1092-68-126 **Hang T. Dinh*** (htdinh@iusb.edu), Indiana University South Bend, Department of Computer & Information Sciences, 1700 Mishawaka Ave. P.O. Box 7111, South Bend, IN 46634. *The Hardness of Code Equivalence for Shor-like Quantum Algorithms and its Application to Post-quantum Cryptography.* Preliminary report.

The Code Equivalence problem is to determine whether two linear codes are identical up to a permutation of the coordinates. This problem is related to the security of McEliece-type cryptosystems in the case where the private code is known to the adversary. On the other hand, Code Equivalence has a direct reduction to a nonabelian hidden subgroup problem (HSP), suggesting a possible quantum algorithm analogous to Shor's algorithms for factoring or discrete log, i.e., algorithms based on measurements of a coset state. However, we show that for certain linear codes, solving this case of the HSP requires rich, entangled measurements. Our results apply to many families of linear codes of cryptographic interest, including rational Goppa codes (or generalized Reed Solomon codes), alternant codes, and Reed-Muller codes. This suggests that code-based cryptosystems using these codes are likely resistant against "Shor-like" quantum attacks, although most such systems have classical weaknesses when the private code is known. We will also discuss how our results can be extended to Linear Code Equivalence – a general version of Code Equivalence. This is joint work with Alexander Russell and Cristopher Moore. (Received August 05, 2013)