6.897: Selected Topics In Cryptography Canetti

Problem Set 2

Apri 2, 2004 *Due: April 16, 2004*

1 Question 1: F_{zk} from F_{ot}.

Show how to realize F_{zk}^{R} for any polytime-decidable relation R, in the F_{ot}-hybrid model, without computational assumptions. (Here F_{ot} provides 1 out of 2 Oblivious Transfer of strings of arbitrary polynomial length.) Can this be done when F_{ot} transfers only individual bits?

2 Question 2: F_{pke} and FF_{pke}.

1. Write FF_{pke}, the multi-session extension of F_{pke}.
2. Show how to realize FF_{pke} in the F_{pke}-hybrid model, with only a single copy of F_{pke}, with respect to adaptive adversaries, and with no computational assumptions.
3. Can F_{pke} be realized with respect to adaptive adversaries without erasures? Can it be realized with erasures?