protection of Systems
and Information

Cryptography Working Group

Friday, May 23, 2014

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

Program

- 10.45 – 11.30 hrs.** **Christian Dörr** (*TU Delft*),
The Ineffectiveness of Network Security Policies against Advanced Cyber
Threats, Rethinking Security Practices after Stuxnet & Co
- 11.30 - 11.45 hrs.** *Coffee / tea break*
- 11.45 - 12.30 hrs.** **Nadia Heninger** (*Univ. of Pennsylvania*),
Approximate common divisors via lattices
- 12.30 - 14.00 hrs.** *Lunch break (lunch not included)*
- 14.00 - 14.45 hrs.** **Roel Verdult**,
Do you trust the cryptography used in your devices?
- 14.45 - 15.00 hrs.** *Coffee / tea break*
- 15.00 - 15.45 hrs.** **Andreas Hülsing** (*TU/e*)
Practical Forward Secure Signatures using Minimal Security Assumptions
-

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>