6.897 Spring 2004
Homework 4
Handed out: 5/6/2004
Due: 5/12/2004 (last day of class!)

This homework problem relates to pairing-based cryptography; see the readings available on the server.

Problem.

Part A:

Give a careful definition of a "trapdoor pairing" (like a standard bilinear map except that the pairing can only be computed if you have certain "trapdoor information").

Part B:

Give an application of trapdoor pairings. (Try to make it interesting...)

NOTE: As far as I know, the notion of a trapdoor pairing doesn't (yet) exist in the literature... Thus, this homework poses two "open problems". If your solution is really good, maybe you can turn it into a paper for Asiacrypt (submission deadline May 21st) or the Cryptography track of the RSA conference (submission deadline June 1st). Of course, the obvious question I didn't ask here is: can you implement a trapdoor pairing?