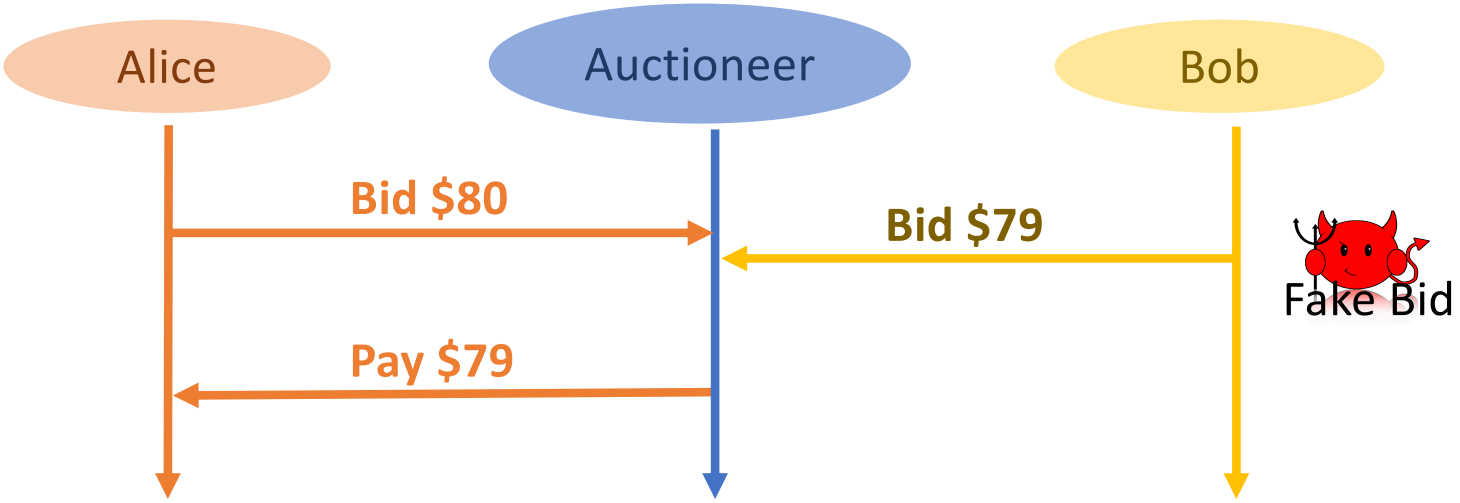
Credible, Truthful, and Two-Round (Optimal) Auctions via Cryptographic Commitments

Matheus V. X. Ferreira, S. Matthew Weinberg

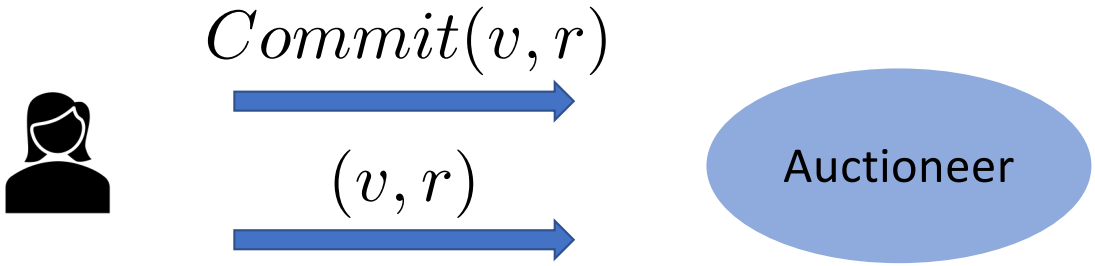
PRINCETON UNIVERSITY

- ***Model:*** There is n bidders with private independent values drawn from D.
  - Quasilinear utility $v - p$
- Myerson Auction is Truthful and Optimal **BUT** not ***credible***.



Credible Auctions [Akbarpour, Li 20']

- The auctioneer publicly ``***promises***'' to implement an auction format.
- ***Safe deviation.*** A deviation of the promise auction is safe if for all bidders, the outcome of the auction is ***always*** consistent with some realization of the auction.
- ***Credible Auction.*** No safe deviation yields more revenue than the promised auction.
- ***Impossibility*** [Akbarpour, Li 20']**.** The ascending price auction is the **ONLY** auction that is Revenue Optimal, Strategyproof, Credible, **BUT** it requires ***unbounded rounds***!
- ***Main Result:*** Assuming cryptographic commitments there is a ***two-round*** auction that is Revenue Optimal, Strategyproof and Credible.

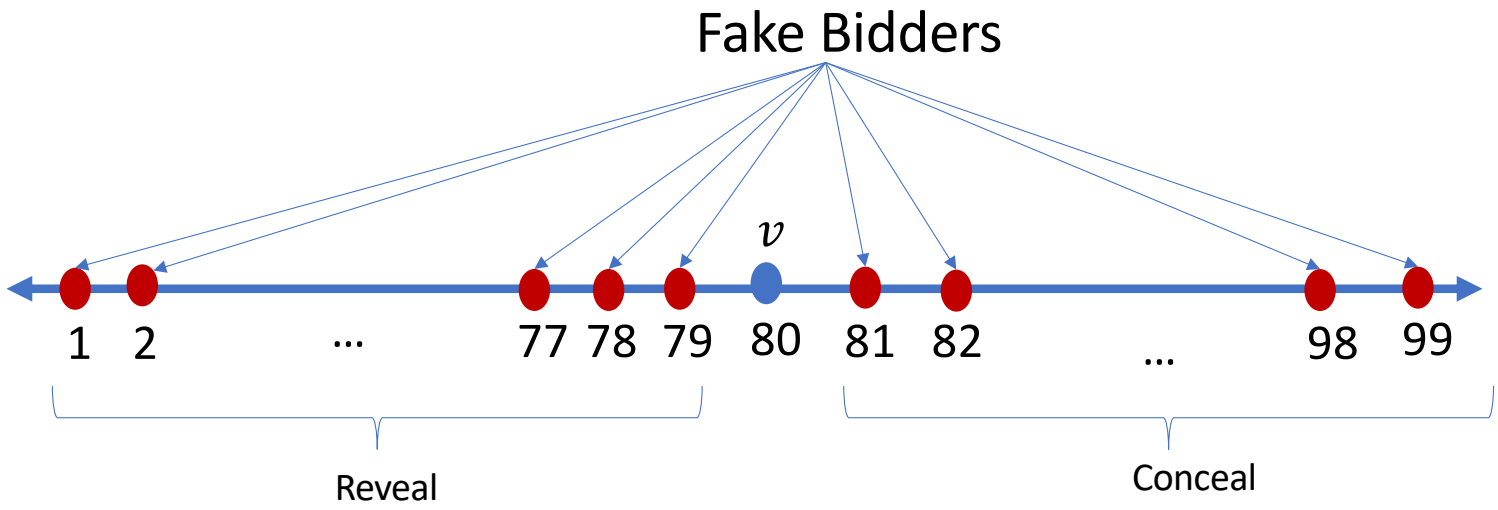


r : random seed

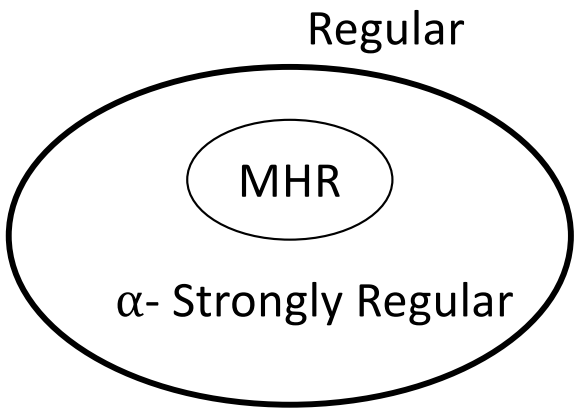
Deferred Revelation Auction

Commit bids $\Longrightarrow$ Broadcast bids $\Longrightarrow$ Reveal bids $\Longrightarrow$ Implement Myerson Auction

- ***Caveat***: There is no cost to submit fake bids.
  - ***AND*** there is no cost for aborting fake bidders.
- ***Solution***: any bidder that aborts loses deposit $f(n, D)$ to the ***WINNER!***



How big should be the penalties?



- MHR Distributions:
  - Credible when fines are at least Myerson reserve.
- Regular Distributions:
  - Not credible.
    - There is distributions where the optimal auction has revenue 1.
    - ***YET***, the auctioneer can extract ∞ revenue.
- For α-Strongly Regular:
  - Credible with a single bidder and ε-Credible with multiple bidders.