1145-I1-1277 **Katharine Ahrens*** (kaahrens@ncsu.edu). *Beyond Cyclotomics: Exploring New Base Rings for Ideal Lattice Cryptography.* Preliminary report.

Hard problems arising from ideal lattices are a leading candidate for implementation in future public key cryptographic schemes due to their conjectured quantum resilience. The majority of post-quantum cryptosystems generate ideal lattices over rings of the form $\mathbb{Z}[x]/\phi_n(x)$ where $\phi_n(x)$ is the nth cyclotomic polynomial. However, the 2014 quantum attack of the ideal lattice-based cryptosystem Soliloquy, which exploits the unit group structure in cyclotomic integer rings, has motivated exploration of alternative polynomials which give rise to rings with less algebraic structure. In this talk, we consider alternative rings, including those of the form $\mathbb{Z}[x]/(x^n - p)$ and $\mathbb{Z}[x]/m_p(x)$ where $m_p(x)$ is the minimal polynomial for $\zeta_p + \bar{\zeta_p}$, ζ_p a primitive pth root of unity. We evaluate the security of these rings both experimentally and algebraically across a variety of a leading candidates for post-quantum cryptographic schemes, including NTRUEncrypt. We compare the resilience of these new rings against state-of-the-art lattice attacks on the shortest vector problem, such as BKZ and hybrid methods, to that of more traditional base rings. Finally, we consider questions of efficiency in implementation and storage costs. (Received September 20, 2018)