



Eindhoven Institute for  
the Protection of Systems  
and Information

## Cryptography Working Group

---

**Friday, November 29, 2013**

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

### Program

- 10.45 – 11.30 hrs.** **Paulo Barreto** (*Univ. of São Paulo*),  
Code-based cryptosystems targeting small embedded devices
- 11.30 - 11.45 hrs.** *Coffee / tea break*
- 11.45 - 12.30 hrs.** **Jurjen Bos** (*Equens*),  
Three paradoxical subjects from cryptography practice
- 12.30 - 14.00 hrs.** *Lunch break (lunch not included)*
- 14.00 - 14.45 hrs.** **Gergely Alpar** (*RU Nijmegen*),  
Crypto and Beyond: from ABCs to IRMA
- 14.45 - 15.00 hrs.** *Coffee / tea break*
- 15.00 - 15.45 hrs.** **Dan Bernstein** (*TU/e*),  
Failures of secret-key cryptography

---

**Dates for the CWG-meetings in 2014 will soon be announced.**

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>