

# Department of Applied and Computational Mathematics and Statistics Colloquium



Joachim Rosenthal  
Institute of Mathematics  
University of Zurich

## *Overview of Post-Quantum Cryptography with an Emphasis on Code based Systems*

With the realization that a quantum computer would make many practically used public key cryptographic systems obsolete (compare with the reports [1, 2]) it became an important research topic to design public key systems which are expected to be secure even if a powerful quantum computer would exist.

In the talk, we will explain about the major possible candidates for post-quantum cryptography and we will then concentrate on so called code based systems which were first proposed in 1978 by Robert McEliece who demonstrated how the hardness of decoding a general linear code up to half the minimum distance can be used as the basis for a public key crypto system.

**Wednesday, October 16, 2019**

**4:30 PM – 5:30 PM**

**127 Hayes-Healy Center**

Colloquium Tea 4:00 PM to 4:30 PM 101A Crowley Commons Room