

Secret, Incoercible and Deniable Bidding Countering Collusions in Auctions

Michael O. Rabin, Hebrew University and Harvard University

Abstract

Recent novel highly efficient Zero Knowledge Proofs demonstrated that an auctioneer can receive bids, determine winners and later prove correctness of announced auction results, without revealing any bids values. New work done with Silvio Micali, allows bidders to submit bids in an incoercible and deniable manner. In certain auctions this combined shield of complete secrecy frustrates collusions of bidders against the auctioneer/seller.