Eindhoven Institute for the Protection of Systems and Information

Cryptography Working Group

Friday, September 8, 2017

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

Program

10.45 – 11.30 hrs. **Daan Leermakers** (*TU/e)*
Optimal attacks on qubit-based Quantum Key Recycling

11.30 - 11.45 hrs. *Coffee / tea break*

11.45 - 12.30 hrs. **Gustavo Souza Banegas** (*TU/e*),
Preimage search using low cost communication parallel Grover algorithm

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

14.00 - 14.45 hrs. **Benoit Viguier** *(RU Nijmegen)*,
GIMLI: a cross-platform permutation

14.45 - 15.00 hrs. *Coffee / tea break*

15.00 - 15.45 hrs. **Stacey Jeffery** *(CWI)*,
Classical and Quantum Meet-in-the-Middle Attacks for
The Mersenne Number Cryptosystem

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