

1125-11-747

Yara Elias, Ekin Ozman, Kristin E. Lauter and Katherine E Stange*
(kstange@math.colorado.edu). *Ring-LWE for the number theorist.*

The talk will give an overview for number theorists of the Ring-Learning-With-Errors problem, a number theoretical hard problem proposed for post-quantum cryptography. I will review joint work on this problem that came about as part of Women in Numbers 3. (Received September 10, 2016)