



Eindhoven Institute for  
the Protection of Systems  
and Information

## Cryptography Working Group

---

**Friday, June 8, 2012**

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

### Program

- 10.45 – 11.30 hrs.** **Jurjen Bos** (*Equens*),  
Public key cryptography on the Internet
- 11.30 - 11.45 hrs.** *Coffee / tea break*
- 11.45 - 12.30 hrs.** **Daniel J. Bernstein and Tanja Lange** (*TU/e*),  
Two grumpy giants and a baby
- 12.30 - 14.00 hrs.** *Lunch break (lunch not included)*
- 14.00 - 14.45 hrs.** **Begul Bilgin** (*KU Leuven*),  
Threshold Implementations of all 3x3 and 4x4 S-boxes
- 14.45 - 15.00 hrs.** *Coffee / tea break*
- 15.00 - 15.45 hrs.** **Niek Bouman** (*CWI*),  
An Introduction to Quantum Cryptography

---

**Dates CWG 2012: March 9, June 8, September 21, November 30**

EiPSI, P.O. Box 513, 5600 MB Eindhoven, The Netherlands

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