Foundations of Privacy 2007/8

Homework Set No. 1

Date Due: TBA (Was Nov 6th 2006)

1. Prove that there are no deterministic protocols for secure evaluation of the sum of n elements, for $n \geq 3$, in the setting discussed in class (private channels, no coalitions, honest-but-curious behavior and a computationally unbounded adversary).

Comment: to prove this you need to argue about the nonexistence of a simulator, but the basic argument follows from very simple principles.

Can you characterize the functions that do have a deterministic protocol?

2. Read the Story Scroogle and write a short essay assessing which technologies mentioned in the story are available and which aren't.