



## EIDMA/DIAMANT Cryptography Working Group

---

**Friday, October 2, 2009**

Trianon Zalencentrum ( <http://www.trianon-zalen.nl/> )  
Oudegracht 252, Utrecht

### PROGRAM

- 10.45 – 11.30 hrs.** **Cees Jansen** (Compumatica),  
Towards Mickey's LEB.
- 11.30 - 11.45 hrs.** *Coffee / tea break.*
- 11.45 - 12.30 hrs.** **Jurjen Bos** (Interpay),  
Leakage-Resilient Storage.
- 12.30 - 14.00 hrs.** *Lunch break (lunch not included).*
- 14.00 - 14.45 hrs.** **Michael Naehrig** (TU/e)  
Efficient computation of pairings on elliptic curves.
- 14.45 - 15.00 hrs.** *Coffee / tea break.*
- 15.00 - 15.45 hrs.** **Ruden Teuben** (NBV Cistron),  
Related-Key attacks on AES.

### Dates of the seminar in 2009:

February 20, October 2 and December 4.