Eindhoven Institute for the Protection of Systems and Information

Cryptography Working Group

Friday, June 16, 2017

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

Program

10.45 – 11.30 hrs. **Yval Yarom** (*Univ. of Adelaide)* and **Léon Groot Bruinderink** (*TU/e)*
To BLISS-B or not to be - Attacking strongSwan's Implementation of Post-Quantum Signatures

11.30 - 11.45 hrs. *Coffee / tea break*

11.45 - 12.30 hrs. **Bart Mennink** (*RU Nijmegen*),
Encrypted Davies-Meyer and Its Dual: Towards Optimal Security Using Mirror Theory

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

14.00 - 14.45 hrs. **Daniel Genkin** *(Univ. of Pennsylvania/Univ. of Maryland)*,
Acoustic Cryptanalysis of RSA

14.45 - 15.00 hrs. *Coffee / tea break*

15.00 - 15.45 hrs. **Marc Stevens** *(CWI)*,
Finding the first collision for SHA-1

Dates CWG 2017: March 24, June 16, September 8 and November 17

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