



EIDMA/DIAMANT Cryptography Working Group

Friday October 5, 2007

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.** **Alexander May** (TU Darmstadt),
Improving Hastad's RSA broadcast attack.
- 11.30 - 11.45 hrs.** *Coffee / tea break.*
- 11.45 - 12.30 hrs.** **Dennis Hofheinz** (CWI),
Secure Hybrid Encryption from Weakened Key Encapsulation
(joint work with Eike Kiltz).
- 12.30 - 14.00 hrs.** *Lunch break (lunch not included).*
- 14.00 - 14.45 hrs.** **Tanja Lange** (TU/e),
Edwards curves for cryptography.
- 14.45 - 15.00 hrs.** *Coffee / tea break.*
- 15.00 - 15.45 hrs.** **Henk van Tilborg** (TU/e),
Communication graphs, key graphs, and Harary graphs.

Dates of the seminar in 2007:

February 2, May 4, October 5, and December 7.

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>