HARVARD UNIVERSITY
17 Oxford Street
Cambridge, MA 02138

Mathematical Picture Language Seminar

Tuesday, April 12

9:30 a.m. Boston time

Post-quantum cryptography and post-quantum key exchange based on the LWE and RLWE problems

Jintai Ding

Beijing Institute of Mathematical Sciences and Applications
& Tsinghua University

Abstract: Public key cryptosystems (PKC) are a critical part of the foundation of modern communication systems. Shor's algorithm shows that the existing PKC like Diffie-Hellmann key exchange, RSA and ECC can be broken by a quantum computer. To prepare for the coming age of quantum computing, we need to build new PKCs that can resist quantum computer attacks. We will give a brief introduction to post-quantum cryptography and present a practical and provably secure (authenticated) key exchange protocol based on the learning with errors problems. We will explain that LWE-based key exchanges are variants of this fundamental design and explain how to use the signal function invented for KE for authentication schemes. Then we will discuss key reuse attacks on those key exchanges.

Zoom QR Code & Link:
https://harvard.zoom.us/j/779283357?pwd=MitXVm1pYUlJVzZqT3lwV2pCT1ZUQT09

https://mathpicture.fas.harvard.edu/seminar