abstract

Computer Science/Discrete Mathematics Seminar I
Topic:

Speaker:

Affiliation:

Date:

Time/Room:

We present practically efficient methods for proving correctness of announced results of a computation while keeping input and intermediate values information theoretically secret. These methods are applied to solve the long standing problem of preventing collusion in second-price auctions.

Second Price auctions, where the highest bidder gets the item and pays the second highest bid value, are theoretically advantageous to the Seller. Namely, absent collusion between bidders, a participant's best strategy is to bid his true private value for the item. In practice, however, Vickery auctions are rarely used because of possibility of collusion amongst bidders. The above secrecy preserving proofs of correctness are enhanced to enable uncontrollable and deniable submission of bids in our collusion prevention mechanism. Joint work with Silvio Micali.