Instructor: Adam O'Neill
adamo@cs.umass.edu

CS-690C: Homework 2

Problem 1. (100 points.)

(Part A - 30 points.) Formulate a notion of *unpredictability* for a function family. Such a notion speaks to the difficulty of predicting an output of the function family, under an unknown key, on an adversarially chosen input. Your notion should give the adversary the ability to see outputs of the function family, under this key, on other inputs of its choice as well. You should formulate the notion using games as done in class and define an associated advantage function. [[**Hint:** In your game the adversary should query for many input-output examples and then at some time specify a "challenge" input along with a guess for the corresponding output. It wins the game if its guess is correct, meaning equal to the function family, under the unknown key, evaluated at the challenge input. It is okay to have just one challenge input (although it may be stronger to have many).]]

(Part B - 40 points.) Show PRF-security of a function family implies unpredictability. To do this, given an adversary A against unpredictability of a function family F, construct an adversary B against PRF-security of F. Adversary B should have similar advantage and running-time to A. Formally analyze its advantage and running-time.

(Part C - 30 points.) Show that unpredictability does not imply PRF-security in general. To do this, assume there is a function family F meeting unpredictability. Construct from it a modified function family F' that (1) still meets unpredictability but (2) is not PRF-secure. To show (1), given an adversary A against unpredictability of F', show there is an adversary B against unpredictability of F with comparable advantage and running-time. To show (2), provide an efficient attack on F' under PRF-security. Analyze advantage and running-time as before.