Interleaving Cryptography and Mechanism Design

The Case of Online Auctions

Edith Elkind and Helger Lipmaa

Princeton University and Helsinki University of Technology

Outline of the Talk

- Introduction and Motivations
- Mechanism Design and Cryptographic Protocol Design
- Online Auctions — Desiderata
- New Cryptographic Mechanism

Introduction and Motivations (I/III))

- *Auction*: people say how much they can pay for an item
- Used for nonstandard items where price depends on need
- Many different mechanisms to conduct an auction:
  - ⋆ English, Dutch, Vickrey, . . .
- Every mechanism has some properties that make it good in some situation

Introduction and Motivations (II/III))

- *Vickrey auctions*: theoretically very good
  - ⋆ One round, incentive-compatible, . . .
- Rarely used in practice since
  - ⋆ Security:
    - ∗ Auctioneer can cheat, no privacy
  - ⋆ Cognitive costs:
    - ∗ One round thus people must know their valuations beforehand

Introduction and Motivations (III/III)

- Security solution: use crypto on top of a mechanism
  - ⋆ I.e., take the existing mechanism + add a new cryptographic layer
- Very common approach: dozens of cryptographic auction papers
- This approach does not take into account cognitive costs
- *May be we could design a new mechanism that takes security and cognitive cost into account from scratch?*

Mechanism Design

- Individuals have some social or financial preferences
  - ⋆ Individuals are usually assumed to be omnipotent, rational, knowledgeable etc
- *Mechanism*: multi-party protocol with additional motivational ingredient:
  - ⋆ Participating in the protocol should not be “bad” for anybody
- Goal of mechanism design:
  - ⋆ Honestly following the mechanism should maximize your utility function

Mechanism Design

- Typical mechanisms:
  - ⋆ Auctions:
    - ∗ English, Vickrey, Dutch, . . .
  - ⋆ Voting:
    - ∗ Plurality, STV, Borda, . . .

Mechanism Design and Security

- Privacy is a non-issue
- Cheating for the purpose of damaging other participants is a non-issue:
  - ⋆ The participants are assumed to act solely so as to maximize their utility
- Security issues in auctions:
  - ⋆ Security against shills, jump bids, . . .

Cryptographic Protocol Design

- Multiple participants
  - ⋆ No restrictions on their behavior
- Every participant has a secret input, the goal is to compute a fixed function of the inputs
- *Correctness*: protocol must compute the output correctly
- *Privacy*: inputs must stay secret

Online Auctions

- People use gadgets to conduct an auction mechanism
  - ⋆ Still being in the same room (or not) as the auctioneer
  - ⋆ E.g., using mobile phones in a last minute ticket auction
- Using gadgets makes it possible to use cryptography, but also to design new mechanisms that people may be even do not understand

Auction Desiderata

- Pareto-efficiency or revenue maximization
- Resource-effectiveness
- Security against malicious auctioneer
- Privacy
- Minimal cognitive cost

Example: Vickrey Auction

- Sealed-bid: one round of bidding, the highest bidder gets the item for the second highest bid
- Good:
  - ⋆ Pareto-efficient, round-effective
- Bad:
  - ⋆ No security against the auctioneer, no privacy, large cognitive costs
- In some other mechanisms, you have much more rounds and thus less cognitive costs, or some other tradeoffs

Cryptographic Vickrey Auction

- Bidders encrypt their inputs. The inputs are sent to "machinery" that computes the second highest bid and the highest bidder

- Different machineries:

  - ⋆ Multi-party computation with n servers

    - ∗ Privacy/correctness are guaranteed if $2/3$ of the servers are correct

  - ⋆ 2 servers, correctness guaranteed if they do not collaborate

- Eliminates security issues, still large cognitive costs

CVA: Mechanism and Scheme

- Mechanism design: defines the goals
  - ⋆ Winner: highest bidder
  - ⋆ Price: second highest bid
  - ⋆ No intermediate bidding
- Cryptography:
  - ⋆ Takes care of privacy and correctness

Tradeoffs

- Cognitive costs vs round-effectiveness:
  - ⋆ The more rounds, the more time the participants have to contemplate on their actual valuation of the item (“common value model”)
- Cognitive costs vs privacy:
  - ⋆ The more information you get about the valuations of other bidders the more you know about your own

Our contributions

- Design a new *cryptographic mechanism* that takes security issues and cognitive cost into account from the beginning
- Mechanism has built in parameters
  - ⋆ Tradeoffs between cognitive costs, security and effectiveness
- Can prove surprising things: security against shills etc
- First work in this direction

New Mechanism: briefly

- Two parameters ε, m
- Multiple rounds of Vickrey auctions
- Only m highest bids of a round are revealed (to all bidders)
  - ⋆ No bidder will drop out before the last round
- Auctions ends when the second highest bid of a round does not change
- The highest bidder of the last round gets the price for the second highest bid

New Mechanism: briefly

- Every bidder must prove that his bid is within the fraction of $1 - \varepsilon$ from his bid of the first round

- Cognitive costs vs effectiveness:

  - ⋆ If ε is large, the bidders must do more homework, but auction converges quicker

- Cognitive costs vs privacy:

  - ⋆ If m is small, privacy properties are better but bidders have less information about their own valuations

Cryptographic Subtleties

- Can use whatever cryptographic protocols that make it possible for the bidders/auctioneer to efficiently prove in zero-knowledge that they behave correctly

- Example setting:
  - ⋆ Use ideas from Lipmaa-Asokan-Niemi (FC 2002)
  - ⋆ Homomomomomorphic auction scheme
  - ⋆ Provides efficient zero-knowledge arguments

- Details omitted from the talk (see the paper)

Conclusions

- First attempt to combine two completely different research communities from scratch
- Constructing a cryptographic mechanism enables to achieve many nice properties not achieved by layered approach
- Concrete cryptographic implementation is very efficient