Private Auctions with Multiple Rounds and Multiple Items

Ahmad-Reza Sadeghi
Universität des Saarlandes
FR 6.2 Informatik
D-66041 Saarbrücken,
Germany
sadeghi@cs.uni-sb.de

Matthias Schunter
IBM Zurich Research Lab
Computer Science Dep.
CH-8803 Rüschlikon,
Switzerland
schunter@acm.org

Sandra Steinbrecher
Technische Universität Dresden
Fakultät Informatik
D-01062 Dresden,
Germany
steinbrecher@acm.org

Abstract

For selling spectrum licenses economists have designed new auction types proceeding over several rounds and offering several licenses simultaneously. Communication between bidders usually is forbidden to prevent collusions (i.e., through separate compartments and supervision). We investigate these auctions from the cryptographic point of view and identify that the usual implementation by a succession of (traditional) sealed-bid auctions where the auctioneer announces at least winner and winning bid of each round offers a covert channel to the bidders. The announcement should be limited to the minimum a bidder needs to know for taking part in the next round. We suggest that the bids made are kept private and she only gets to know which items she currently wins. Only at the end, overall winners and winning bids are revealed. We present a protocol based on a special sealed-bid auction that implements this idea.

1. Introduction

Auctions are methods to determine the price people are willing to pay for rare items without common valuation. Every participant (seller, auctioneer and bidder) has a valuation of the item offered. Economists distinguish different models of valuation [8]. In the private-value model every participants' valuation is only known to her. The more she finds out about others' valuations, the more her own might change. A well-investigated auction type based on this model is the sealed-bid auction. Every bidder only has one chance to bid. Without knowing the other bidders' valuation she submits her bid secretly to the auctioneer who opens all bids simultaneously and determines winner and winning bid. Cryptographic potocols realizing sealed-bid auctions are described in Section 2.1.

New auction types were designed and tested for selling spectrum licenses (especially by the Federal Communications Commission (FCC)) because they are multiple interdependent items without common valuation. The auctions proceed over multiple rounds and sell multiple items simultaneously. In every round every bidder has to increase or hold the bid she has made for an item in the previous round. After each round winner and winning bid of every item are announced. The auction terminates when no bid was raised. Often there are several restrictions on (e.g., in the German UMTS auction every winner had to win at least 2 licenses).

The execution of multiple rounds gives a bidder the chance to win items desired as the FCC argues [6]. By the way this increases the seller's (in the U.S. the FCC's) profit.

If items have interdependencies they should be sold simultaneously. E.g., a license for an area may be worthless without the license for an adjoining area. If they were sold sequentially a bidder's chance to obtain a subset with the required interdependence is worse than in a simultaneous auction where she can change the desired subset [6].

Cryptographers have not investigated these auctions types in detail so far although some protocols for sealed-bid auctions can be used as building blocks as a note in [13] already suggests. Multiple rounds only have been a solution to collisions of winning bids in sealed-bid auctions [12]: The 'winners' take part in one or several additional sealed-bid auction(s) on their bid increments. But auctions with multiple rounds and items cannot always be implemented by a succession of sealed-bid auctions because this leads to auctions not necessarily sealed-bid during the whole duration but only during one round. Since this may lower the bids auctions based on the private-value model try to prevent any communication between bidders by organizational measures (e.g. separate compartments, supervision). Even though these measures reach their goal there are still other possibilities for communication between the bidders. Every information they get during the auction enables covert channels between colluders or competitors. Experience has shown that bidders use these channel and vary their strategy due to changes in others' behavior during the auction.

In the FCC spectrum auctions in the U.S. bidders used the last few digits to encode their company names or numbers of desired markets [3] (bid signaling).

Some strategies against covert communication have been used in the FCC spectrum auctions [3], but they do not always limit the information given in a round to the minimum. The only information a bidder needs to participate in the next round is if she currently wins an item. In the later rounds she can increase her bid as much as necessary. This strategy might be inefficient it does not lower the winning bids. Only at the end, winner and winning bids are revealed.

We investigate the requirements on and the properties of auctions with multiple rounds and items in Section 2.2 and show the differences to sealed-bid auctions. Finally, in Section 3 we suggest an implementation limiting the information given to a bidder to the above minimum.

2. Cryptographic Auction Design

We describe sealed-bid auctions and auctions with multiple rounds and items, their necessary requirements and additional properties. In both an auctioneer $\mathcal{A}$ and m bidders $\mathcal{P}_1, \ldots, \mathcal{P}_m$ participate.

2.1. Sealed-Bid Auction

1. **Announcing phase:** $\mathcal{A}$ announces the offered item, the auction rule and the possible additional properties.
2. **Submission phase:** $\forall j \in [1:m]$: $\mathcal{P}_j$ turns in her bid b_j secretly to the auctioneer.
3. **Determination phase:** $\mathcal{A}$ determines winner and winning bid according to the auction rule and announces his outcome.

An exchange phase has to be added to guarantee a fair exchange of money and item. A solution can be found in [17]. We will not dispose on the exchange in the following.

Auction Rule: The auction rule specifies winner and winning bid determination and the length of the submission phase. The winner usually is the bidder who turned in the highest bid, while the winning price is the α-th-highest bid ($1 \leq \alpha \leq m$) in the so-called sealed-bid α-price auction.

Necessary Requirements:

- **Accountability:** Every bidder is responsible for her bids. Especially the auctioneer must be able to prove that a certain bid has been turned in by the bidder.
- **Correctness:** Winner and winning bid are determined correctly among the bids that have the corrrect form and were handed in during the bidding phase. If the auctioneer is not totally trusted either his task should be split among several auction servers or every participant must be able to verify the auctioneer's evaluation.
- **No Communication:** Direct communication between the bidders is forbidden to prevent collusions.

Additional Properties:

(α) **Anonymity:** Bidders might use either their real names or pseudonyms.

- **Possible bids:** The number of possible bids influences the probability of collisions of the winning bid. These collisions have to be solved in an additional phase of tie-breaking where the winners take part in an additional sealed-bid auction on their bid increments [12].

(β) **Privacy:** The bids are private during the submission phase, but in the determination phase at least one is revealed. In the case of future auctions with similar items this might influence bidders' bids and the reserve price an auctioneer might set. To prevent the auctioneer from learning all bids the determination of winner and winning bid might be performed on encrypted inputs or inputs are shared between several auction servers.

The first cryptographic realization of a sealed-bid first-price auction was presented in [4]. Correctness and privacy are guaranteed by distributing the auction service on $n > 1$ servers of which $\leq \lfloor \frac{n-1}{3} \rfloor$ may be adversaries. With verifiable secret and signature sharing the bids are shared among the servers. Bids and winner are revealed to everyone in the determination phase. A similar implementation of a sealed-bid second-price auction is introduced in [1] where winner and winning bid are computed among n auction servers. Therefore every bidder provides each auction server with a share of a secret sharing polynomial encoding her bid.

Another protocol [10] uses general public key cryptography and focuses on the time-dependent application of the auction rule. Unfortunately full trust in three auction servers is needed to guarantee privacy of the bids.

The protocol in [5] uses a primitive solving the millionaire's problem [16] to implement a sealed-bid first-price auction with two semi-trusted auction servers which only outputs the winner. But one server learns a partial order of the bids, and interaction between the bidders is needed.

The only primitive the protocol in [9] uses are hash chains guaranteeing the bidder's accountability. In the determination phase only bids greater than or equal to the winning bid are revealed. But the number of possible bids is very small as in the protocol presented in [7] where the calculation of the m-price sealed-bid auction is split among a number of auction servers greater than the number of possible bids. The bids are encoded in degrees of random polynomials to compute winning bid and winners.

Another protocol [13] shares the computation of an arbitrary auction function between two auction servers. One only constructs the encrypted circuit of the function while the other one uses the garbled values of the bid's bits to evaluate the circuit. This server learns the garbled values by participating in a proxy oblivious transfer protocol.

[11] introduces the primitive Mix-and-Match which is a new approach to general multi-party computation avoiding the use of verifiable secret sharing for distributing the inputs among the participants. This can be applied to auctions.

In [2] only one auction server is involved to calculate the auction function on the encrypted bids' bits for every bidder. Only the correspondent bidder learns if she is the winner. The winner has to prove herself by opening her encrypted bids. If she isn't willing to do so all other bidders are able to prove they are not by opening their bids.

2.2. Auction with multiple rounds and items

1. **Announcing phase:** $\mathcal{A}$ announces the offered item, the auction rule and the possible additional properties.
2. **Bidding phase** $i > 0$**:**
   (a) **Submission** i**:** $\forall j \in [1:m]$: $\mathcal{P}_j$ turns in her bid b_{ji} for every item secretly to the auctioneer.
   (b) **Determination** i**:** Following the auction rule $\mathcal{A}$ determines if the auction should proceed to bidding phase $i+1$ and announces his outcome.
3. **Closing phase:** The auctioneer determines winners and winning bids of every item according to the auction rule and announces his outcome.

Auction Rule: As in sealed-bid auctions the auction rule determines how winners and winning bids are determined. Additionally the auction rule determines for every round which items a bidder is allowed to bid for (e.g., only for the items she has bid in the preceding round). Further the auction rule indicates how the end of the auction is determined depending on the bidders' behavior during the auction (e.g., as long as there are bidders whose bids are greater than a certain bound the auction proceeds to the next round).

Necessary Requirements: Accountability, correctness and no possibility for communication have to be guaranteed as in sealed-bid auctions.

Additional Properties: The following properties have to be upgraded in comparison to Section 2.1:

(α) **Anonymity:** If bidders use pseudonyms they might want to change them depending on round and item to prevent linkability of their bids. But depending on the auction rule his bids for one or several item(s) have to be traceable (e.g., 'Every winner must win at least two items'). The use of pseudonyms certainly should not offer an additional covert channel to colluding bidders.

(β) **Privacy:** Everything a bidder gets to know after a round might influence her bids in subsequent rounds.

(γ) **Repudiation of bids:** Published repudiation of bids offers an additional covert channel [3]. The repudiation of a previous bid can be realized by either allowing lower bids, or by adding a repudiation phase as additional phase 2(c) in the protocol.

(δ) **Possible bids:** If repudiation is not allowed a bidder's bids should rise or stagnate with each round. The smaller the number of possible bids the smaller is the covert channel to everyone who gets to know a bid.

Most sealed-bid auctions presented in 2.1 can be used as building blocks for auctions with multiple items and rounds. But the properties of the first influence the properties of the latter. Our goal is to limit the information given during the auction. We assume that no direct communication is needed to guarantee the necessary requirements and that organizational measures prevent direct communication completely. The above properties are chosen in a way that the information given is reduced to the minimum. Properties already examined and implemented by the FCC [3] are:

($\delta 1$) **Possible bids:** The number of possible increments on bids in every round is limited, especially there is only one. In this special case every bidder only has to decide if she is still interested or not (bid or not bid).

($\gamma 1$) **Repudiation of bids:** The repudiation of a previous bid is only allowed a limited number of times by the organizational measure of a repudiation phase 2(c). Especially after a repudiation the bidder has to pay a fine and is not allowed to bid on the same item again.

So far the following property does not seem to be considered in the FCC spectrum auctions:

($\beta 1$) **Privacy:** Until the end of the auction neither auctioneer nor bidders learns anything except a bidders learns which items he currently wins. After the auction has terminated winners and the winning bids are revealed.

It can be achieved by the following implementation of the bidding phase (2.):

(b1) **Determination:** Only the current winners are able to determine this fact out of $\mathcal{A}$'s broadcasted outcome, none learns anything else.

This implementation might prolong the auction duration but does not influence the auction's reasons for proceeding

over multiple rounds and selling the items simultaneously because every bidder gets the information she needs to proceed: 'Shall I make a higher bid or not?'.

Because auctions are often offered by one entity (e.g. a company or government) it makes no sense to distribute the auction service on several auction servers if they are all under its control. In Section 3 we present a protocol implementing an auction with multiple rounds and items with the bidding phase (b1) based on the primitive from [2] which involves only one auction server. As mentioned in Section 2.1 this protocol enables every bidder to determine whether she is the winner without revealing any additional information. This is exactly the form of implementation needed for phase (b1) of auctions with multiple rounds and items.

Additionally in the FCC auctions it has been observed that the property anonymity might influence the auction as well. Bidders might be cautious to overbid influential companies [3]. Our protocol can be combined with anonymity measures but needs traceability throughout different rounds. For brevity we forbid the possibility of repudiation of bids. The number of possible bids is arbitrary.

3. Implementation

We assume a synchronous network model and authentic channels between $\mathcal{P}_j$ ($1 \leq i \leq m$) and $\mathcal{A}$ to guarantee accountability. Let $l \in \mathbb{N}$ be a public parameter indicating the set of possible bids $[0 : 2^l - 1]$. We use Paillier encryption [14] E with cipher space C and message space $M = \mathcal{Z}_N$ ($|N|$ security parameter). We assume a reliable public key infrastructure is provided. Because in spectrum auctions bidders are companies this assumption is realistic.

3.1. Sealed-Bid First-Price Auction [2]:

1. **Announcing phase:** $\mathcal{A}$ announces the auction with the offered item, the length of the submission phase, the set of possible bids and the auction rule (The auction is first-price and the winner has to prove herself but $\mathcal{P}_j$ learns nothing except whether she is the winner.).
2. **Submission phase:** $\mathcal{P}_j$ ($1 \leq i \leq m$) sends to $\mathcal{A}$ m encryptions (with the other bidders' public keys) of each bit of her bid b_j together with a zero-knowledge proof that she encrypted a bit in $\{0, 1\}$ and a proof of equality of the bits under the m different encryptions.
3. **Determination phase:** $\mathcal{A}$ performs a secure function evaluation on the handed in encryptions and broadcasts his result consisting of m parts. The j-th part ($1 \leq j \leq m$) represents a predicate $b_j \geq \max(b_1, \ldots, b_m)$ which can only be evaluated by $\mathcal{P}_j$ to determine if the is the winner. $\mathcal{A}$ is able to determine the winner by asking everyone to open her encrypted bits.

Efficiency: Obviously the protocol is quite inefficient [2] but still much more efficient than generic techniques [15].

Security: Incorrect encryptions of bidders are prevented by the proofs of correct encryption. The Paillier encryption's self-randomization property prevents bidders from linking inputs and resulting encryptions.

$\mathcal{A}$ is semi-trusted. The bidders trust him that he correctly verifies the bidders' proofs and correctly evaluates the auction function. The opposite of the latter case could be proved by any bidder revealing herself. Privacy of bids against a honest but curious server is ensured by the Paillier encryption's semantic security.

No further active attacks on the protocol are considered in [2]. If the auctioneer colludes with any bidder beneath cheating with the proofs they can trace bids in the circuit and at least find out a partial order of the bids.

3.2. Auction with multiple rounds and items

We use the techniques of the above sealed-bid auction to construct a protocol implementing an auction with multiple rounds. The predicates needed are straightforward extensions of the building blocks in [2]. Especially the gates are calculated in the same way. Due to the lack of space we omit the detailed formulas that have to be fulfilled.

1. **Announcing phase:** $\mathcal{A}$ announces the auction with the offered items, the length of the submission phases, the set of possible bids (depending on item/round), the privacy property ($\beta 1$) and the auction rule (first-price auction, winners have to reveal themselves at the end, every bidder has to bid for each item in every round, the auction ends if no bids are increased). We assume the auction rule contains no further restrictions (e.g., reserve prices).
2. **Bidding phase** $i > 0$**:**
   (a) **Submission** i**:** For every item the submission phase of the sealed-bid auction is executed.
   (b) **Determination** i**:** For every offered item $\mathcal{A}$ verifies the bidders' proofs and performs and announces for every bidder three secure function evaluation on the received encryptions:
      i. Every bidder can check for every item if $\mathcal{P}_j$'s bid b_{ji} in round i is greater than or equal to her bid $b_{j(i-1)}$ in the previous round (expressed by the predicate $b_{ji} \geq b_{j(i-1)}$).
      ii. Every bidder can check if she is the current winner of an item by using the auction function from [2] with the slightly modified predicate $b_j > \max_{1 \leq i \leq m, i \neq j}(b_i)$ to guarantees that no collisions between bids occur at the end of the auction.

iii. Every bidder can check if the auction should proceed to round $i+1$. The auctions ends if no bidder increased her bids in this round (predicate $(b_{ji} = b_{j(i-1)})_{1 \le j \le m}$).

3. **Closing phase:** The winners of the items are the winners of round $i-1$. They indicate the end to the auctioneer (iii) and are able to prove themselves (ii).

Security: The protocol cannot be more secure than its building block. Bidders trying to hand in encryptions of false bids are identified by other bidders (i) or the auctioneer. The result of the three predicates do not help to get any partial information about the bids in this round.

If only winners can indicate the end of the auction some additional rules have to be added to deal with the case of a dishonest ones. A certain number of bidders should be allowed to indicate the end of the auction as well.

Bidders might try to exchange messages by misbehaving (e.g. bidding less than in previous rounds). Measures against this could be to exclude them from further bidding and/or to permute the predicates.

$\mathcal{A}$ is semi-trusted. He has to verify the proofs and performs the three secure function evaluations correctly. The opposite case could be proved by a bidder revealing herself.

A collusion of any bidder and the auctioneer can trace her bids and decrypt the bits encrypted with her public key and at least find out a partial order.

Efficiency: Because the additional secure function evaluations' complexity is negligible in comparison to the overall complexity of the used sealed-bid auction, the complexity of our protocol is about $|items| \cdot |rounds|$ its complexity.

Changing the Properties:

(α) **Anonymity:** Our implementation can be combined with additional anonymity measures. But pseudonyms have to be linkable throughout the rounds.

(γ) **Repudiation of bids:** The proof in phase 2.(b)i. can be extended to allow lower bids than in the previous round. Or in round i it can be executed between $\mathcal{P}_j$'s bids b_i and b_{i-2} to allow the withdrawal of bid b_{i-1}.

Changing the Auction Rule: Restrictions on bidding and winning can be implemented by secure function evaluation.

4. Conclusion

We analyzed the requirements on auctions with multiple rounds and items and the possible properties they might have. Especially we presented a new protocol based on the techniques in [2] that reduces the covert channel between bidders to the minimum. Unfortunately its efficiency makes it only suitable for small sets of bidders and a quite long duration of the auction but in the case of spectrum auctions this usually is fulfilled. In future work we will extend our work to more general sealed-bid auctions as building blocks.

References

[1] M. H. J. D. Tygar Hiroaki Kikuchi. Electronic auctions with private bids. 3rd USENIX Workshop on Electronic Commerce, 1998, 61-73.

[2] O. B. Jaques Stern. Non-interactive private auctions. to appear in Financial Cryptography 2001, Springer-Verlag, Berlin 2001.

[3] P. C. Jesse A. Schwartz. Collusive bidding: Lessons from the fcc spectrum auctions. Journal of Regulatory Economics 17/3 (2000) 229-252.

[4] M. K. F. Michael K. Reiter. The design and implementation of a secure auction service. 1995 IEEE Symposium on Research in Security and Privacy, IEEE Computer Society Press, Los Alamitos 1995, 2-14.

[5] C. Cachin. Efficient private bidding and auctions with an oblivious third party. 6th ACM Conference on Computer and Communications Security (CCS), ACM Press, New York 1999, 120-127.

[6] F. C. Commission. All about auctions (revised 9/21/99). available from http://www.fcc.gov/wtb/auctions/.

[7] H. Kikuchi. (m+1)st-price auction protocol. to appear in Financial Cryptography 2001, Springer-Verlag, Berlin 2001.

[8] P. Klemperer. Auction theory: A guide to the literature. Journal of Economic Surveys 13/3 (1999) 227-286.

[9] K. K. Koutarou Suzuki and H. Morita. Efficient sealed-bid auction using hash chain. Information Security and Cryptology - ICICS 2000, LNCS 2015, Springer-Verlag, Berlin 2001, 183-191.

[10] M. Kudo. Secure electronic sealed-bid auction protocol with public key cryptography. The Transactions of The Institute of Electronics, Communications and Computer Sciences IEICE E81-A/1 (1998) 20-27.

[11] A. J. Markus Jakobsson. Mix and match: secure function evaluation via ciphertexts. Asiacrypt 2000, LNCS 1976, Springer-Verlag, Berlin 2000, 162-177.

[12] H. K. Michael Harkavy, J. D. Tygar. Multi-round anonymous auction protocols. 1st IEEE Workshop on Dependable and Real-Time E-Commerce Systems, 1998.

[13] R. S. Moni Naor, Benny Pinkas. Privacy preserving auctions and mechanism design. 1st ACM Conference on Electronic Commerce, ACM Press, 1999.

[14] P. Paillier. Public-key cryptosystems based on composite degree residuosity classes. Eurocrypt '99, LNCS 1592, Springer-Verlag, Berlin 1999, 223-238.

[15] M. Y. Tomas Sander, Adam Young. Non-interactive cryptocomputing for nc^1, proceedings of the 31st stoc, acm, 1999.

[16] A. C. Yao. Protocols for secure computations. 23rd Symposium on Foundations of Computer Science (FOCS) 1982, IEEE Computer Society, 1982, 160-164.

[17] V. V. Yi Mu. An internet anonymous auction scheme. Information Security and Cryptology - ICICS 2000, LNCS 2015, Springer-Verlag, Berlin 2001, 171-182.