Eindhoven Institute for the Protection of Systems and Information

Cryptography Working Group

Friday, September 21, 2012

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

Program

10.45 – 11.30 hrs. **Jan-Jaap Oosterwijk** (*TU/e*),
Dynamic Traitor Tracing for Arbitrary Alphabets: Divide and Conquer

11.30 - 11.45 hrs. *Coffee / tea break*

11.45 - 12.30 hrs. **Gergely Alpar** (*RUN*),
Designated attribute proofs

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

14.00 - 14.45 hrs. **Baris Ege**
Differential Scan Attack on AES with X-Tolerant and X-Masked Test

14.45 - 15.00 hrs. *Coffee / tea break*

15.00 - 15.45 hrs. **Craig Costello** (*TU/e*),
Fast implementations in genus 2

Dates CWG 2012: March 9, June 8, September 21, December 7

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