1125-11-748 **Hao Chen**, **Kristin E Lauter** and **Katherine E Stange*** (kstange@math.colorado.edu).

Security and attacks on Ring-Learning-with-Errors.

The Ring-Learning-with-Errors problem is a hard problem based on ideal lattices proposed for post-quantum cryptography. I will give an overview of joint work investigating the security of the problem from the perspective of attacks based on the ring structure. (Received September 10, 2016)