Computer and Network Security

©Copyright 2000 R. E. Newman

Computer & Information Sciences & Engineering
University Of Florida
Gainesville, Florida 32611-6120
nemo@cise.ufl.edu
Electronic Auctions
1 Types of Auctions

1.1 Open-Cry Auctions

1. English Auction
2. Dutch Auction

1.2 Sealed-Bid Auctions

1. First Price
2. Second Price
3. (m+1)st Price
2 Players

1. Bidders
2. Seller
3. Auction Managers (Auctioneers)
3 Requirements

3.1 Basic Requirements

1. Privacy
2. Anonymity
3. Non-repudiation
4. Fairness
5. Unforgeability

3.2 General Requirements

1. Robustness
2. Efficiency
3.3 Advanced Requirements

1. One-time registration
2. Revocation
3. Unlinkability within an auction
4. Unlinkability across multiple auctions
5. Distrust of authorities
6. Secrecy of highest bid
4 Auction Phases

4.1 Initialization
1. seller provides AM information
2. AM sets auction parameters (timing, etc.)
3. AM publishes parameters
4. AM advertises auctioned items

4.2 Bidder Registration
1. Bidder sends public key(s) to register
2. Bidder receives identifier, key(s)

4.3 Bid Submission
1. Bidders place bids
2. Bidder obtain receipts

4.4 Winning Bid Computation
1. Winning bidder(s) determined
2. Winning price determined

4.5 Winner Announcement
1. AM discloses winner to seller
2. AM discloses winning price
5 Trust Models

5.1 Threshold (Symmetric) Trust
1. Multiple AMs - $N$ of them
2. At most $K$ dishonest
3. ($K = N/2$ or $N/3$ usually)

5.2 Two-party (Asymmetric) Trust
1. Auction manager $AM$ and seller $S$
2. At least one of $AM$ and $S$ assumed to be honest
3. $AM$ and $S$ split duties
4. $AM$ and $S$ check each other
6 Examples

6.1 KHT-1 Protocol

6.1.1 Model

1. \( N \) bidders, \( M \) AMs, \( S \)
2. At most \( K = M - 1 \) AMs dishonest

6.1.2 Basics

1. Based on secure addition
2. Bid-vector with entry for each possible price
3. Bid ID or 0
4. Blind values so can’t tell IDs or 0s
5. Add vectors
6. No bid \( \Rightarrow 0 \) in sum vector
7. More than one bid \( \Rightarrow \) garbage in sum vector
8. Exactly one bid \( \Rightarrow \) (blinded) ID in sum vector
6.1.3 Details

1. Bidders get secret ID value from the Seller, $S$
2. $ID_j$ for bidder $B_j$ is

$$ID_j = D_S(j)$$

i.e., the identity signed by the Seller
3. The blinded ID (one per price) is

$$ID_{j,k} = E_S(ID_j || r_{j,k})$$

where $r_{j,k}$ is a random number chosen by $B_j$ for price $k$, and the concatenation of $ID_j$ and the confounder is encrypted with $S$'s public key.
4. The whole vector is signed by $B_j$
5. Bidder applies secret-sharing to bid vector elementwise (one polynomial per price)
6. The $i^{th}$ share of each vector element is sent to $AM_i$
7. Each AM computes sum of vector shares, elementwise
8. If at least $K$ AMs are honest, can recover sum vector
9. Seller then decrypts winner’s identity and bid