# EIDMA/DIAMANT Cryptography Working Group

---

## Friday, December 4, 2009

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

## PROGRAM

**10.45 – 11.30 hrs.** **Jeroen Doumen** (*Irdeto*),
Recent attacks on AES: should we be worried?

**11.30 - 11.45 hrs.** *Coffee / tea break*

**11.45 - 12.30 hrs.** **Peter Schwabe** (*TU/e*),
Implementing Wagner's generalized birthday attack.

**12.30 - 14.00 hrs.** *Lunch break (lunch not included)*

**14.00 - 14.45 hrs.** **Lejla Batina** (*RU Nijmegen*)
Differential cluster analysis.

**14.45 - 15.00 hrs.** *Coffee / tea break*

**15.00 - 15.45 hrs.** **Dan Bernstein** (*Univ. of Illinois at Chicago*),
Breaking ECC2K-130.

**The dates of the seminar in 2010 will be announced soon.**

---

*EIDMA, P.O. Box 513, 5600 MB Eindhoven, The Netherlands*

*Telephone: +31 40 247 5141, Telefax: +31 40 243 5810, E-mail: seccc@tue.nl, http://www.win.tue.nl/math/eidma*