1154-D5-1862 **Katharine Ahrens*** (kaahrens@ncsu.edu). *Beyond Cyclotomics: Polynomial Roots, Vandermonde Matrices, and RLWE 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. One notable example is the Ring Learning with Errors (RLWE) problem, which is used in many submissions to the 2017 NIST Post-Quantum Cryptography challenge. A version of RLWE is known to be weak for certain classes of polynomials. In the process of widening the attack, we have found fascinating connections to analytic polynomial theory, matrix analysis, and enumerative combinatorics. We present our methodology and some of our most recent results. (Received September 16, 2019)