Eindhoven Institute for the Protection of Systems and Information

Cryptography Working Group

Friday, March 9, 2012

NOTICE DIFFERENT LOCATION!!

De Kargadoor (http://www.kargadoor.nl/utrecht/zaalverhuur.html)
Oudegracht 36, Utrecht

Program

10.45 – 11.30 hrs. **Lejla Batina** (*KU Leuven*),
Getting More from PCA: First Results of Using Principal Component Analysis for Extensive Power Analysis

11.30 - 11.45 hrs. *Coffee / tea break*

11.45 - 12.30 hrs. **Peter Schwabe** (*Academia Sinica, Taipei*),
How to use the negation map in the Pollard rho method

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

14.00 - 14.45 hrs. **Klaus Kursawe** (*RU Nijmegen*),
TBA

14.45 - 15.00 hrs. *Coffee / tea break*

15.00 - 15.45 hrs. **Marc Stevens** (*CWI*),
Joint local-collision analysis of SHA-1

Dates CWG 2012: March 9, June 8, September 21, November 30

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

Telephone: +31 (0)40 247 2254, , E-mail: secdm@tue.nl, http://www.win.tue.nl/eipsi/seminars.html