1116-11-729 **Hao Chen*** (chenh123@uw.edu), **Kristin Lauter** and **Katherine E Stange**. *Attacks on search-RLWE.*

We describe a new attack on search Ring learning-with-errors (RLWE) problem based on the chi-square statistical test, and give examples of Galois number fields vulnerable to our attack. We also analyze the security of cyclotomic fields under our attack using Fourier analysis on finite fields. (Received September 11, 2015)