EIDMA/DIAMANT Cryptography Working Group

Friday, October 3, 2008

Regardz Meeting Center La Vie
Lange Viestraat 351, Utrecht

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

PROGRAM

10.45 – 11.30 hrs. **Rob van Esch** (*TU/e*),
Provable security in Cryptography. Reductionist security arguments for EC-KCDSA.

11.30 - 11.45 hrs. *Coffee / tea break*

11.45 - 12.30 hrs. **Jurjen Bos** (*Equens*),
Zero knowledge and Sudoku.

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

14.00 - 14.45 hrs. **Eric Verheul** (*PricewaterhouseCoopers / Radboud Universiteit Nijmegen*),
An analysis of the vector decomposition problem in Elliptic curve groups (joint work with Steven Galbraith).

14.45 - 15.00 hrs. *Coffee / tea break*

15.00 - 15.45 hrs. **Cees Jansen** (*DeltaCrypto*),
The Linear Equivalence Bias in Jump Controlled Linear Finite State Machines.

Seminar dates 2008:
February 15, October 3 and December 7.

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