CS 7111: Cryptography for the Cloud Jan 27, 2017

Homework 1

Instructor: Shweta Agrawal *Due: Feb 8, 2017*

Please state your answers *formally*. The tone of your writing should be crisp and mathematical, not conversational. Answers are expected in latex. A sample tex file will be provided on the webpage.

Problem 1: Semantic Security (5 pts).

In class we saw the IND-CPA definition of security for PKE. I mentioned the notion of semantic security and its equivalence to IND-CPA. Notes describing this equivalence are `http://www.cs.cornell.edu/courses/cs687/2006fa/lectures/lecture13.pdf`. Read and understand this equivalence. I will ask questions in class to verify.

Problem 2: RSA (10 pts).

Write down the textbook RSA scheme and explain why it is not semantically secure. Describe the extensions of RSA that are semantically secure and explain why they are not homomorphic.

Problem 3: Circular Security (10 pts).

Show correctness of the leveled homomorphic scheme we saw in class, where we do not make the circular security assumption.

Problem 4: Least or Most (15 pts)

In class we saw an LWE based scheme where the message was encoded in the MSB. It is also possible to encode the message in the LSB as follows:

$$c = a, \ < a, t > +2e + m$$

Here, m is a bit, e is the error and $s = (-t, 1)$ as before. To recover the message, compute $\langle c\ ,\ \ s\rangle \mod q \mod 2$.

Rework the FHE as we have seen so far with this new message encoding.