EIDMA/DIAMANT Cryptography Working Group

Friday February 15, 2008

Regardz Meeting Center La Vie
Lange Viestraat 351, Utrecht

See http://www.lavie.nl/ (Contact en route) for a route description and information about parking possibilities.

PROGRAM

10.45 – 11.30 hrs. **Karin Poels** (NLNCSA),
Recent work of Dubois, Fouque, Shamir & Stern:
Cryptanalysis of SFLASH; from a standard for fast signatures to an attack that forges fast signatures for any message.

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

11.45 - 12.30 hrs. **Peter Birkner** (TU/e),
Edwards Curves and the ECM Factorisation Method.

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

14.00 - 14.45 hrs. **Bert den Boer**,
A Simple Side-Channel Attack on RSA.

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

15.00 - 15.45 hrs. **Tomas Toft** (TU/e),
Practical MPC for practical problems.

Dates of the seminar in 2007:
February 15, October 3 and December 7.

GRAND OPENING of EiPSI (see http://www.win.tue.nl/eipsi):

April 21 and April 22.

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

Telephone: +31 40 247 3121, Telefax: +31 40 243 5810, E-mail: eidma@tue.nl, http://www.win.tue.nl/math/eidma