FOQUS – Frontiers of Quantum-Safe Cryptography

Saturday April 29

- 8 :30-9 :30 Registration and Welcome Coffee
- 9 :30 - 11 : 45 Session 1
    - 9 :30-10 :15
    - Michele Mosca (IQC Waterloo)
    - *The urgency of quantum-safe cryptography*
    - 10 :15-11 :00
    - Vadim Lyubashevsky (IBM Zurich)
    - *Standardizing Lattice Cryptography*
    - 11 :00-11 :45
    - Leo Ducas (CWI Amsterdam)
    - *Short Stickelberger Class Relations and application to Ideal-SVP*
- 14 :00 - 15: 30 Session 2
    - 14 :00-14 :45
    - Christian Schaffner (U Amsterdam)
    - *Quantum Cryptography Beyond Quantum Key Distribution*
    - 14 :45-15 :30
    - Gaëtan Leurent (INRIA Paris)
    - *Breaking Symmetric Cryptosystems Using Quantum Algorithms*
- 15 :30 - 16: 00 Coffee break
- 16 :00 - 17 : 30 Session 3
    - 16 :00-16 :45
    - Dominique Unruh (U Tartu)
    - *Post-quantum security of hash functions*
    - 16 :45-17 :30
    - Stacey Jeffery (CWI Amsterdam)
    - *Quantum algorithms for the subset-sum problem*

Sunday April 30

- 8 :30-9 :15 Coffee break

- 9 :15 - 10 : 45 Session 4

    - 9 :30-10 :15
    - Norbert Lütkenhaus (IQC Waterloo)
    - *How secure are Quantum Key Distribution protocols and their implementations?*

    - 10 :15-11 :00
    - Mehdi Tibouchi (NTT Labs, Tokyo)
    - *Physical attacks against lattice-based schemes*

- 10 :45 - 11: 15 Coffee break

- 11 :15 - 12 : 45 Session 5

    - 9 :30-10 :15
    - Stephanie Wehner (QuTech Delft)
    - *Talk title be announced*

    - 10 :15-11 :00
    - Jean-François Biasse (U South Florida)
    - *Finding approximate short vectors in certain ideal lattices with a quantum computer*.