Securing Auctions using Cryptography

Richard Barnes

Cryptography Applications Bistro
University of Virginia, March 16, 2004

Outline

- Context: Definitions and roles
- Types of auctions
- Vulnerabilities and Approaches
- Cryptographic solutions
  - Adding security to a Vickrey Auction
  - Adding security to a Combinatorial Auction
  - Building in security into a novel mechanism

Context

- Once upon a time: Bartering
- Unfamiliar or unknown buyers and sellers
- Multi-party price negotiation
- Auction: An organized way for many buyers and a seller to agree on a price goods.

Types of Auctions

- **English:** Start low, bid up, highest bid wins. E.g: eBay, Sotheby's
- **Dutch:** Starts high, auctioneer drops price, first to bid wins. (Can go multiple rounds or sealed) E.g: Salon IPO
- **Double Auction:** Both buyers and sellers submit prices, matched by auctioneer. E.g: NYSE, NASDAQ, CBOT
- **First-price sealed-bid:** Bidders submit closed bids; highest wins. E.g: eBay proxy bidding

Types of Auctions

- **Second-price sealed-bid** or **Vickrey**: All bidders submit sealed bids, second-highest bid wins.
  - Maximizes seller revenue by encouraging upward bidding.
  - Optimal strategy is to bid private valuation.
  - Open to dishonest auctioneers.
- Generalizations: **M-th price**

Types of Auctions

- **Combinatorial Auction**: Given a pool of available goods, buyers bid on all possible allocations of these goods.
  - Maximizes seller revenue and social surplus
  - Winning allocation maximizes total price
  - Each bidder pays difference between the total price that would have been paid without him and the other bidders total payment.
- FCC uses a modified combinatorial auction to sell rights to EM spectrum.

Vulnerabilities

- Auction fraud: 46.1% of reported Internet frauds, Median loss $320
- Bidders can collude to bid below their valuations (Insider trading) or place unreasonably high bids (Jump bidding)
- Auctioneers and sellers can insert bids to raise prices (Shill bidding) or tamper with Vickrey prices
- Many exploits are out-of-bandwidth, esp. on eBay: Non-delivery, fake escrow, etc.

Security Goals

- Prevent buyers, sellers, and auctioneers from tampering with the proper course of the auction.
- Provide privacy for buyers and sellers
  - Separate bid information from buyer identification.
  - Maintain secrecy of bids in sealed auction.

Approaches to Security

- Legislative: Make laws against breaking the rules of the auction, as for insider trading.
- Economic/Social: Provide economic incentives for following the rules, as with the eBay recommendation system.
- Cryptographic: Incorporate a cryptographic protocol to ensure that rules are followed.

Cryptographic Solutions

- Public auction + Cryptograpic privacy
- Combinatorial auction + Cryptographic enforcement
- Elkind & Lipmaa's novel protocol
- Many others exist, especially studying Vickrey auctions. Financial Cryptography has several recent examples.

Secure Public Auction

Lee, Kim, & Ma, Indocrypt 2001

- Provide bidders privacy and anonymity while keeping bid prices public.
- Introduce two agents:
  - Registration Manager: Tracks identities of bidders by tying their Diffie-Hellman public key to a secret string (unique for each bidder) and generates round keys.
  - Auction Manager: Prepares tickets and decides winner without knowing true identities.

Secure Public Auction

Lee, Kim, & Ma, Indocrypt 2001

I. Bidders register with RM by providing public key, secret string. RM keeps secret string.

II. RM creates, shuffles, and publishes a list of round keys, one for each bidder, based on public key and a hash of the secret string.

III. AM creates "bidding tickets" consisting of a hash of a round key and an auction key.

IV. Bidders find their tickets and place bids by posting their ticket ID and their price.

V. The winning ticket is chosen, and the RM reveals a hash of the winner's secret string.

Secure Public Auction

Lee, Kim, & Ma, Indocrypt 2001

- At each step, the bidder can recognize information for himself, but AM, RM, and other bidders cannot:
- Round keys are shuffled, but tied to secret information.
- Tickets are based on round keys and common information.
- Bids are tied only to ticket ID numbers.

Secure Combinatorial Auction

Suzuki & Yokoo, FC2003

- Homomorphic crypto: E(ab) = E(a) E(b)
- Represent prices as "base-1" numbers:

$$\mathbf{e}(w) = (\underbrace{E(z), \ldots, E(z)}_{w \text{times}}, \underbrace{E(1), \ldots, E(1)}_{n-w \text{times}})$$

- Can find max. bid, add a constant without decrypting.
- Want to bid on allocations, i.e. maps $f : B^G \to P$
- Bid has the form: $\mathbf{E}(f) = (\mathbf{e}(f(A)))_{A \in B^G}$

Secure Combinatorial Auction

Suzuki & Yokoo, FC2003

- Each bidder has valuation function b_x
- Auctioneer creates "blank bids"

$$\mathbf{E}_0 = \cdots = \mathbf{E}_b = \mathbf{E}(0)$$

- Each bidder adds his bid to every blank except the one with his number, so at the end,

$$\mathbf{E}_0 = \mathbf{E}(\sum_i b_i), \quad \mathbf{E}_x = \mathbf{E}(\sum_{i \neq x} b_i)$$

- $\mathbf{E}_0$ tells which bid maximizes total price
- $\mathbf{E}_x$ tells what would be paid without bidder x

Secure Combinatorial Auction

Suzuki & Yokoo, FC2003

- All calculations are performed on encrypted values.
- Neither buyers nor the auctioneer know the values of the individual bids.
- Tampering is obviated by lack of information.
- Hard part is complexity: $O(b^g)$

Elkind & Lipmaa's Auction

Elkind & Lipmaa, FC2004

- Goals:
  - Protect privacy of bidders
  - Prevent seller/auctioneer tampering
  - Minimize cognitive costs to bidders
- Perform a series of secure 2nd-price auctions until there is a stable selling price.

Elkind & Lipmaa's Auction

Elkind & Lipmaa, FC2004

- Before auction, agree on a shared masking function.
- For each round:
  - Bidders submit masked, encrypted bids to auctioneer, with a zero-knowledge proof that this bid is within a small range below the last bid.
  - All bids are published without names.
- Auction proceeds until second price stabilizes
- Identity of winner is determined by a distributed protocol matching the (unknown) max bid to its bidder.

Elkind & Lipmaa's Auction

Elkind & Lipmaa, FC2004

- Secure against shill bids, collusive bids, and jump bidding because bids are constrained to be decreasing.
- Secure against auctioneer tampering because all bids are encrypted.
- Maintains anonymity of all bidders except winner.

Summary

- Auctions play a central role, as a way of organizing price negotiations.
- Many security vulnerabilities introduced by auction mechanisms can be addressed with cryptographic auction protocols.
- Cryptographic protocols can also add privacy features lacking in normal mechanisms.
- However, protocol solutions don't address other attacks, e.g. bait-and-switch.

References

- Elkind & Lipmaa (2004) *Interleaving Cryptography and Mechanism Design*. Financial Cryptography 2004.

- Gottlieb (1999) *What is a Dutch auction IPO?* Slate Magazine. <http://slate.msn.com/id/1002736/>

- Internet Fraud Complaint Center (2002) *IFCC 2002 Internet Fraud Report.* <http://www.ifccfbi.gov/strategy/2002_IFCCReport.pdf>

- Lee, Kim, & Ma (2001) *Efficient Public Auction with One-time Registration and Public Verifiability*. Indocrypt 2001.

- Suzuki & Yokoo (2003) *Secure Generalized Vickrey Auction using Homomorphic Encryption*. Financial Cryptography 2004.