1116-11-1407 **Kim Laine*** (kim.laine@gmail.com) and **Kristin Lauter** (klauter@microsoft.com). *Key Recovery for LWE in Polynomial Time.*

The Learning With Errors problem (LWE) has attracted a lot of interest in recent years as a building block of homomorphic cryptosystems. To optimize the performance of these cryptosystems, it is essential to understand in great detail how the hardness of LWE depends on its parameters. This boils down to analyzing the performance of modern lattice reduction algorithms, which is a difficult task.

Our point of view is different. We look instead at what can be broken using a polynomial time lattice reduction algorithm (LLL). We show that the LWE secret can always be recovered in polynomial time when one of the parameters (the modulus) is large enough. This will be demonstrated with several enlightening examples. (Received September 19, 2015)