CAS CS 538. Problem Set 9
Due via websubmit on Monday, November 23, 2015, at 11:59pm

Problem 1. (60 points, 15 for each part) Suppose \( \{F_s\} \) is a pseudorandom function family from \( n \)-bit inputs to \( n \)-bit outputs, with a \( n \)-bit seed \( s \). Also, let \( \circ \) denote concatenation, \( \bar{x} \) denote the bit-by-bit negation of \( x \), and \( 0^n \) denote the string of \( n \) zeroes.

We are trying to construct a function family with \( 2n \)-bit outputs out of \( \{F_s\} \). Which of the following are pseudorandom function families? Prove your answers (negative answers should be proven by showing a distinguisher; positive answers should be proven by our usual techniques—reductions, hybrid arguments, etc.).

(a) \( F_s^1(x) = F_s(0^n) \circ F_s(x) \).

(b) \( F_s^2(x) = F_s(x) \circ F_s(\bar{x}) \).

(c) \( F_s^3(x) = F_{0^n}(x) \circ F_s(x) \).

(d) \( F_s^4(x) = G(F_s(x)) \), where \( G \) is a length-doubling PRG.

Problem 2. (40 points). Let \( \{F_s\} \) now be a pseudorandom family with arbitrary-length inputs, \( n \)-bit seeds \( s \), and \( n \)-bit outputs, where \( n \) is the security parameter. Show that it is a secure message authentication code: specifically, show that if Gen chooses \( K = s \) uniformly at random, Tag\(_s\)(\( m \)) outputs \( t = F_s(m) \), and Ver\(_s\)(\( m, t \)) tests if \( t = F_s(m) \), then the resulting (Gen, Tag, Ver) is a secure MAC according to the Definition 5 in the last section of the notes. Hint: first show that the adversary wouldn’t be able to successfully forge, except with negligible probability, in case a truly random function were used in place of \( F_s(m) \). Now show that if the adversary succeeds with non-negligible probability in this real scheme, then you can build a distinguisher to tell \( F_s \) from a truly random function.