Distributed Auction Servers
Resolving Winner and Winning Bid without Revealing Privacy of Bids

Hiroaki Kikuchi
Shinji Hotta
Kensuke Abe
Shohachiro Nakanishi
Outline

- Protocol
  - Issues in Internet Auction
  - Anonymous Auction Protocol
  - New Protocol

- Implementation
  - Building Blocks
  - Performance
Auction Style

- English Auction
- Dutch Auction
- Sealed-bid Auction
Issue 1: Which is the first?

- Seller
- Bidder
Issue 2: Cancel bidding

A

$50

B

$100

C

$40

$30

Cancel!

$100

$40

A

B

C
Issue 3: Malicious Auctioneer
Issue 4: Privacy of bidder
Related Works

- **Distributed Approach**
  - Secret Sharing
    - (Franklin and Reiter 1997)
  - Group Encryption (Sako 1999)

- **Dutch Approach**
  - Undeniable Signature
    - (Miyazaki & Sakurai 1999)
  - One-way hash
    - (Kobayashi & Morita 1999)
## Basic Protocol

<table>
<thead>
<tr>
<th></th>
<th>$10</th>
<th>$20</th>
<th>$30</th>
<th>$40</th>
<th>$50</th>
<th>$60</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>A</strong></td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td><strong>B</strong></td>
<td>B</td>
<td>B</td>
<td>B</td>
<td>B</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td><strong>C</strong></td>
<td>C</td>
<td>C</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td><strong>Sum</strong></td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>B</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Secret function computation

$3 + 5 = 8$
Secret Sharing

Bidder A

$g_A$

S1 S2 S3
Secret Computation

Sum of $g_A + g_B$

Bidder A

$g_A$

Bidder B

$g_B$
Difficulty

- Security Flaw
  - The second highest bid be known by winner
- Computational Cost
  - Bidding Client
  - Declaring client
- Communication Cost
Security Flaw
Our Approach

- New Protocol
  - Masking the second highest
- Trial Implementation
  - Performance Analysis
# Masking Protocol

- To reveal loser’s bids
  - Random polynomial G

<table>
<thead>
<tr>
<th></th>
<th>1 1 1 0 0 0</th>
<th>F</th>
<th>6 6 3 2 0 0</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>2 2 2 2 0 0</td>
<td>×</td>
<td>× × × × × ×</td>
</tr>
<tr>
<td>B</td>
<td>3 3 0 0 0 0</td>
<td>G</td>
<td>4 3 5 7 3 6</td>
</tr>
<tr>
<td>+</td>
<td>6 6 3 2 0 0</td>
<td>F</td>
<td>4 8 5 4 0 0</td>
</tr>
<tr>
<td>F</td>
<td>6 6 3 2 0 0</td>
<td>W</td>
<td>- - 2 - -</td>
</tr>
</tbody>
</table>

(i) winning bid  (ii) Winning bid  (iii) winner
## Masking Protocol

- To reveal loser’s bids
  - Random polynomial $G$

<table>
<thead>
<tr>
<th></th>
<th>A</th>
<th>1</th>
<th>1</th>
<th>1</th>
<th>0</th>
<th>0</th>
<th>0</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>B</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>F</strong></td>
<td>6</td>
<td>6</td>
<td>3</td>
<td><strong>2</strong></td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

- $F \times G = 4 \quad 3 \quad 5 \quad 7 \quad 3 \quad 6$

- **F**x**G** = 4 \quad 8 \quad 5 \quad **4** \quad 0 \quad 0

(ii) winner: 2

(i) winning bid: 4
## Implementation

<table>
<thead>
<tr>
<th>Platform</th>
<th>Auction Server</th>
<th>bidder/declaring client</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sun SPARC Station 5, 20, Ultra S-7/300U, Sun OS 4.1, Solaris 2.5.1</td>
<td>PC Windows 9x/NT</td>
<td></td>
</tr>
<tr>
<td>base software</td>
<td>Apache v1.3.9, OpenSSL v0.9.4</td>
<td>IE v4.x, NN v4.x</td>
</tr>
<tr>
<td>language</td>
<td>Perl 5.005(CGI)</td>
<td>JavaScript 1.1</td>
</tr>
</tbody>
</table>
System Architecture

JavaScript 1.1

Perl 5.005

JavaScript 1.1

S1

S2

S3

abe $600

abe $600

Perl 5.005
Step 1: Registration

- Bidding client
  - contract
    » good info.
    » time table
    » cleaning
  - user ID
  - Bid
- Server Frames
Step 2: Distributed Bids

- Encoding
  - 10 times 3 matrix
- Getting Distributed
  - into three servers
- Casting
  - bids to each server
  - recipient for bidding
Step 3: Resolving Winner

PUSH!!

A

B

C
Performance of bidding

- Secret Sharing
- Multiple Sending
- Single Sending
Opening bids

![Graph showing the relationship between processing time and price candidates. The graph has a linear trend line with points scattered around it, indicating a correlation between the two variables.](image-url)
Upper bound of $k$

- Processing time
  - secret sharing
    \[ T_1(k) = 2 \cdot 10^{-7}k^2 - 1.2 \cdot 10^{-3}k + 2.23 \]
  - sending to 3 servers
    \[ T_2(k) = 4.4 \cdot 10^{-3}k + 0.94 \]

- with $T^* = 60$ [s],
  \[ k^* = 10658 \]
Conclusion

- We have developed distributed auction server which
  - prevent servers from cheating
  - prevent bidders from canceling bids
- We proposed a modified protocol (MASK) which
  - improves privacy of bid.