



EIDMA/DIAMANT Cryptography Working Group

Friday February 20, 2009

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

PROGRAM

10.45 – 11.30 hrs. **Lejla Batina** (KU Leuven),
Recent Developments in Side-Channel attacks.

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

11.45 - 12.30 hrs. **José Villegas Bautista** (TU/e),
Verifiable Rotators of Homomorphic Encryptions.

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

14.00 - 14.45 hrs. **Balazs Dosa** (TU/e)
Traitor Tracing in Broadcast Networks.

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

15.00 - 15.45 hrs. **Christiane Peters** (TU/e),
Advances in Information-Set Decoding.

Dates of the seminar in 2009:

February 20, October 2 and December 4.

First Anniversary of EiPSI (<http://www.win.tue.nl/eipsi/anniversary.html>):

April 24, 2009.