Eindhoven Institute for the Protection of Systems and Information

Cryptography Working Group

Friday, November 29, 2019

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

Program

10.45 – 11.30 hrs. **Jelle Don** (*CWI*)
Security of the Fiat-Shamir Transformation in the Quantum Random-Oracle Model

11.30 - 11.45 hrs. *Coffee / tea break*

11.45 - 12.30 hrs. **Andreas Hülsing** (*TU Eindhoven*)
Decisional second-preimage resistance: When does SPR imply PRE?

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

14.00 - 14.45 hrs. **Benoît Viguier** (*RU Nijmegen*)
A Coq proof of the correctness of X25519 in TweetNaCl

14.45 - 15.00 hrs. *Coffee / tea break*

15.00 - 15.45 hrs. **Marloes Venema** (*RU Nijmegen*)
How to Break Attribute-Based Encryption

Dates CWG 2019: April 12, September 6, November 29

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