1148-68-100 **Jintai Ding*** (jintai.ding@gmail.com), 8770 wellerstation dr, cincinnati, OH 45249.

Post-quantum Key Exchange based on LWE.

In this talk, we will present the first post-quantum Diffie-Hellman like key exchange, which was built upon the learning with error problem (LWE) invented by Regev in 2005. We will review the history of key exchange and explain how we came up with the new design. We will explain New Hope, another post-quantum key exchange, which was used by Google, is a variant of our post-quantum key exchange. (Received January 27, 2019)