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

**Matheus V. X. Ferreira**

S. Matthew Weinberg

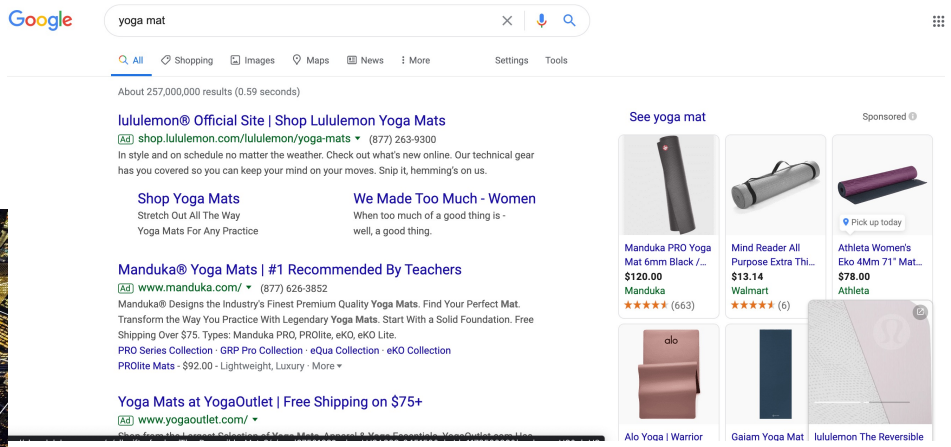
PRINCETON
UNIVERSITY

# Auctions

## Auction Houses

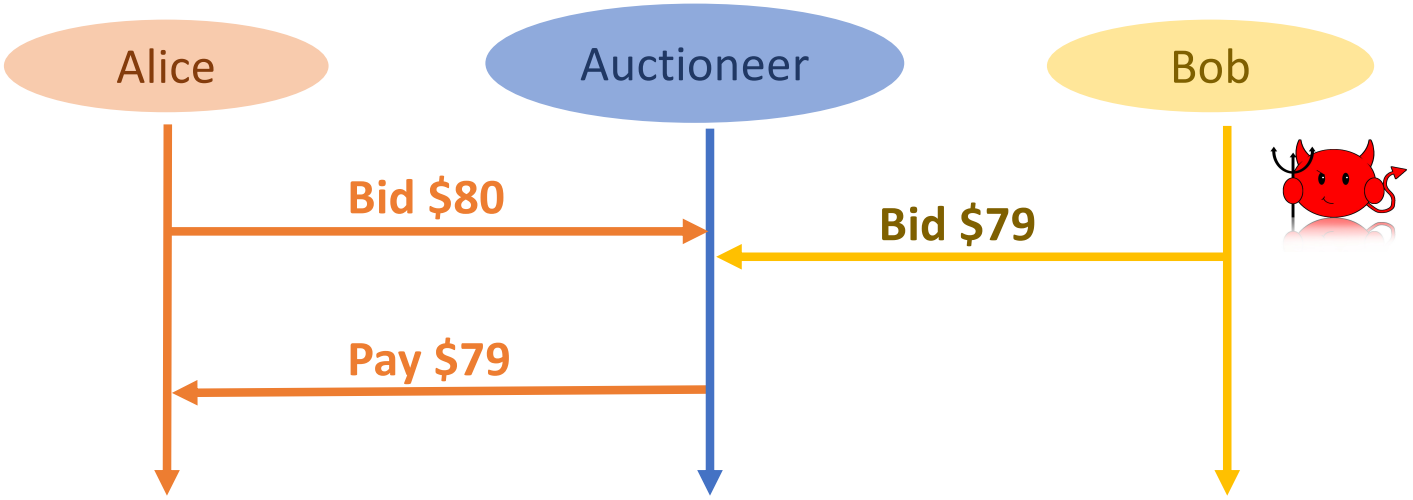

## Spectrum Auctions


## Ad Auctions



# Single Item Auctions

- There is $n$ bidders with private independent values drawn from $D$.
- Quasilinear utility $v - p$
- Optimal Auction (Myerson 1981): second-price auction with reserves.



# Second-Price Auction is not Strategy-Proof for the Auctioneer

**F.B.I. Opens Investigation of EBay Bids**

*Suspicion of Shills Rises as Web Auctions Grow*

By JUDITH H. DOBRZYNSKI

Business ▸ Policy

**eBay jewellery store fined $400,000 for shill bidding**

eBay reports offender to authorities

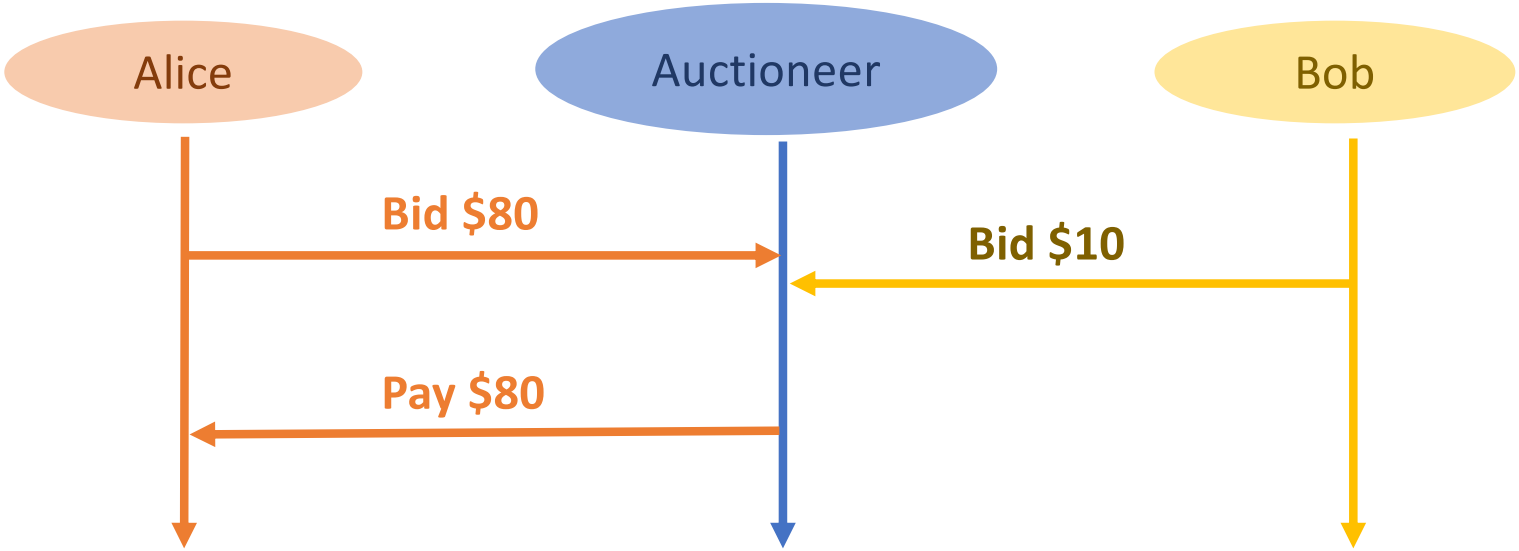
By Lester Haines 11 Jun 2007 at 11:17 18 SHARE ▼

Legislators Seek to Stop 'Chandelier Bidding' at Auction

BY *Daniel Grant* ORIGINALLY PUBLISHED 09/04/07

# Single Item First-Price Auction

- Sell to the highest bidder and charge the highest bid.
- Auctioneer cannot undetectably cheat and improve revenue.
- **BUT** not **TRUTHFUL**.



Are there revenue optimal auctions that are:

- Strategyproof for Bidders.
- **AND** Strategyproof for the Auctioneer (Credible)?

# Ascending Price Auction with Reserves

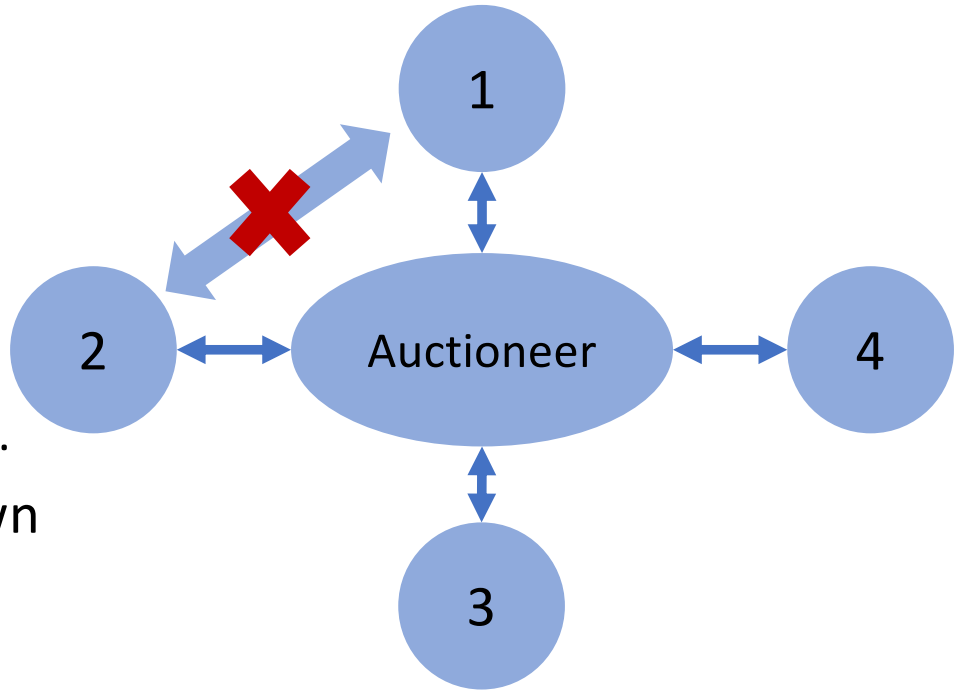
- Equivalent implementation of the second-price auction with reserves.
- [Akbarpour, Li (EC 2018, Econometrica 2020)] There is an ascending price auction with reserves that is credible.
- ***Impossibility.*** The ascending price auction is the **ONLY** auction that is:
  - Revenue Optimal.
  - Strategyproof.
  - Credible.
  - **BUT** it requires ***unbounded rounds***!
- ***Main Question.*** Can we introduce additional assumptions to circumvent their impossibility?

# Main Result

- Under mild cryptographic assumptions there is an auction that is:
  - Revenue Optimal.
  - Strategyproof.
  - Credible.
  - **AND** requires only ***two-rounds***.
- Caveat: our auctions are **NOT** credible for all distributions.

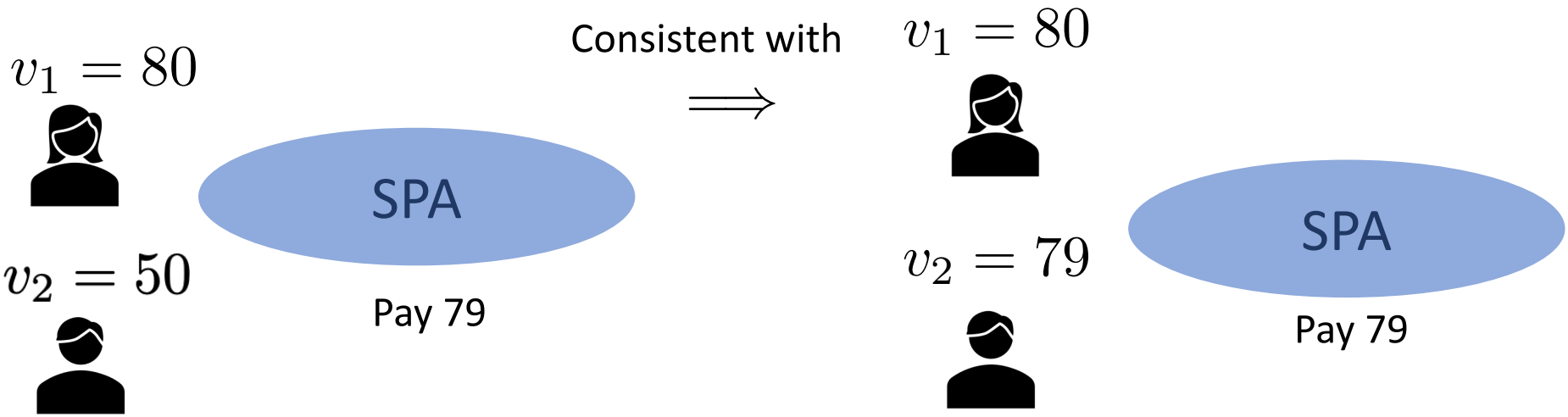
# Communication Model

- The auctioneer communicates privately with bidders.
- Bidders cannot communicate (collusion).
- Voluntary Participation
  - Bidders can abort at any point in time.
- The number of bidders is only known by the auctioneer.



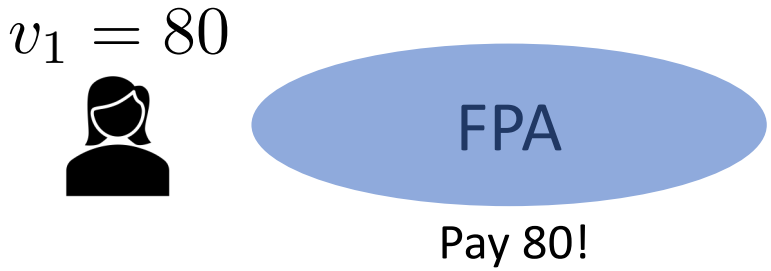
# Safe Deviations [Akbarpour, Li 20']

- The auctioneer publicly ``promises'' to implement an auction format.
- A deviation is safe if for all bidders, the outcome of the auction is ***always*** consistent with some realization of the auction.



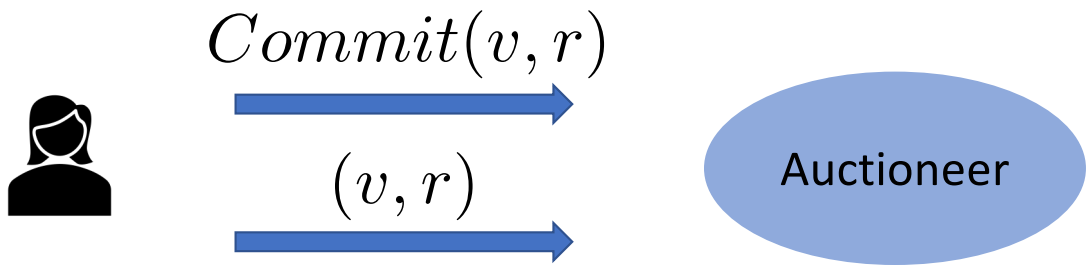
# Credible Auction

- No safe deviation from the promised auction yields more revenue than implementing the promised auction in earnest.



# Deferred Revelation Auction

# Cryptographic Commitments



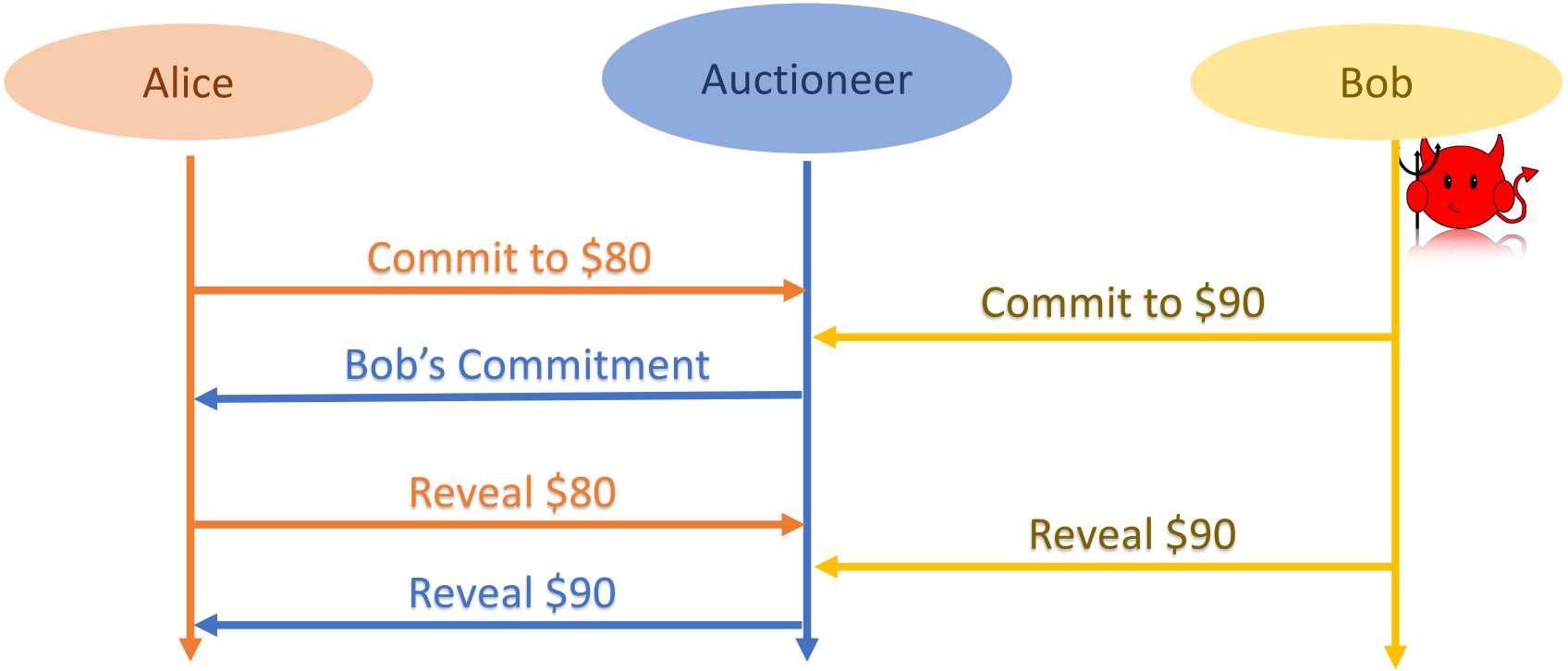

$r$ : random seed

- **Perfectly Hiding**: auctioneer learns nothing about the bid by only observing the commitment.
- **Computationally Binding**: ``hard'' for the sender to find pairs $(\boldsymbol{v}', \boldsymbol{r}')$, $(\boldsymbol{v}, \boldsymbol{r})$ that opens the same commitment: Commit(v', r') = Commit(v, r).

# First Attempt

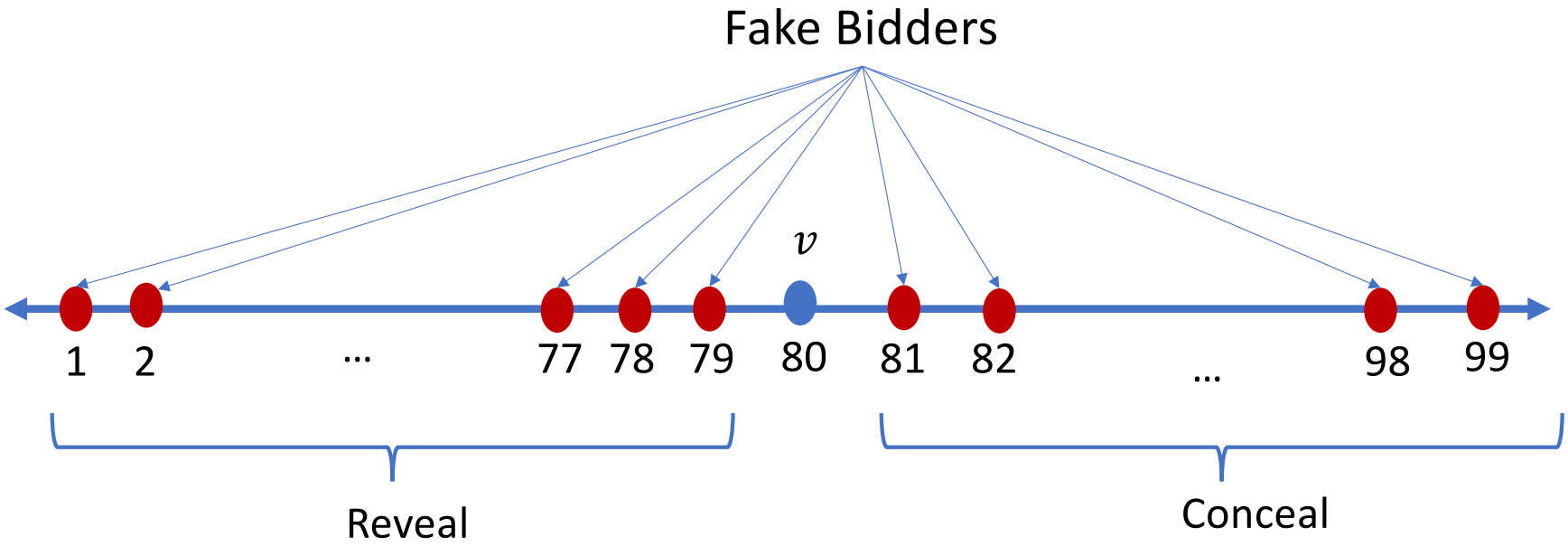
Commit bids $\Longrightarrow$ Broadcast bids $\Longrightarrow$ Reveal bids

$\Longrightarrow$ Implement Myerson Auction



# Sybil Attack

- There is no cost to submit fake bids.
- **AND** there is no cost for aborting fake bidders.



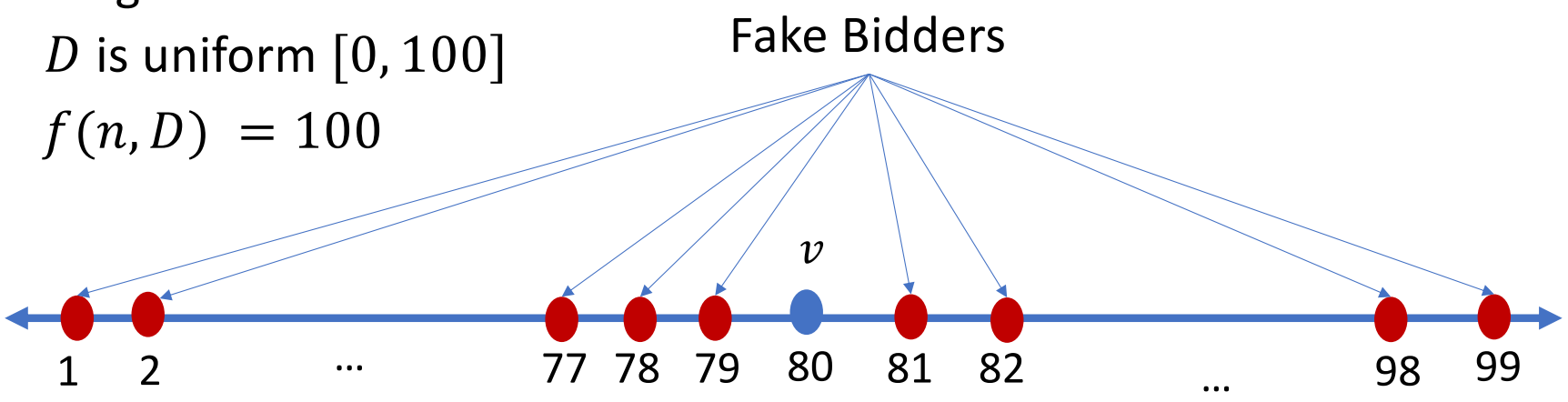
# Deferred Revelation Auction

- Same as before **BUT** *a*ny bidder that aborts pays $f(n, D)$ to the **WINNER*!***

Single bidder

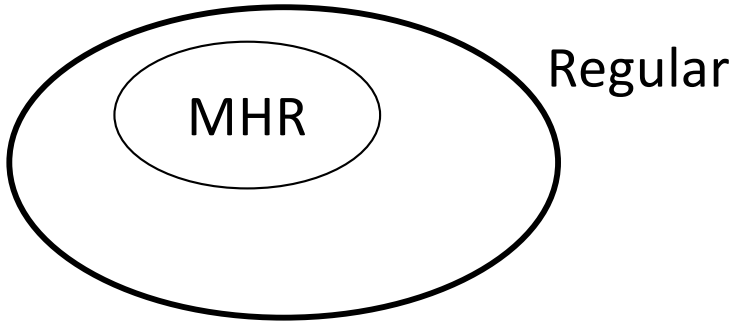
$D$ is uniform $[0, 100]$

$f(n, D) = 100$



# How big should be the penalties?

- Bounded Distributions:
  - Credible when fines above the support of the distribution.
- MHR Distributions:
  - DRA is Credible when fines are at least Myerson reserve $f(n, D) = r(D)$.
- Regular Distributions and unbounded:
  - DRA is **NOT** necessarily credible.
    - There is a distribution where the optimal auction has revenue 1.
    - **YET**, for all $f(n, D)$, the auctioneer can extract $\infty$ revenue.



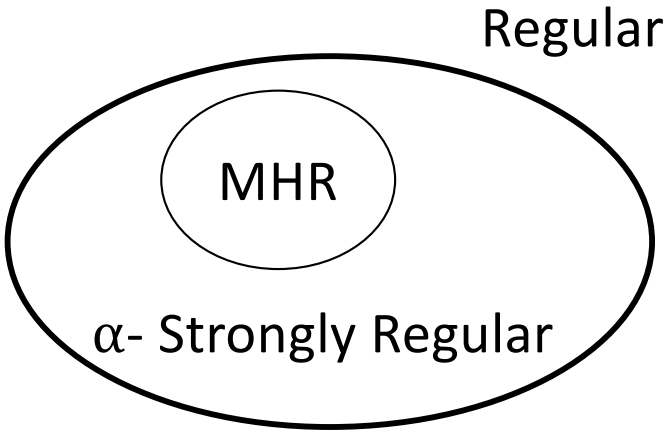
# Counterexample for Regular Distributions

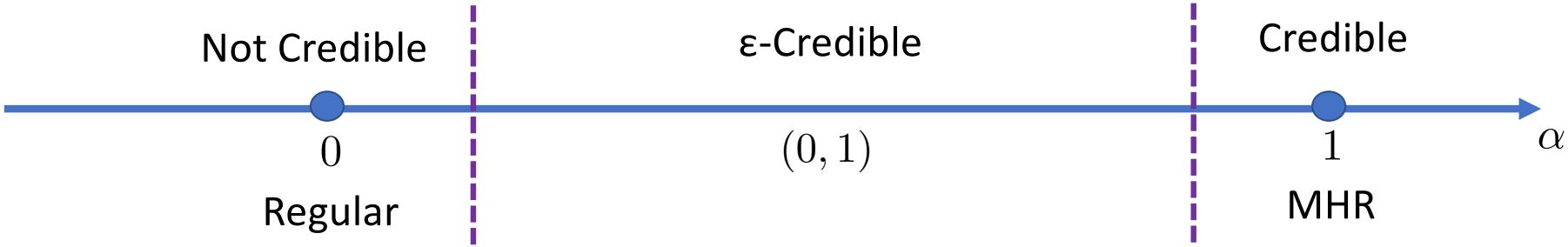
- Single bidder from equal revenue: $Pr[v \geq p] = \frac{1}{p}$
- Submit two fake bids $2k, 4k > k = f(3, D)$.
- When $v < 2k$: reveal all bids.
- When $v \in [2k, 4k)$: conceal $4k$.
- When $v > 4k$: reveal all bids.


$$E[R] = \underbrace{0 \cdot Pr[v < 2k]}_{0} + \underbrace{(2k - k) \cdot Pr[2k \leq v < 4k]}_{>0} + \underbrace{4k \cdot Pr[v \geq 4k]}_{1}$$

# Extensions for α-Strongly Regular

- For α-Strongly regular:
  - Credible with a single bidder
    $$f(n, D) = poly_\alpha(r(D))$$
  - ε-Credible with multiple bidders:
    $$f(n, D) = poly_\alpha(n, r(D), 1/\varepsilon)$$



# Conclusion

- [Akbarpour, Li 20'] The unique truthful, credible (optimal) auction takes unbounded rounds.
- Under cryptographic assumptions, we construct a two-round, truthful, credible (optimal) auction for MHR distributions and extensions for $\alpha$-strongly regular distributions.
- Open Question:
  - Is there a two-round, truthful, credible (optimal) auction for Regular?
  - What about k-round for some finite k?

Thank You!

# References


- [Vickrey, 1961] Counterspeculation, auctions, and competitive tenders, The Journal of Finance.
- [Myerson, 1979] Incentive Compatibility and the Bargaining Problem, Econometrica.
- [Myerson, 1981] Optimal Auction Design, Mathematics of Operations Research.
- [Akbarpour, Li, 2020] Credible auctions: A trilemma, Econometrica.