

How to Force Mechanisms to Commit

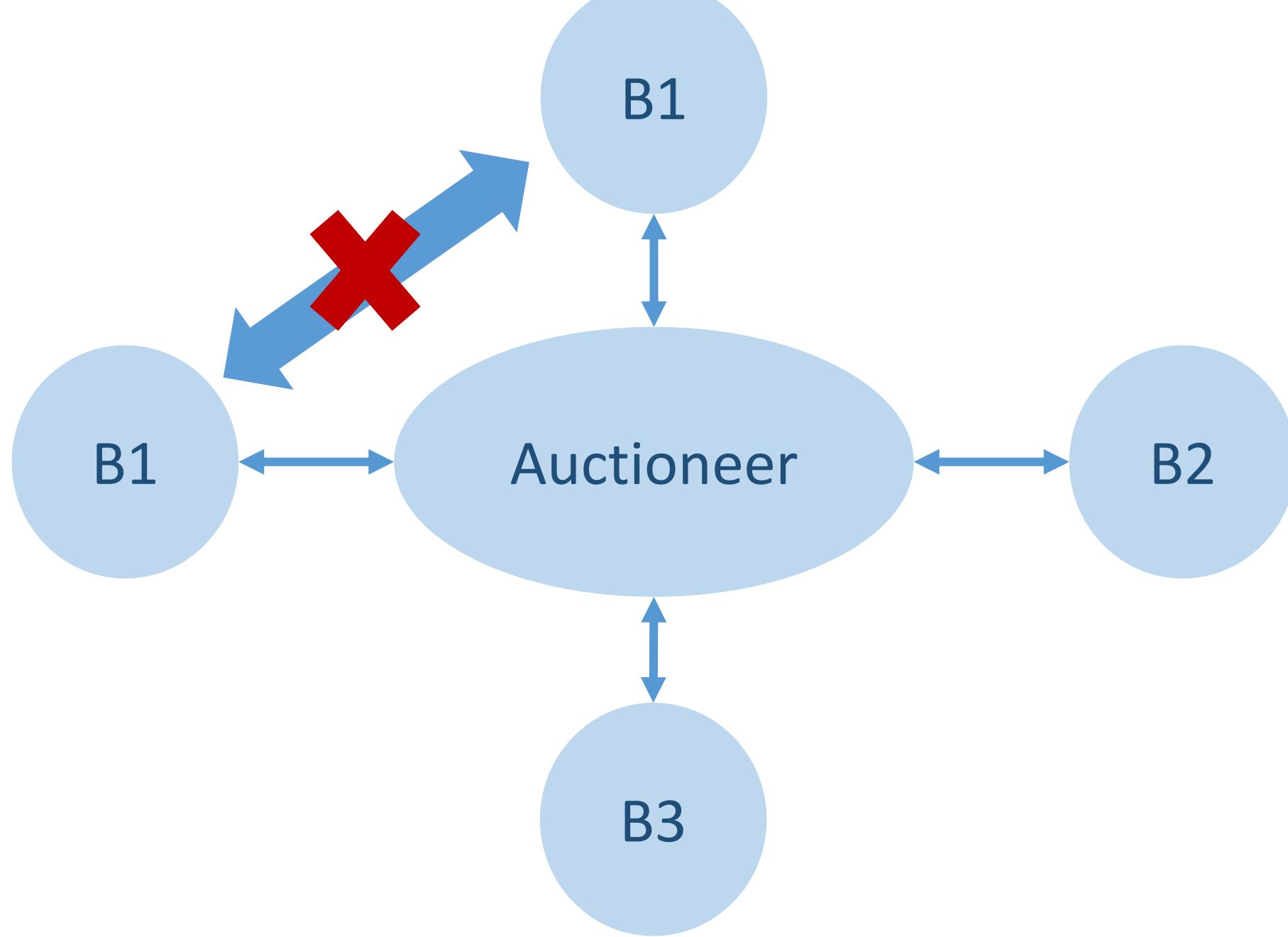
Matheus V. X. Ferreira, S. Matthew Weinberg
{mvxf, smweinberg}@princeton.edu
Princeton University

OBJECTIVES

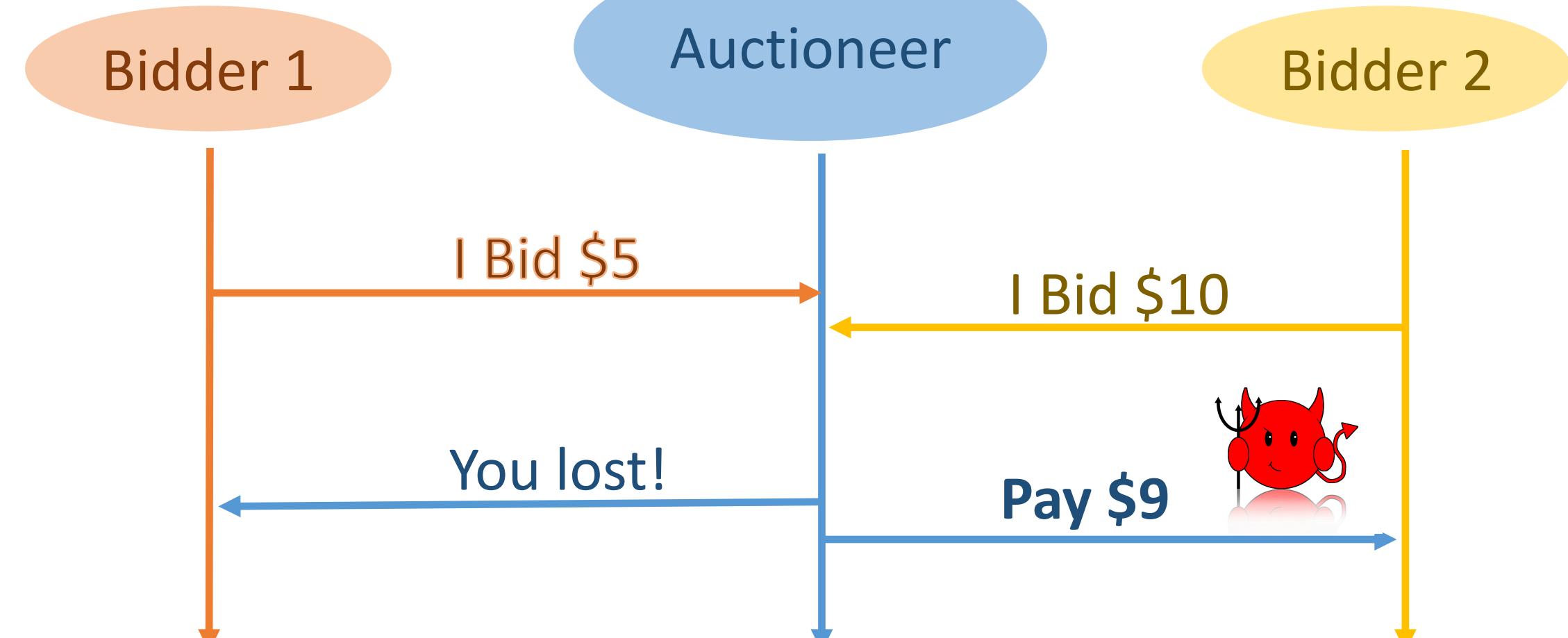
Main Question: How to design efficient auctions that are strategy-proof and credible. A mechanism is credible if it is in the best interest for the auctioneer to not deviate from the mechanism rules during the execution of the auction.

Model:

- The auctioneer is free to deviate from the protocol as long as deviations are undetectable by bidders.
- Bidders can abort from the protocol at any point.



Sealed Bid Second-Price Auction is not Credible



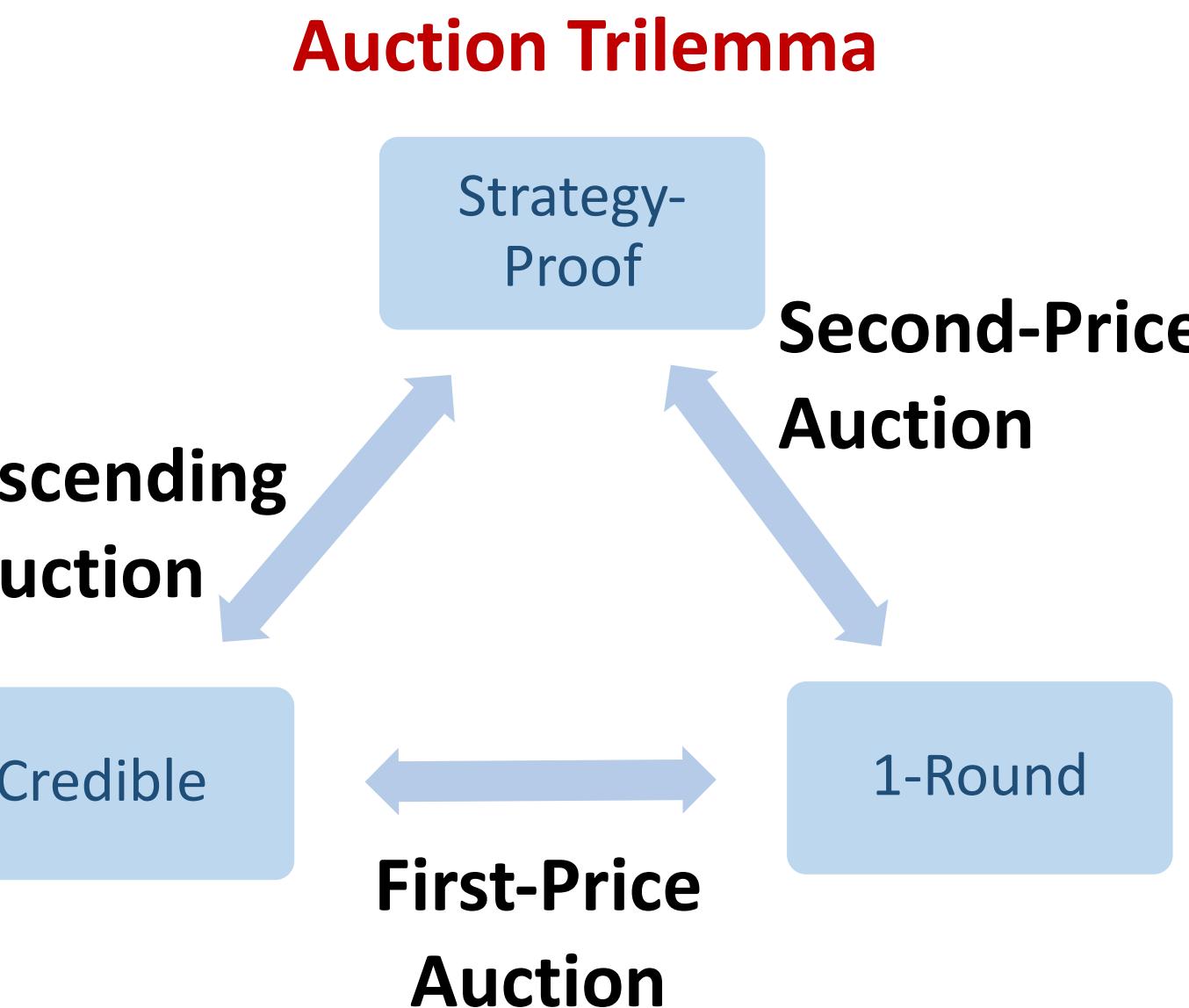
Properties:

- Efficient (1 round).
- Not credible.
- Strategy-proof:



Feasibility of Strategy-Proof and Credible Mechanisms

- A known Impossibility (Akbarpour, Li 18'): ascending auction is the only strategy-proof, credible auction.



Deferred Revelation Auction (DRA)

- Our Main Result:** under distribution and cryptographic assumptions, the deferred revelation auction is a 2-rounds, strategy-proof and credible optimal auction.

Setup: Mechanism sets a reserve price r and an entry fee k.

Commitment Phase:

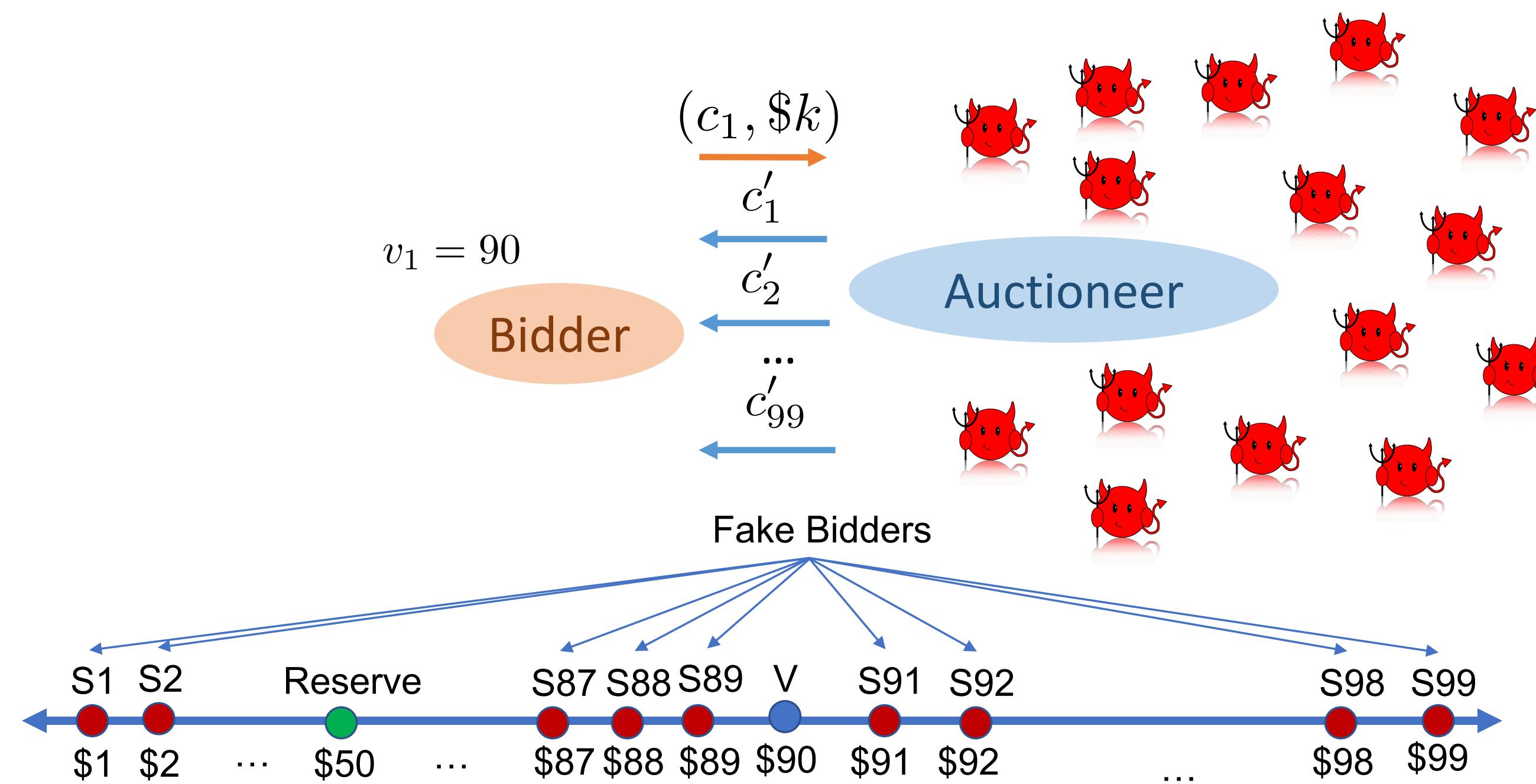
- Bidders deposit entry fee and send cryptographic commitment of bids.
- Auctioneer broadcast cryptographic commitments.

$$v_1 = 90 \\ r_1 \leftarrow U_\lambda \\ c_1 = \text{Commit}(v_1, r_1)$$



The Sybil Attack and The Use of Entry Fees

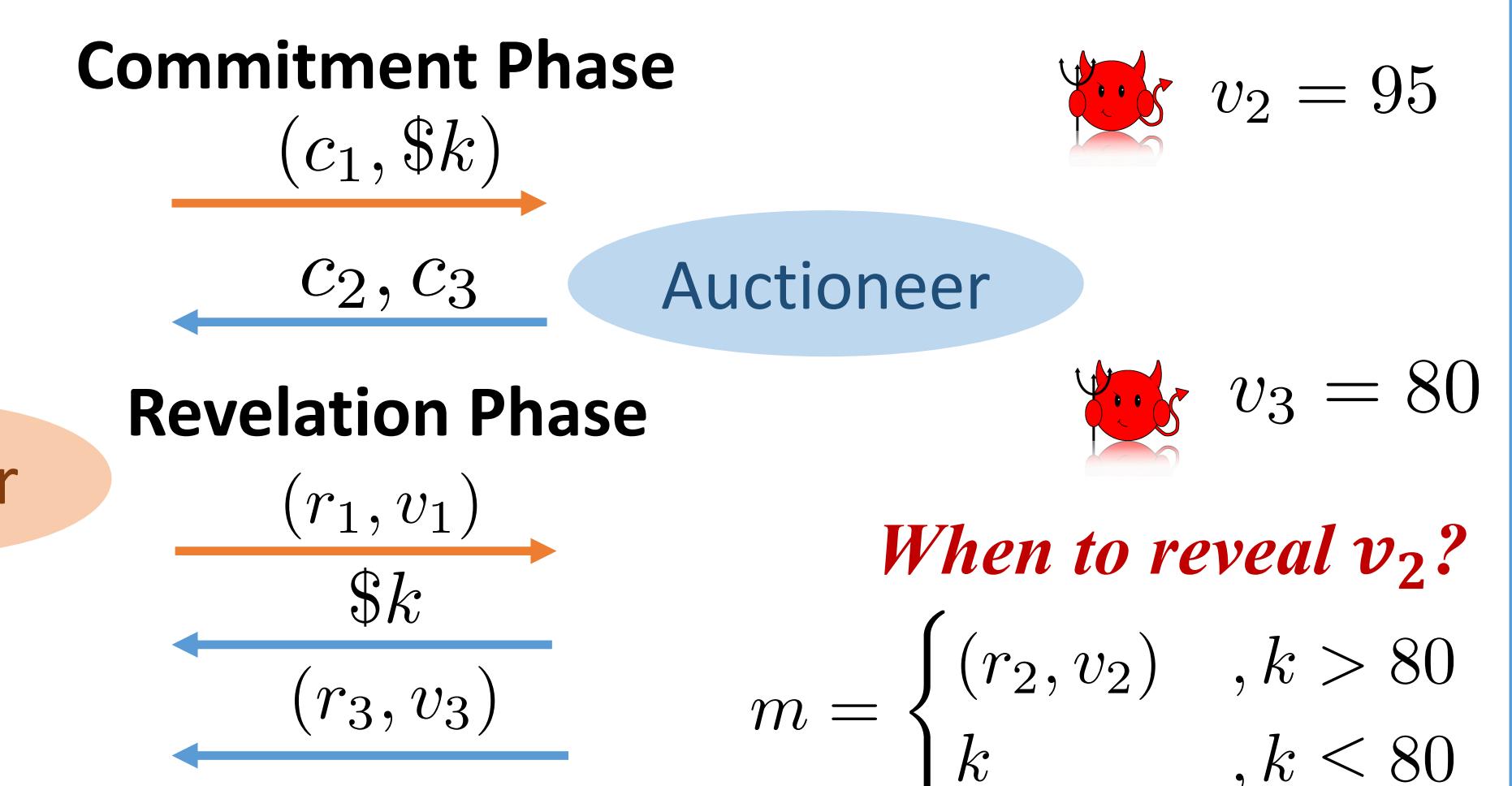
- The auctioneer impersonate fake bidders.
 - The auctioneer selectively reveal information:
- Innocent Explanation:** Bidders aborted before opening commitments.



Revelation Phase:

- Bidders open their commitments.
- Auctioneer open all possible commitments and refund entry fees.
- The auctioneer prove that a bidder aborted by refunding the entry fee to the highest bidder.

$$v_1 = 90 \\ r_1 \leftarrow U_\lambda \\ c_1 = \text{Commit}(v_1, r_1)$$



Theorem (Regularity and Incredibility)

There is a regular distribution D where for every L, for every entry fee, there is a safe deviation that obtains revenue at least $L \cdot \text{Rev}(D)$

Theorem (Strong Regularity and Credibility)

- If bidders have α -strongly regular distribution, DRA is a credible auction when the entry fee is $k = \text{poly}(n, r)$
- If the distribution is MHR, DRA is a credible auction when the entry fee is at least the optimal reserve r .

$$\alpha\text{-strongly regularity: } \forall v' > v, \phi(v') - \phi(v) \geq \alpha(v' - v)$$

Credibility of the Ascending Auction

- The Ascending Auction and the Deferred Revelation Auction are credible if they are optimal.

$$\underbrace{-f(b_1)b_1}_{\text{Expected loss of 1 quitting}} + \underbrace{(1 - F(b_1))\epsilon}_{\text{Expected gain by deviating}} - f(b_1) \left(b_1 - \underbrace{\frac{1 - F(b_1)}{f(b_1)}\epsilon}_{\text{Virtual Value}} \right) < 0$$

