The Dining Bidders: Secure Auctions for a Paranoid World

Terence Kelly

tpkelly@rand.org
RAND Corporation
1700 Main Street
Santa Monica CA 90407-2138

tpkelly@eecs.umich.edu
http://ai.eecs.umich.edu/~tpkelly/
U. Michigan AI Lab
1101 Beal Avenue
Ann Arbor MI 48109-2110

21 July 1998

Draft paper available at
http://www-personal.engin.umich.edu/~tpkelly/auc/

$Id: dnbdrs.tex 1.19 1998/07/19 06:07:46 tpkelly Exp $

CREDITS

Guidance from Professors Michael Wellman and Peter Honeyman of U. Michigan

Redmond trip logistics by Dave Pennock of Microsoft Research

Wardrobe by Paul Dryer of RAND Corporation

AUCTIONS

> "An auction is a market institution with an explicit set of rules determining resource allocation and prices on the basis of bids from the market participants."
> — *McAffee & McMillan*

Input: buy & sell bids
Output: buyer-seller pairs, prices

Examples:
- English open-outcry ("going once...")
- Dutch descending price
- Sealed-bid (gov't. contracts)
- Vickrey (2nd price)
- Continuous double auction (stock market)

ONLINE AUCTIONS:
TWO PROBLEMS

1. Generality:
   existing auction servers support only a few points in the space of possible auction types

2. Privacy/Trust Tradeoff:
   bidders must either trust auctioneer or reveal bids in order to ensure correctness

ONLINE AUCTIONS:
TWO SOLUTIONS

1. Generality:
   University of Michigan AuctionBot
   Supports *generalizations* of several familiar auction types (English, Vickrey, continuous double auction)
   http://auction.eecs.umich.edu/

2. Privacy/Trust Tradeoff:
   subject of this talk

DESIGN GOALS

- Privacy: don't disclose bidders' secrets (reserve prices, utility functions)
- Correctness: cheating & error impossible
- Paranoia: no trust required
- Generality: support *any* type of auction
- Economy: use off-the-shelf algorithms
- Simplicity: no new weaknesses

PREVIOUS WORK

Franklin & Reiter, "The Design and Implementation of a Secure Auction Service," *IEEE Trans. Software Eng.* 22(5) May 96.

Replicated auction service with a clever application of digital cash technology.

Guarantees that
- Bids are not revealed prematurely
- Winning bidder pays auctioneer
- Losing bidders keep their money
- Only winning bidder can collect item

Drawbacks:
- Limited to single-good sealed-bid auctions
- Fails if over 1/3 of auctioneers are corrupt
- Complex protocol; hard to analyze & implement

SECURE MULTIPARTY COMPUTATION

- n agents agree on function F, wish to compute and reveal $F(x_1, x_2, \ldots, x_n)$ where x_i is agent i's secret input.
- Output is correct and inputs remain secret if fewer than $n/3$ agents are faulty or corrupt (unconditional security)
- Probabilistic guarantee possible for up to $n/2$; requires broadcast channel
- Conceptually evaluate function within acyclic Boolean or arithmetic circuit

Yay! We're done! (?)

PROBLEMS WITH SECURE MULTIPARTY COMPUTATION FOR AUCTIONS

- Privacy?
  too much: insincere bids possible
  too little: state of market concealed
- Correctness? Paranoia?
  honest majority required
- Generality?
  auction type hard-coded at design time
  dynamic auctions (e.g. English, CDA)
- Simplicity?
  representing auction as acyclic circuit
- How to execute transactions computed by auction?

SECOND TRY:

Turn problem upside down:
reveal all bids, still guarantee privacy.

Conceal mapping between bidders and bids. To deter insincere bids, retain ability to recover this mapping until auction ends.

Compute the auction in the open, so guarantee of correctness is trivial without honest majority.

BUILDING BLOCKS

- Mental poker:
  assign unforgeable and nonrepudiable identifiers to bidders
- Dining cryptographers:
  anonymous broadcast channel ("shared whiteboard")
- Diffie-Hellman key exchange:
  secure anonymous communication channel for buyer-seller pairs

MENTAL POKER

- Uses public-key cryptography with a temporary key pair
- To prove ownership of card hand, reveal private key
- If players destroy private keys, impossible to recover hands

DINING CRYPTOGRAPHERS

Untraceable Morse code:
each agent may tap, or not tap.

- Each pair of agents shares a secret key bit (one-time pad)
- Each agent computes $b =$ sum modulo 2 of all key bits he shares
- To tap, broadcast $\neg b$; else broadcast b
- If an agent taps, sum modulo 2 of all broadcasts must be one; else it must be zero

Demonstrates that unconditional secrecy channels can be used to construct an unconditional sender-untraceability channel.

DIFFIE-HELLMAN KEY EXCHANGE

- Alice & Bob agree on large prime n and g such that g is primitive mod n (these are *not* secret)
- Alice chooses x
  Bob chooses y
  (secret large random integers)
- Alice sends Bob $X = g^x$ mod n,
  Bob sends Alice $Y = g^y$ mod n
- Alice computes Y^x mod $n = g^{xy}$ mod n,
  Bob computes X^y mod $n = g^{xy}$ mod n
  (this is shared secret)
- Eavesdropper who knows n, g, X and Y cannot compute shared secret (assuming discrete logarithms are hard)

PROTOCOL

- ID assignment:
  bidders are dealt mental poker ID cards
- Bidding:
  anonymously broadcast (ID, price, qty)
- Clearing:
  bidders run auction independently
  (compute buyer-seller pairs & prices)
- Transaction:
  buyers & sellers establish secure channel via Diffie-Hellman, transact
- Conclusion:
  bidders "burn ID cards" by destroying key pair used in mental poker

In case of insincere bid, wronged party "cries foul," bidders are forced to reveal temporary key pair (and hence IDs), villain is unmasked and punished.

EXAMPLE: Bidding

(A♠, \$7, 1)

(J♣, −\$5, 1)

(K♢, \$4, 10)

(Q♡, −\$2, 10)

EXAMPLE: Clearing

(A♠, \$7, 1)

1 at \$6

(J♣, −\$5, 1)

(K♢, \$4, 10)

10 at \$3

(Q♡, −\$2, 10)

EXAMPLE: Transaction

(A♠, \$7, 1)

1 at \$6

(J♣, −\$5, 1)

(K♢, \$4, 10)

10 at \$3

(Q♡, −\$2, 10)

A♠: "g^x mod n"
J♣: "g^y mod n"
A♠: (encrypted) "here's my money..."
J♣: (encrypted) "here's your stuff..."

PROBLEM SOLVED?

√ Privacy

√ Correctness

√ Paranoia

√ Generality

√ Economy

√ Simplicity

CRITIQUE

Advantages:

- Auction protocol decided at run time, not hard wired into circuit as in secure multiparty computation
- Supports any auction type
- Correctness guarantee is trivial; no trust required
- State of market is fully revealed to all

Disadvantages:

- Efficiency: mental poker can be computationally burdensome
- Key distribution: simplest variant of dining crypto requires every pair of bidders to share one-time pad

SECURITY ANALYSIS

Malfeasance that *is* possible:

- Denial-of-service attacks using another person's ID, or against anonymous broadcast channel
- $n-1$ bidders collude against remaining one
- Shills in single-good English auction

What's not possible

- Insincere bids
- Learning mapping between bidders and bids if fewer than $n-1$ bidders are corrupt
- Man-in-middle attacks on Diffie-Hellman channel

Causes for concern

- Attacks on mental poker?
- Information leakage for small n?

VALUE ADDED

In what kinds of real situations might this mechanism be useful?

- Indulgences ??
  buy & sell forgiveness

- EPA Waivers ?
  buy right to pollute, avoid bad press

- Stock Market !
  bidder-bid mapping distorts market
  example: Bill Gates sells MS stock

CRYPTOGRAPHY AT ITS BEST

Trust management?

Trust is a point of failure, at best a necessary evil.

To needlessly trust *anyone* is to take an unnecessary risk. (Consider key escrow/recovery.)

The best applications of cryptography *obviate the need for trust.*

REFERENCES

Brief survey of auction types: `http://www.agorics.com/new.html`

Excellent review of auction theory:
R.P. McAfee & J. McMillan, "Auctions and Bidding," *Journal of Economic Literature* XXV (June 1987), pp. 699–738.

General crypto, mental poker, Diffie-Hellman:
Bruce Schneier, *Applied Cryptography* 2nd Ed., Wiley, 1996.
Errata at `http://www.counterpane.com/applied.html`.

D. Chaum, "The Dining Cryptographers Problem," *Journal of Cryptology* (1988)1:65–75.

Secure multiparty computation:

M. Ben-Or, S. Goldwasser & A. Wigderson, "Completeness Theorems for Non-Cryptographic Fault-Tolerant Distributed Computing," *Proc. 20th ACM STOC* (1988), pp. 1–10.

D. Chaum, C. Crépeau & I. Damgård, "Multiparty Unconditionally Secure Protocols," *Proc. 20th ACM STOC* (1988), pp. 11–19.

T. Rabin & M. Ben-Or, "Verifiable Secret Sharing and Multiparty Protocols with Honest Majority," *Proc. 21st ACM STOC* (1989), pp. 73–85.

D. Beaver, "Secure Multiparty Protocols and Zero-Knowledge Proof Systems Tolerating a Faulty Minority," *Journal of Cryptology* (1991)4:75–122.