1126-94-346 **Qi Cheng*** (qcheng@ou.edu), 110 W. Boyd St., Norman, OK 73072, and **Jincheng Zhuang**.

LWE from Non-commutative Group Rings.

The Ring Learning-With-Errors (LWE) problem, whose security is based on hard ideal lattice problems, has proven to be a promising primitive with diverse applications in cryptography. There are however recent discoveries of faster algorithms for the principal ideal SVP problem, and attempts to generalize the attack to non-principal ideals. In this talk, we study the LWE problem on group rings, and build cryptographic schemes based on this new primitive. One can regard the LWE on cyclotomic integers as a special case when the underline group is cyclic, while our proposal utilizes non-commutative groups that eliminates the weakness associated with the principal ideal lattices. In particular, we show how to build public key encryption schemes from dihedral group rings, which maintains the efficiency of the Ring-LWE, and improves its security. We also propose a simple modification of the Peikert-Vaikuntanathan-Waters cryptosystem, which is an amortized version of Regev's original proposal based on LWE. Our modification improves the encryption and decryption complexity per bit to sublinear in the security level, without affecting the security. (Received January 17, 2017)