1145-06-2948 **Alice Chudnovsky**, **Jake Januzelli*** (jaj226@cornell.edu) and **Jacob Brazeal**. *Obstructions to LWE-based Homomorphic Encryption with Uniform Error.* Preliminary report.

The Learning With Errors (LWE) problem was introduced by Regev in 2009 and asks that an adversary, given a uniformly chosen matrix A and $As+e$ where e has is drawn from a probability distribution with small entries on average, can recover s. The best hardness results known currently for LWE rely on the error distribution being Gaussian distributed: however, sampling from Gaussian's can be quite computationally expensive. A natural modification is to choose a bounded uniform distribution instead, being extremely easy to sample from. There are some known hardness reductions ([**?**]) for bounded uniform, but the parameters needed aren't sufficient for instantiation of practical encryption schemes. We present compelling evidence that the techniques used in the Gaussian case cannot be adapted to a bounded uniform distribution. (Received September 25, 2018)