Collusion And Privacy In Mechanism Design

Silvio Micali

Laboratory for Computer Science
MIT, Cambridge, MA 02139
silvio@csail.mit.edu

Abstract. Mechanism design aims at engineering games that, rationally played, yield desired outcomes. In such games, multiple players interact very much as in a cryptographic protocol. But there are some fundamental differences. No player is "good", that is, always follows his prescribed instruction. No player is "malicious", that is, always acts so as to prevent the desired outcome from being achieved. Rather, every player is RATIONAL, that is, always acts so as to maximize HIS OWN utility.
Rational players too, however, have incentives to collude, and value privacy. Thus, privacy and collusion can disrupt the intended course of a game, and ultimately prevent the desired outcome from being achieved. Mechanism design has been only moderately successful in protecting against collusion, and has largely ignored privacy.
I believe that there is an opportunity for cryptographers and game theorists to join forces and produce new mechanisms that are resilient to collusion and privacy issues. I also believe that, to be successful, this effort requires a good deal of modeling and the development of new conceptual frameworks. In sum, there is the promise of a great deal of fun, challenge, and excitement, and I would like to recruit as much talent as possible towards this effort.
As a concrete example of what may be done in this area, I will describe a (quite) resilient mechanism, designed by Jing Chen and I, for achieving a (quite) alternative revenue benchmark in unrestricted combinatorial auctions. In such auctions there are multiple distinct goods for sale, each player privately attributes an arbitrary value to any possible subset of the goods, and the seller has no information about the players valuations. (Traditional mechanisms for unrestricted combinatorial auctions were uniquely "vulnerable" to collusion and privacy.)