Cryptobazaar

Private Sealed-bid Auctions at Scale

NDSS 2026

Andrija Novakovic
Bain Capital Crypto

Alireza Kavousi
University College London

Kobi Gurkan
Bain Capital Crypto

Philipp Jovanovic
University College London

Digital auctions are everywhere

- Online ads / ad exchanges
- Pricing compute and storage resources
- Blockchain transaction ordering / assignment of sequencing rights
- Optimization of transaction settlement in major DeFi protocols

Why privacy is important

- Censoring and front-running attacks
- Public bids reveal preferences/strategy (especially in iterative auctions)
- Reduces long-term market competitiveness
- Manipulation of auction dynamics
- Price discrimination

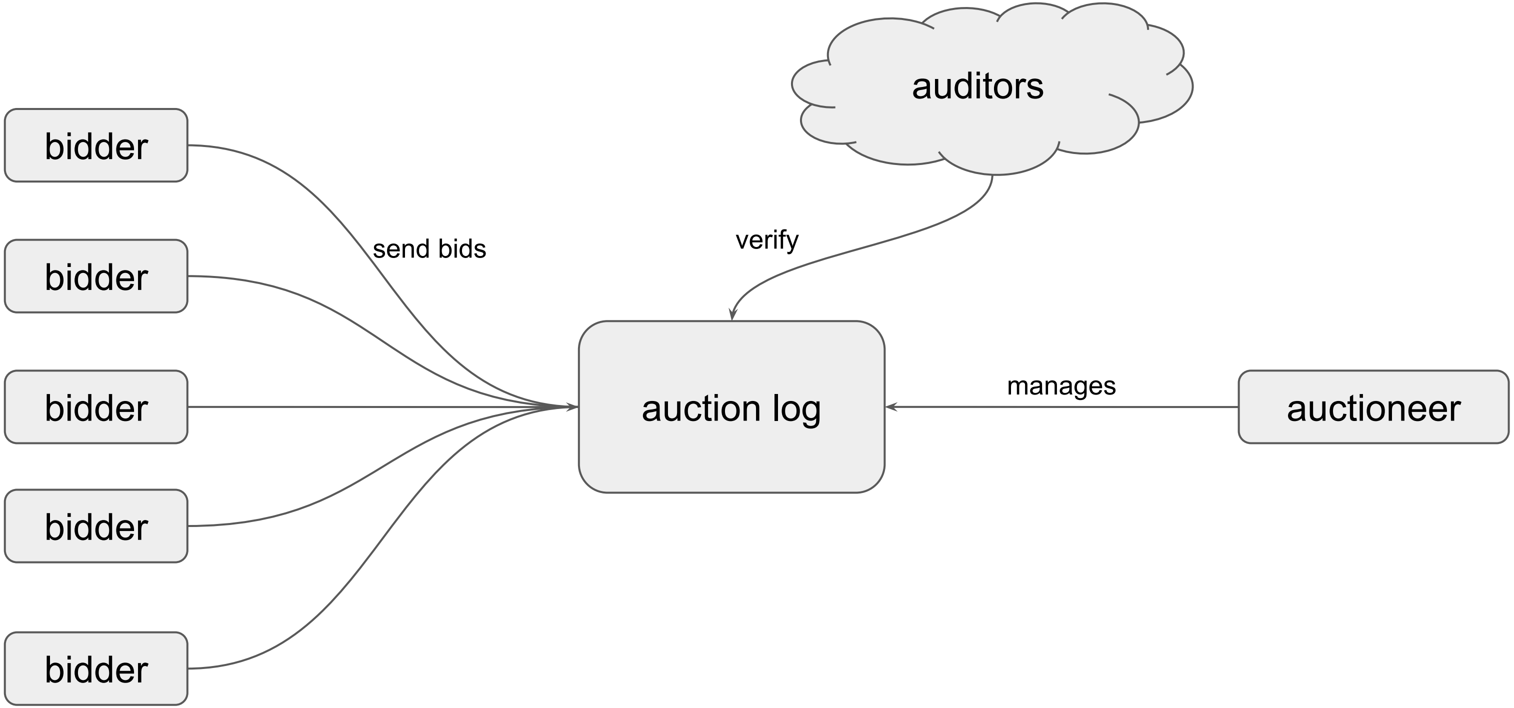
Goals

- **Privacy**: only winning price revealed
- **Verifiability**: all steps of the protocol can be externally checked
- **Trust minimization**: no honest assumptions (e.g. threshold security) or trusted auctioneer (except for liveness)
- **Scalability**: many bidders, large price ranges, low compute and bandwidth cost
- **Versatility**: different auction types with minimal protocol changes

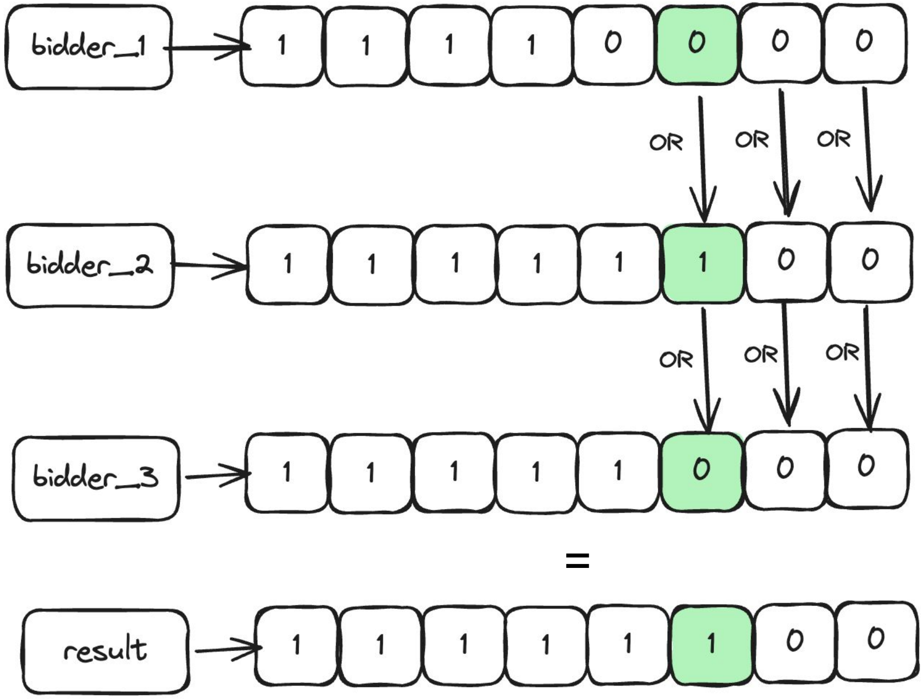
Contributions

- Cryptobazaar: a scalable private seal-bid auction protocol
    - Distributed “OR” primitive with unary encoded bids (inspired by anonymous veto [HZ06]) to privately evaluate encrypted bids
    - Zero-knowledge proofs (ZKPs) to ensure public verifiability of the protocol
- New ZKP techniques useful beyond the auction setting
- Support for different auction types (first price, second price, iterative)
- Practical implementation with low bandwidth and compute cost

Cryptobazaar system overview



Privacy-preserving evaluation of bids



bidder_1 → 1 1 1 1 0 0 0 0

bidder_2 → 1 1 1 1 1 1 0 0

bidder_3 → 1 1 1 1 1 0 0 0

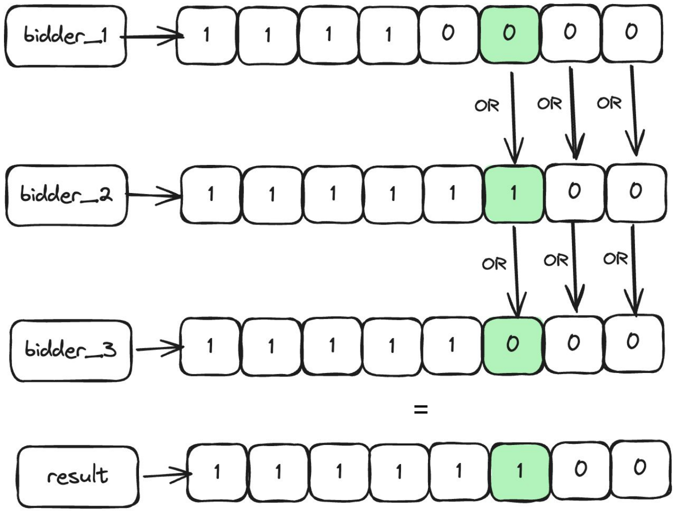
=

result → 1 1 1 1 1 1 0 0

- Run distributed 2-round logical "OR" protocol on each position of the bid
- First non "0" position determines the highest bid
- All bids are kept private and each step is supported with a proof of correctness

High-level protocol flow

- Preprocessing phase
  - Bidders commit to their bids **b** (blinded unary encoding), some randomness **x** and **r** and send proofs of correct encoding.
  - Auctioneer combines the bidders commitments (via the 1st AV step) into **Y** and sends the results back to the public log.
- Bidding phase
  - Bidders finalize their bids to the auction (by combining **b**, **x**, **r**, and **Y** via the 2nd AV step), compute ZK validity proofs and send everything to the public log.
  - Auctioneer finalizes the distributed OR protocol and publishes the result, everyone can check the result of the auction.



Implementation

Artifact Evaluated
NDSS
SYMPOSIUM
Available
Functional
Reproduced

- In Rust using the **`arkworks`** zero-knowledge proof library over any pairing-friendly elliptic curve
- Encompasses the Cryptobazaar protocol (w/o networking) and all ZKPs
- Satisfies all artifact evaluation criteria
- Available at https://github.com/akinovak/cryptobazaar-impl

Benchmarks

Environment: Apple MacBook Pro (M1 Max Chip, 8 cores, 64 GB RAM)

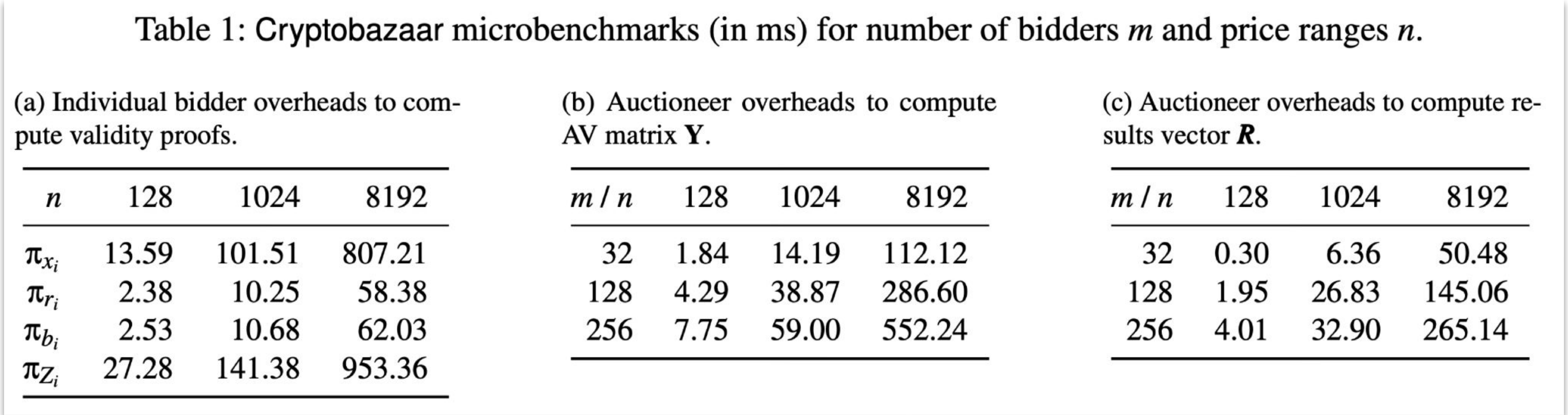


Table 1: Cryptobazaar microbenchmarks (in ms) for number of bidders m and price ranges n.

(a) Individual bidder overheads to compute validity proofs.

n	128	1024	8192
π_{x_i}	13.59	101.51	807.21
π_{r_i}	2.38	10.25	58.38
π_{b_i}	2.53	10.68	62.03
π_{Z_i}	27.28	141.38	953.36

(b) Auctioneer overheads to compute AV matrix $\mathbf{Y}$.

m / n	128	1024	8192
32	1.84	14.19	112.12
128	4.29	38.87	286.60
256	7.75	59.00	552.24

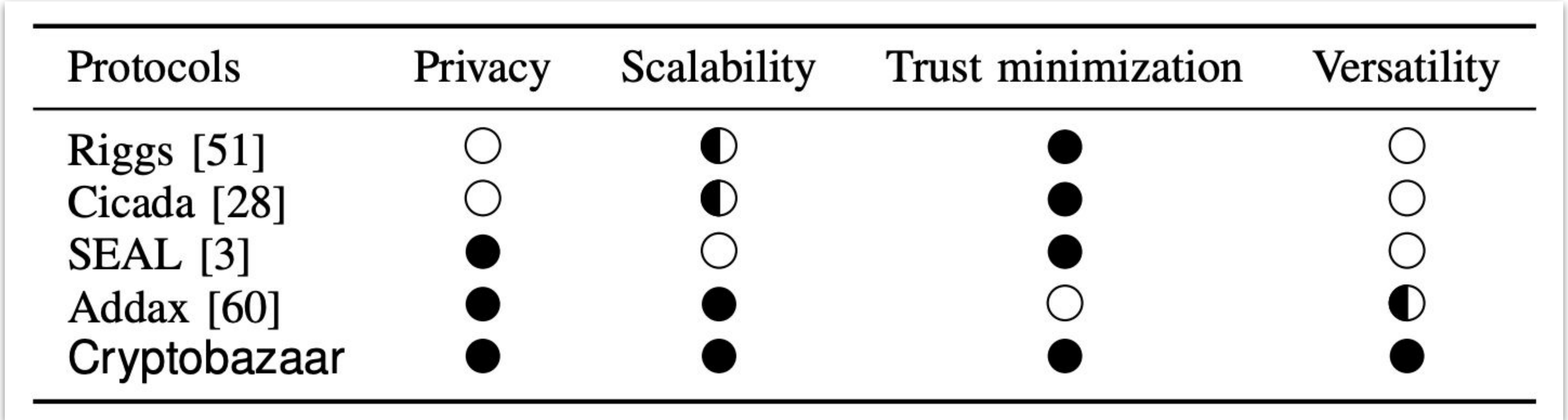
(c) Auctioneer overheads to compute results vector $\boldsymbol{R}$.

m / n	128	1024	8192
32	0.30	6.36	50.48
128	1.95	26.83	145.06
256	4.01	32.90	265.14

Take-away: Crypotbazaar scales very well across number of bidders and price ranges.

For example, for n=1024 bidders and m=128 prices, **bandwidth** cost are **32KB per bidder** (~4MB in total) and the protocol executes in **<0.5 sec**.

Comparison with state-of-the-art



Protocols	Privacy	Scalability	Trust minimization	Versatility
Riggs [51]	○	◐	●	○
Cicada [28]	○	◐	●	○
SEAL [3]	●	○	●	○
Addax [60]	●	●	○	◐
Cryptobazaar	●	●	●	●

Take away: Cryptobazaar is the first auction protocol satisfying privacy, scalability, trust minimization and versatility.

Summary

- Private sealed-bid auctions with public verifiability
- Builds on unary encoding, AV protocol and ZKPs certifying correctness of each protocol step
- Scalability across price ranges and numbers of bidders

Paper:
ia.cr/2024/1410

Code:
github.com/akinovak/cryptobazaar-impl

Thank you!