1147-11-794 **Katherine E Stange*** (kstange@math.colorado.edu). *On the number theory of the Ring Learning with Errors problem.* Preliminary report.

Ring Learning with Errors is a variant of a well-studied lattice problem, placed in the context of a cyclotomic field (or other number field). It is very enticing as a cryptographic problem, because it lends itself to a wide variety of protocols and capabilities, and appears to be quantum-resistant. My aim for the talk is first to give an accessible introduction to the problem for a number theorist. Then I will discuss the question of whether the ring structure, which adds greater efficiency in cryptographic implementations, adds any potential vulnerability to attack. I'll highlight the number theoretical features of the problem and mention some recent results. (Received January 28, 2019)