Secure Vickrey Auctions without Threshold Trust

Helger Lipmaa
Helsinki University of Technology, {helger}@tcs.hut.fi

N. Asokan, Valtteri Niemi

Nokia Research Center, {n.asokan,valtteri.niemi}@nokia.com

Overview

- A project between the HUT and Nokia (2001)
- The goal: design an *efficient*, *cryptographically protected* auction protocol that can be implented in *mobile phones*
- Nokia patent application from October 2001
- Paper published at Financial Cryptography 2002 (Bermuda)

Intro: auctions

Examples:

- Government sells 3G licenses
- Airline company sells last-minutes tickets
- Colombian fisher from a fishing village sells fresh swordfish
- *Trust models are completely different*

Auction = the ideal model of selling an item with an unknown price

Intro: auctions

Auction call Auction is opened by publishing its details (auction mechanism, dates, name of auctioneer and sold items)

Bidding phase All auctioneers bid, according to published *mechanism*

Auction closing After closing time, the winner and winning price are decided according to the *mechanism*

Exchange Item is given to the winner in exchange for the winning price

Motivations: general

Dream: ideal auctions

- Pareto-efficient
- Sealed-bid
- Incentive-compatibility
- Secure against malicious auctioneers

Pareto-efficiency

- Game-theory: people do not usually often the mechanism
- Why not? It is often benefitial for them to cheat
- An (auction) mechanism is *Pareto-efficient* if the benefit of each bidder is maximized by *honestly* following the protocol
- . . . given that the auctioneer is honest $\leftarrow$ Often forgotten in game-theoretic literature

English auctions

- The most common type of auctions
- Everybody overbids everybody else, until nobody overbids some fixed bid X_1
- X_1 is then the winning price, its bidder is the winner
- English auctions are Pareto-efficient, incentive-compatible but not computationally efficient (many, many rounds)

First-price sealed-bid auctions

- Sealed-bid: All bidders enclose their bids in an envelope. In bid opening phase, all envelopes are opened.
- Highest bidder pays the highest (“first”) bid
- Efficient: one round only
- Not *Pareto*-efficient!

Vickrey auctions

- Idea: highest bidder pays the second highest bid
- Good: Pareto-efficient, sealed-bid, incentive-compatible, ...
- Still not used widely in practice
- One of the main reasons for this: insecurity
  - ⋆ auctioneers can change the winner and the winning price undetectably
- High motivation for cryptographic Vickrey auctions

Security model (1/2)

- Cryptographic Vickrey auctions need computing devices and connection
- Concrete example: mobile phones and WLAN in the same room with the goods
  - ⋆ so that goods can be inspected and payment enforced
- Thus two major security problems of Internet auctions are avoided

Security model (2/2)

- Such auctions have usually

  ⋆ an occassional, *untrusted*, auctioneer with potentially *large number* of bidders

  ⋆ this auctioneer has a single server, or has supreme control over several servers

- In both cases, *threshold trust is not an option*

  ⋆ threshold trust is also bad in Internet auctions

Security requirements

- Correctness
  - ⋆ Highest bidder Y_1 should win
  - ⋆ He should pay the second highest bid X_2
- Privacy: S should not get any information about the bids but (Y_1, X_2)

Related work: Vickrey auctions w/o threshold trust

- Cachin, Baudron-Stern: oblivious third party, seller will get to know partial order between bidders valuations and Y_2

- Naor-Pinkas-Sumner: an established third party (auction authority)
  - ⋆ A designs a circuit that is executed by seller
  - ⋆ Drawback 1: large communication complexity
  - ⋆ Drawback 2: corrupt A can be detected only by using a cut-and-choose technique

Our model

- B bidders, effectively $B \leq 1000$

- Seller S

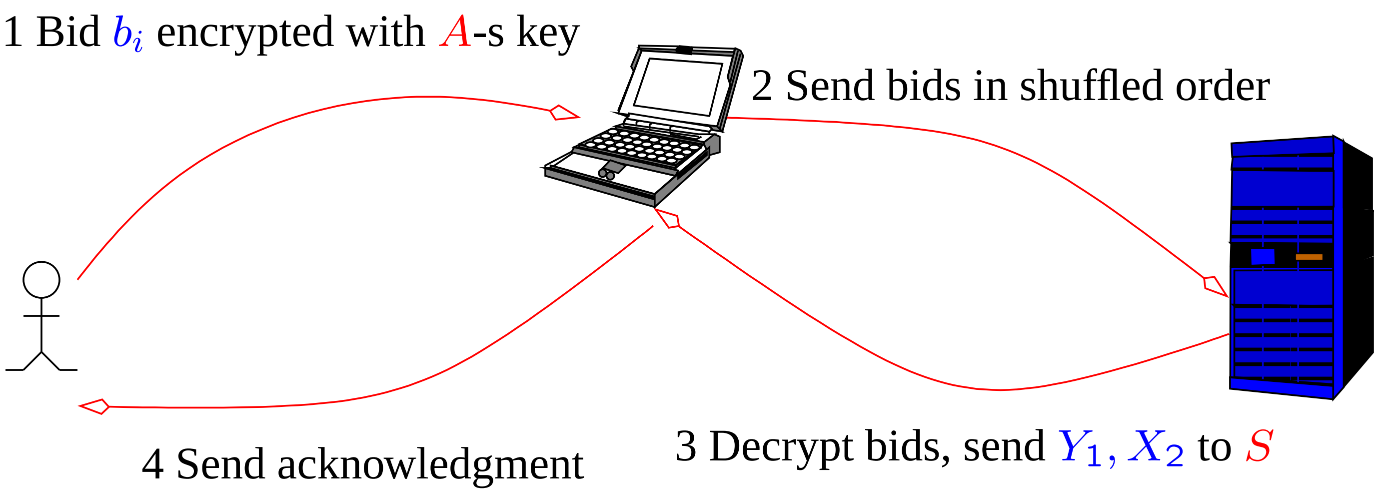
  ⋆ Occasional seller (auctioneer)

- Third party A (auction authority)

  ⋆ A is assumed to be an established party

- Scheme should be secure unless both A and S are malicious

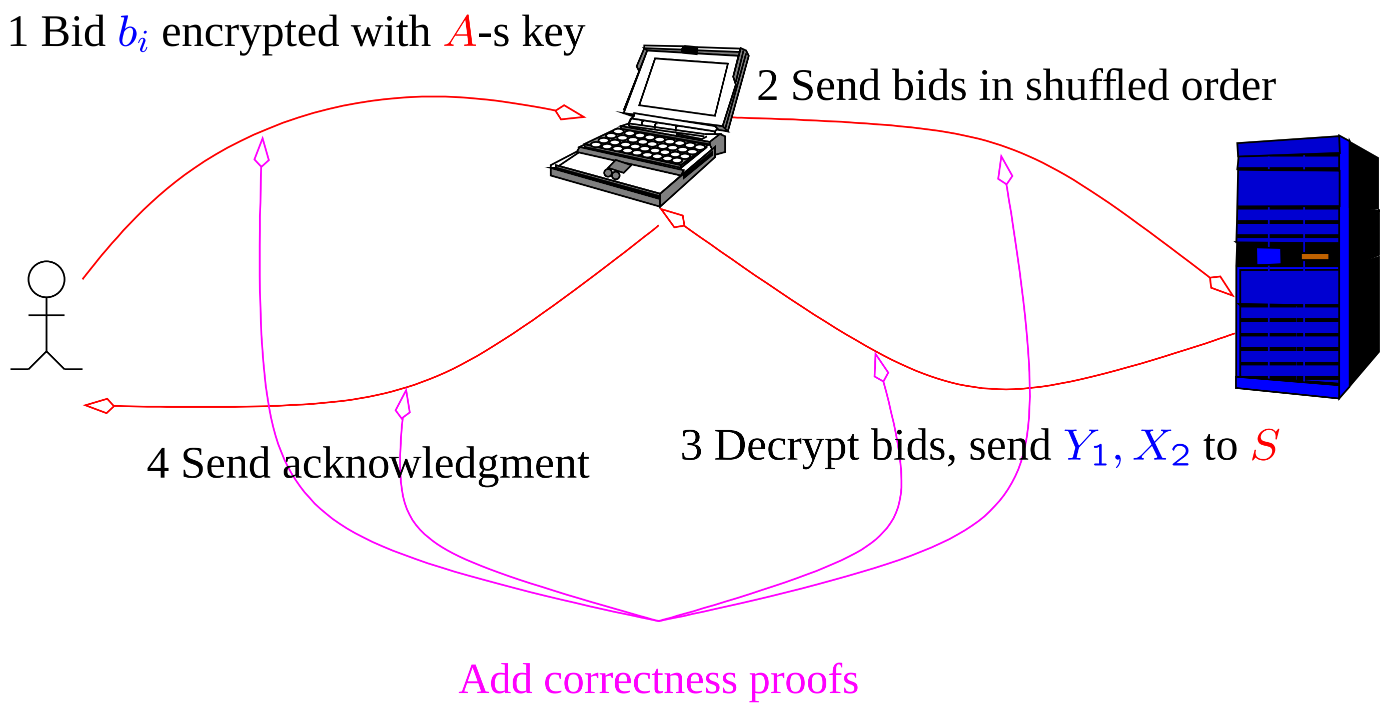
Simple scheme



S will not get any extra information, but S can increase X_2

$A \rightarrow S$ interaction is quite large

Simple scheme → complex scheme



Proofs of correctness

1. Complex: use bulletin board, prove that bid belongs to some set

2. Complex: combine bids, prove correctness of combination

3. Complex: extract X_2, prove it

4. Simple: (Y_1, X_2) signed by S

Bid encoding and combination

1. Encoding: bid b_i is encoded as B^{b_i}, B — maximum number of valuations (bid)

2. Bidder sends a $c = E_A(B^{b_i})$ together with a proof and that b_i is encoded correctly

3. S combines $\{E_A(B^{b_i})\}$ by $c = \prod_i E_A(B^{b_i})$

4. S broadcasts c and all bids

5. Everybody can verify that c was correctly computed

(Similar to Damgård-Jurik voting scheme.)

How to prove that bid is correct?

- Bidder proves that $c = E_A(B^{b_i})$ encodes a number B^{μ} with $\mu \in [0, V-1]$

How to prove that X_2 is correct?

- A has decrypted c and decoded it as $s = \sum_j x_j B^j$

- Second highest bid X_2 has the next properties: Either

  ⋆ (no tie-break) $s = B^\chi + B^{X_2} + \tau$, $\chi > X_2$ and $\tau < B^{X_2+1}$, for some χ, τ, or

  ⋆ (tie-break) $s = 2B^{X_2} + \tau$, $\tau < B^{X_2+1}$, for some τ

- Everything is standard, except for the range proofs of form $a <^? b$ and range proofs in exponents of form $g^a <^? g^b$

Range proofs in exponents (R-PIE)

- Show that encrypted value is g^a, $a \in [\ell, h]$

- Proof 1: Use oblivious binary search (1-out-of-2 proofs)
  - ⋆ Proposed in [Damgård-Jurik 2001]
  - ⋆ Their proof had a flaw that is corrected in our paper

- Proof 2: Prove that $g^\ell \mid g^a$ and $g^a \mid g^h$
  - ⋆ More efficient than proof 1 but assumes that g is a prime

Range proofs

- Show that encrypted value is a, $a \in [\ell, h]$
- Idea: Use Lagrange's theorem that every nonnegative number is a sum of four squares, prove that $c = E_K(\mu_1^2 + \cdots + \mu_4^2; \rho)$
  - ⋆ Very efficient communication-wise
  - ⋆ Drawback: must use an integer commitment scheme [Damgård-Fujisaki 2001]

Encryption scheme

- We use Damgård-Jurik encryption scheme

  ⋆ doubly homomorphic:
  $E_K(m_1 + m_2; r_1 + r_2) = E_K(m_1; r_1)E_K(m_2; r_2)$

  ⋆ plaintext space can be flexibly enlarged

  ⋆ *coin-extrability*: private key can be used to extract coin r from ciphertext $c = E_K(m; r)$

Extensions

- Influence of collisions can be reduced
  - ⋆ Collaborating A and S cannot change (Y_1, X_2)
- Efficient $(m+1)$-st price auctions
  - ⋆ $A \to S$ proof length increases by $(m-2)(C+\ell) \approx 5000(m-2)$ bits
  - ⋆ C — length of ciphertext space, ℓ — length of the R-PIE

How to prove that X_{m+1} is correct?

- A has decrypted c and decoded it as $s = \sum_j x_j B^j$

- $(m+1)$st highest bid X_{m+1} has the next properties: Either

  ⋆ (no tie-break) $s = B^{\chi_1} + \cdots + B^{\chi_m} + B^{X_2} + \tau$, $\chi_j > X_{m+1}$ and $\tau < B^{X_{m+1}+1}$, for some χ_i, τ, or

  ⋆ (tie-break) $s = 2B^{X_{m+1}} + \tau$, $\tau < B^{X_{m+1}+1}$, for some τ

Comparisons with Naor-Sumner-Pinkas

- NPS: the only serious contender (at the time of writing)

$+$ efficiency: interaction $A \leftrightarrow S$ greatly reduced (more than 100 times in large-scale auctions)

$+$ security: a cheating A can be detected without cut-and-choose attacks

$-$ efficiency: number of valuations V is effectively limited to ≤ 500

$-$ security: A will know the bid statistics (how many bidders bid b for every b)

Why knowing bid statistics might not be bad?

- Our target: large-scale occasional auctions
- The next auction rarely has the same bidders
- Use designated verifier signatures
  - $\star$ A has no means to convince she is selling correct data
- A has a brand name, easily ruined by selling the data

Applications to e-voting

- Damgård-Jurik voting scheme: vote b_i is encoded as B^{b_i}, B the maximum number of voters

- Similar to our auction scheme, except that they do not require to prove the correctness of X_2

- Therefore, A can be thresholded

- Our improvements: more efficient vote correctness proof via R-PIE

Open problems

- How to avoid A to get knowing the bid statistics?
  - ⋆ Threshold the proof that X_2 is correct
- Our efficient R-PIE required B to be a prime
  - ⋆ How to escape this assumption?
  - ⋆ Unfortunately, we have already solved this
- NPS comunication $O(B \log_2 V)$, our complexity $O(V \log_2 B)$.
  - ⋆ Is there anything in between?

Conclusions

- A new Vickrey auction scheme that works without threshold trust
  - $\star$ threshold trust is unacceptable in our target scenarios
- Only serious contender: Naor-Sumner-Pinkas auction scheme
  - $+$ ours is $10 \dots 100$ times more communication-efficient
  - $-$ but limits the number of valuations to ≈ 300
- We proposed some novel general cryptographic protocols
- Our scheme is an e-voting protocol in disguise