Abstract:

All widely-deployed public-key encryption algorithms are threatened by the possibility of a quantum computer that can run Shor's algorithm. The most popular approach for future, "post-quantum" encryption is the "learning with errors" (LWE) problem, and its variants Ring-LWE, Module-LWE, Integer-Module-LWE, etc. Compared to elliptic curves, LWE systems are tricky to parameterize. The relationship between the parameters and the security they provide is complex, and there is also the threat of attacks based on decryption failures.

In this talk, I will cover how to choose parameters for LWE systems. I will focus especially on how to estimate failure probabilities, and the difficulty of attacks based on decryption failure.