Eindhoven Institute for the Protection of Systems and Information

# Cryptography Working Group

---

## Friday, September 6, 2019

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

## Program

**10.45 – 11.30 hrs.** **Frank van den Bosch-Blom** (*TU/e*)
Efficient Secure Ridge Regression from Randomized Gaussian Elimination

**11.30 - 11.45 hrs.** *Coffee / tea break*

**11.45 - 12.30 hrs.** **Benjamin Wesolowski** (*CWI*)
Verifiable delay functions

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

**14.00 - 14.45 hrs.** **Ko Stoffelen** (*RU Nijmegen*)
pqm4: Testing and Benchmarking NIST PQC on ARM Cortex-M4

**14.45 - 15.00 hrs.** *Coffee / tea break*

**15.00 - 15.45 hrs.** **Thijs Laarhoven** (*TU/e*)
Approximate Voronoi cells for the closest vector problem, revisited

---

**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*