abstract

COMPUTER SCIENCE/DISCRETE MATH I
Topic:

Speaker:

Affiliation:

Date:

Time/Room:

We prove a general result bridging the fields of Secure Protocols and Game Theory. We show that ANY mediated game with incomplete information can be perfectly simulated by the players alone, essentially by means of an extensive-form game in which the trusted mediator is replaced by a ballot box---the venerable device used throughout the world to privately and correctly compute the tally of secret votes.

In cryptographic terms, we show that, in ANY joint computation, security can be achieved based solely on the players RATIONALITY, rather than on the HONESTY of at least some players.

Our result has broad implications for Mechanism Design. In particular, it enables Modular and Competitive Mechanism Design.

Joint work with Sergei Izmalkov and Matt Lepinski