



Eindhoven Institute for
the Protection of Systems
and Information

Cryptography Working Group

Friday, March 1, 2013

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

Program

- 10.45 – 11.30 hrs.** **Thijs Laarhoven** (*TU/e*),
The Shortest Vector Problem in Lattices Faster Using Quantum Search
- 11.30 - 11.45 hrs.** *Coffee / tea break*
- 11.45 - 12.30 hrs.** **Wouter Lueks** (*RU Nijmegen*),
Forward Secure and Efficient Distributed Encryption
- 12.30 - 14.00 hrs.** *Lunch break (lunch not included)*
- 14.00 - 14.45 hrs.** **Francesco Regazzoni** (*ALaRI - USI, Lugano*),
Towards the Automatic Application of Countermeasures Against
Physical Attacks
- 14.45 - 15.00 hrs.** *Coffee / tea break*
- 15.00 - 15.45 hrs.** **Peter Schwabe** (*RU Nijmegen*),
NaCl on small devices

Dates CWG 2013: March 1, June 14, September 6, November 29

Telephone: +31 (0)40 247 2254, , E-mail: secdm@tue.nl, <http://www.win.tue.nl/eipsi/seminars.html>