Eindhoven Institute for the Protection of Systems and Information

Cryptography Working Group

Friday, November 9, 2018

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

Program

10.45 – 11.30 hrs. **Leo Ducas** (*CWI)*
The General Sieve Kernel and New Records in Lattice Reduction

11.30 - 11.45 hrs. *Coffee / tea break*

11.45 - 12.30 hrs. **Stacey Jefferey** (*CWI, QuSoft*),
On non-adaptive quantum chosen-ciphertext attacks and Learning with Errors

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

14.00 - 14.45 hrs. **Christian Majenz** (*CWI, QuSoft, UvA*),
Quantum-secure message authentication via blind-unforgeability

14.45 - 15.00 hrs. *Coffee / tea break*

15.00 - 15.45 hrs. **Matthias Kannwischer** *(RU*),
Faster multiplication in $Z_{2^m}[x]$ on Cortex-M4 to speed up NIST PQC candidates

---

Dates CWG 2019: TBA

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