Lattices and Homomorphic Encryption, Spring 2013 Instructors: Shai Halevi, Tal Malkin

Problem Set #5

April 9, 2013 Due April 23, 2013

1 Computation Delegation Scheme from LWE

The purpose of this problem is to flesh out the sketch construction that we saw in class.

A. Definition. Write a formal definition of a computation-delegation scheme. Your definition must formalize both the functionality of such schemes and their security. Security should be defined in terms of a game between the scheme and an adversary. Pay attention to details such as who determines the program to be delegated, the ordering of the different messages in the security game, etc.

B. Scheme. Describe all the procedures in the scheme that was sketched in class. Explain/prove why the scheme satisfies the functionality properties.

C. Security. Prove that the scheme meets the security definition, under the assumed hardness of decision-LWE.