CS174 Sp2001 **Homework 12** **out: Apr 26, 2000**
J. Canny **due: May 3, 2001**

This homework is due by 5pm on Thursday May 3. Please hand it to the CS174 homework box on the second floor of Soda Hall.

1. Show that the Shamir secret-sharing scheme doesnt support multiplication directly. That is, if $h(a_1, \ldots, a_{t+1}) = a$ is the reconstruction function, then $h(a_1 b_1, \ldots, a_{t+1} b_{t+1}) \neq ab$.

2. Show that Shamir secret-sharing *does* support multiplication by publicly-known scalars. That is, if a is a shared, secret number, we can compute the shares of ka where k is a known constant.

3. Give a zero-knowledge proof of the following facts: There are numbers u and v which should be kept secret. Your ZKP(s) should prove that exactly one of u, v is one, and the other zero.