1072-94-104 **Vladimir Shpilrain*** (shpil@groups.sci.ccny.cuny.edu), Department of Mathematics, The City College of New York, New York, NY 10031. *Reflections on learning with errors.* Preliminary report.

Recovering a homomorphism between groups from several (preimage, image) pairs is a well studied problem. For some groups, it is known to be NP-hard, although this does not really help in assessing security of relevant cryptographic primitives. It gets more interesting when images are distorted by "small errors". Recovering a homomorphism gets much harder in this setting, which makes this problem potentially suitable for applications in cryptography since the problem may become NP-hard generically (or on average) for some instantiations. However, there are some auxiliary problems about platform groups, including the geodesic length problem, that one has to address first. (Received June 23, 2011)