Auctions with Rational Adversary

Sourya Joyee De and Asim K. Pal

Management Information Systems Group,
Indian Institute of Management Calcutta, India

Abstract. Security of various types of online auctions has received a considerable attention from researchers. However, very few works have analyzed the problem of security in online sealed-bid auctions from the point of view of rational participants. The paper deals with an online auction scenario where two types of participants co-exist: 1) a party corrupted by a rational adversary that have positive utilities from information gained and that has no valuation for the items on auction enabling them to bid arbitrarily and 2) rational parties that are privacy conscious, positively value information gain and have a valuation for items on auction. The secure auction protocol proposed here addresses 1) privacy concerns of the rational players from themselves as well as the rational adversary; 2) prevention of 'throwing away' of contracts by rational adversaries and 3) prevention of sellers from obtaining their copy of the contract while winners do not receive theirs.

1 Introduction

Security of various types of online auctions (such as combinatorial, Vickery-Clarke-Groves, first price etc) has received considerable attention from researchers during the past two decades [1–3, 8, 11–13]. Important security concerns in online auctions include bid privacy, bidder anonymity, correct evaluation and declaration of winner etc. Both the auctioneer and the bidders can be considered dishonest – while bidders may try to know the bid values of other bidders, the auctioneer may not only try to know the bid values (for e.g. the knowledge of the second highest bid value helps to set reservation price in second price auction) but also manipulate results. Incorrect outcome may result from introduction of false bids or modification of submitted bids, undue extension or shortening of bidding period and introduction of new bids based on information about submitted bids, bidder-auctioneer collusion, collusion among bidders etc. For bidders, bid values may be sensitive information and loss of bid-privacy may reveal important information such as financial status etc. against their wishes. Cryptographic techniques have been predominantly used to overcome these difficulties. However, very few works have analyzed the problem of security in online sealed-bid auctions from the point of view of rational participants. Traditionally, cryptographic protocols for secure computation in auctions have achieved privacy and security not as an equilibrium strategy to the game which every party will find in their best interest to follow but as "...a second-phase technical level outside of the scope of game and parties' strategies.."[10].

A. Bagchi and I. Ray (Eds.): ICISS 2013, LNCS 8303, pp. 91–105, 2013.

In [10], the authors discuss about privacy-enhanced auctions with rational cryptography and propose a protocol that is in computational Nash Equilibrium for even privacy-conscious players to follow. Here, bidders wish to know information about other bidders' valuations or types while not revealing any information about its own type. More formally, rational players have a hybrid utility i.e. a monetary utility from winning an item in the auction as well as an information utility from learning about others' bids while not giving up any information about ones own bid. Bidders participate in a secure multi-party computation simulating the mediator of a mediated auction mechanism Mec and at the end each winner receives a contract which is a document digitally signed by all participants associating the winner with the correct item-value pair. The seller is assumed to have made a commitment to sell his items to bidders who can show him a valid contract. Fair distribution of contracts has been achieved in non-simultaneous, point-to-point channel using concepts from rational secret reconstruction mechanisms [4, 5, 7, 9] where a winner receives its contract in a randomly chosen epoch. Each player obtains a list of shares of the contracts after the computation of Mec and in each epoch, players communicate their shares one by one so that at the end of the epoch a player can reconstruct a value which is either the contract or some other default value. When there are multiple winners, a privacy-conscious winner who has been able to reconstruct its contract at the end of a particular epoch shall find it beneficial to stop communicating its shares henceforth because contracts of other winners may reveal some information about its valuation. So other winners are unable to reconstruct their contract. This problem is solved by revealing the information in the contract in a round prior to the one in which the actual contract is to be received. If any player aborts in this round then nobody gets the contracts due to be revealed in the next round. Since each player has a monetary utility of obtaining this contract they continue communicating shares even in the next round. A winner can reject the contract he won, modelled by the mediated setting with reject. However, the authors consider that when winners opt for 'reject' they gain zero monetary utility instead of the contract. Winners do not 'throw away' their contracts without buying the item simply because they assign a positive utility for the contract.

Given this background, we are interested in what happens when at least one player is only interested in the information revealing round rather than the contract reconstruction round that comes after it, other players being rational in the sense described earlier? Such a player is only interested in knowing the information revealed in the contracts but not in the item won i.e. it positively valuates the information it learns while it has no valuation of the items being sold in the auction. We call a player behaving in this way a rational adversary. We assume the availability of non-simultaneous channel for communication and deal with only first price and second price auctions. If a rational adversary were to participate in the privacy-enhanced auction mechanism just described, no winner will be able to reconstruct his contract because the adversary will have no

incentive to continue after the information-revealing round and hence will abort immediately. The following practical examples suitably describe this situation.

Example 1. Bob is selling an old painting using Vickery auction through an online auction website. Coincidentally, Alice also possesses a painting of the same painter but has no idea how much price such a painting could fetch her if she sold it. However, she is certain that no one will be willing to pay more than a million dollars for that painting. So, she bids a million dollars for Bob's painting and waits to hear the winning price. As a rule, the winning price is only announced to the winner and the seller. Alice wins the auction and comes to know that the best bid next to hers was only a thousand dollars. She does not buy the painting of course. Bob can only mark her with a negative reputation as a buyer.

Example 2. Bob is selling a painting using a first price sealed bid auction in an online site. Alice wants to know whether a similar painting will fetch her a thousand dollars or not. The auction site enables buyers to blacklist any seller who does not deliver a sold item. So instead of directly putting up the painting for auction, she bids a thousand dollars at Bob's auction; if she wins then she knows that the painting may not actually fetch her as much money as she requires. This information can enable her to decide whether to put up the painting for auction. Throwing away of the contract leads to a loss for other bidders who would have bought the item if they won and the seller who has to conduct yet another auction for the same item to sell it, still being unsure whether someone like Alice will not participate again. Additionally, bidders may also wish to know information on the types of other bidders. Bidders who are privacy conscious have disincentives to participate in an auction protocol which leaks information about their types. On the other hand, sellers are revenue conscious and thus will not have any incentive to hold an auction of their items if adversaries place arbitrary bids in the auction to win and then never actually buy the item.

Our Contributions. We discuss a problem scenario consisting of two types of participants that co-exist: 1) a party corrupted by a rational adversary that have positive utilities from information gained and that has no valuation for the items on auction enabling them to bid arbitrarily (leading to "gain information, win and throw away contract"behavior) and 2) rational parties that are privacy conscious, positively value information gain and have a valuation for items on auction. Neither privacy conscious rational participants nor revenue-conscious sellers will find it beneficial to participate in online auctions that are not secure against a rational adversary. Our secure auction protocol addresses 1) privacy concerns of the rational players from themselves (because of conflicting interest in information gain and privacy-consciousness) as well as the rational adversary; 2) prevention of 'throwing away' of contracts by rational adversaries and 3) prevention of sellers from obtaining their copy of the contract while winners do not receive theirs. It uses the concept of rational secret reconstruction. Each winner is to receive a contract which is a legal document stating the item-value pair it has won. The seller possesses a counter-part of this contract having the same information. If either of them fails to honor the commitment associated with the

contract then the other can seek suitable compensation in the court of law. Each winner partially reconstructs its contract by participating in a fair reconstruction mechanism with other players while the contract is fully recovered only after the winner communicates with the seller. We show that it is in computational strict Nash Equilibrium for rational adversaries, rational players and a seller to follow this protocol while rational adversaries only bid values that are upper-bounded by their information utility of the contract.

Online auctions inevitably result in the transfer of physical goods from the buyer to the seller (unless the item on auction is an electronic file). To enforce the physical transfer of goods and payment for the same, the contract must be enforced. Many popular vendors such as eBay do this by means of reputation scores, user agreements etc. The reputation score of a buyer has to be computed over a period of time, based on many instances of the buyer's participation. So, new buyers do not have reputation scores. Moreover, sometimes reputed buyers may also behave like a rational adversary. It is not necessary that a buyer always exhibits the same kind of behavior, whether honest or adversarial. He may honestly buy the items he has won most of the times, thus obtaining a good reputation score, but once in a while, he may wish to deviate. Reputation score can limit the number of instances of rational adversarial behavior but cannot totally eradicate the problem. The legal contract in our system is no better or no worse than that being used by eBay, as both are expected to operate under the same domestic or international laws. The major difference between eBay and our system is that eBay acts as a trusted third party (TTP) that computes the result of the auction, while, in our case, the bidders and sellers can themselves compute the output without relying on any TTP. In the absence of a trusted mediator, if fairness is not ensured then even if the contract is enforced or there is a user agreement, the winner (seller) can abort early so that the seller (winner) may not even know who has won. The situation is further complicated by the fact that the communication takes place over an unreliable channel, the Internet, so that a bidder may have to abort early, not intentionally but due to failure of communication. Under this situation our protocol ensures fairness even after allowing early abort in the presence of rational adversary, rational players and the seller.

Organization of the Paper. This paper is organized as follows. In section 2, we describe the preliminaries such as utilities of rational adversary, rational players and the seller and finally define what we mean by a secure auction protocol. In section 3, we propose our secure auction mechanism while in section 4 we finally conclude.

2 Sealed-Bid Auctions and Its Participants

In this section we describe sealed-bid auctions followed by equilibrium notions and nature of participants in an online auction and their utilities. We finally use these concepts to define secure online auctions in our settings.

Table 1. Symbols Used

Symbol	Meaning
$Mec()$	The auction/allocation mechanism
k	Security parameter
$\mu^{'}$, $\mu^{''}$, $negl$	Negligible functions
r	Index of a run of the unmediated auction mechanism
P_i (P_{-i})	ith player or bidder or participant (any player other than P_i)
A	Rational adversary
T_i	Type space of bidder P_i
t_i	Type of bidder P_i
t	Vector of types of bidders
b_i	Bid value of bidder P_i
o_i	Output of the auction mechanism for P_i
(Γ, σ)	A mechanism consisting of the game Γ and the strategy $\sigma = (\sigma_i, \sigma_{-i})$ suggested by the protocol designer
σ_i, (σ_{-i})	Suggested strategy for P_i (P_{-i})
$\sigma_i^{'}$	Any strategy other than the suggested strategy followed by P_i
$u_i(\sigma)$	Utility of P_i when everybody (including itself) follows σ
$u_i(\sigma_i^{'}, \sigma_{-i})$	Utility of P_i when it follows $\sigma_i^{'}$ while everybody else follows σ_{-i}
$Info_i^r$ ($Info_{-i}^r$, $Info_A^r$)	Information set consisting of pieces of information collected by P_i (P_{-i}, A) about other participants in run r of an unmediated auction mechanism
$u_A^I(Info_A^r, Info_{-i}^r)$	Information utility of A when its information set is $Info_A^r$ and that of others are $Info_{-i}^r$
$u_i^I(Info_i^r, Info_{-i}^r)$	Information utility of P_i when its information set is $Info_i^r$ and that of others are $Info_{-i}^r$
o_r	Vector of outputs received by all participants at the end of run r
o_i^r (o_A^r, $o_{r,s}$)	Output received by P_i (A, seller) at the end of run r
$u_i^{auc}(o_r, t)$ ($u_A^{auc}(o_r, t)$, $u_S^{auc}(o_{r,s}, t)$)	Auction utility of P_i (A, seller)
$u_i(r, t)$	Overall utility of P_i for run r

2.1 Sealed-Bid Auctions

Classical sealed bid auctions can be looked upon as Bayesian games of incomplete information. The n players $P_1, \ldots, P_n$ participating in this game are called bidders. At the beginning of the game, each bidder P_i receives private information regarding its type $t_i \in T_i$ where T_i is the type space of that bidder. The vector of bidders types $t = (t_1, \ldots, t_n)$ is drawn from $T = T_1 \ldots T_n$ according to a probability density $\phi(.)$. Each bidder P_i then strategically chooses and submits his bid b_i according to its type t_i (a bidder's type is its valuation of the item on auction). The allocation mechanism Mec, depending on the received bids $b = (b_1, \ldots, b_n)$ allocates items to bidders as well as computes a price of each item won. We have $o = (o_1, \ldots, o_n) = Mec(b)$ where o_i represents whether P_i is the winner or not and if he is the winner then the price of the item he has won. For a single item auction, if it wins P_i has the positive utility of $(t_i - p)$ where t_i is P_i's true valuation of the item and p is the price of the item; otherwise its utility is 0. In the particular case of Vickery auction, if P_i is the winner then, $p = Max(b_1, \ldots, b_{i-1}, b_{i+1}, \ldots, b_n)$.

A secure rational unmediated auction mechanism consists of the game Γ and a suggested strategy σ. The game can be looked upon as a tree of all possible paths formed by combination of all possible strategies that participants may follow. Each such path can be called a run. The root node of the tree is the initial state of the game, whereas later nodes depict states as the game progresses (for example, as participants exchange messages) [7]. For different runs, participants will have different information gains and obtain different outcomes (i.e. all winners receive contract or only one receives etc). The suggested strategy or protocol will lead to a run that each player will find it in its best interest to follow. Such a strategy is said to be in equilibrium, such as Nash Equilibrium.

2.2 Equilibrium Notions

A suggested strategy σ of a mechanism (Γ, σ) is said to be in Nash equilibrium when there is no incentive for a player P_i to deviate from the suggested strategy, given that everyone else is following this strategy. In the setting of cryptography, in many cases, players are assumed to be computationally bounded which calls for a suitable modification in the notion of Nash equilibrium used. Here we reiterate the definition of computational strict Nash Equilibrium [4] which we use for our protocol.

Definition 1. *(Computational strict Nash Equilibrium [4]) The suggested strategy σ in the mechanism (Γ, σ) is a computational strict Nash Equilibrium if for every P_i and for any probabilistic polynomial time strategy $\sigma_i^{'}, u_i(\sigma_i^{'}, \sigma_{-i}) < u_i(\sigma) + \mu^{''}(k)$ for some negligible $\mu^{''}$.*

2.3 Nature of Participants and Utilities

The first consideration of rational adversaries appears in the context of the Byzantine Agreement problem in [6] where a rational adversary is said to be

characterized by some utility function describing its preference over the outcomes of the protocol in question. In their case, at most t players are controlled by this rational adversary who wishes to achieve a particular outcome (different from the intended one) for the Byzantine agreement protocol while the rest are honest. In our case, the utility of the rational adversary is defined over the information it gains during the protocol execution as well as the outcome of the protocol itself i.e. over a run of the unmediated auction mechanism. We assume that a corrupted player is controlled by the rational adversary. Uncorrupted players are rational with preferences as mentioned earlier. We do not model envy i.e. neither the rational players nor the rational adversary prevents others from gaining monetary utility due to the item on sale. All players are computationally bounded. The seller finds it beneficial to participate in protocols where contracts are honored by winners. This is depicted by the auction utility of the seller. However, the seller may try to be unfair and try to obtain the contract alone. This is because the contract is assumed to have a monetary value for the seller. We define two types of utilities: the information utility and the auction utility. However we distinguish between the information and auction utilities of the rational adversary from those of the rational players. For sellers only auction utility is defined. The overall utility of a player is the combined value of the auction utility and the information utility.

Information Utilities. Suppose $Info_i^r$ is the information set consisting of pieces of information I_{ij}^r collected by a participant P_i about another participant P_j $(j \neq i)$ in a run r of an unmediated auction mechanism.

Information Utility of Rational Adversary. Suppose the rational adversary A controls the bidder P_i while the remaining bidders are rational players, denoted by P_{-i}. Then, I_A denotes the set of information pieces gathered by the adversary A and I_{-i} denotes the sets of information pieces gathered by the rational player P_{-i} in a particular run of the unmediated auction mechanism. Then the information utility for the adversary is expressed by the function u_A^I such that:

1. $u_A^I(Info_A^r, Info_{-i}^r) > 0$ whenever $Info_A^r \neq \phi$ and $u_A^I(Info_A^r, Info_{-i}^r) \leq 0$ otherwise,
2. $u_A^I(Info_A^r, Info_{-i}^{r'}) \geq u_A^I(Info_A^r, Info_{-i}^r)$ whenever $Info_A^r \subseteq Info_A^{r'}$.

In other words, the rational adversary has a positive information utility whenever it gains a piece of information about any other participant. Moreover, it is not privacy conscious; it is only interested in gaining whatever information it can. The utility maximizing rational adversary thus prefers a run for which it gathers the most information, irrespective of the information gathered by others.

Information Utility of Rational Party. Suppose P_j is a rational party. The information utility for any rational party P_j is expressed by the function u_j^I such that it captures any arbitrary privacy concern with the constraint that [10]:

1. $u_j^I(Info_j^{r'}, Info_{-j}^{r'}) \leq u_j^I(Info_j^r, Info_{-j}^r) + \epsilon$ whenever $Info_j^r \subset Info_j^{r'}$ and $Info_{-j}^r = Info_{-j}^{r'}$ where ϵ is negligible.
2. u_j^I is poly-time computable.

Therefore, a rational party prefers a run of the unmediated auction mechanism which has the least privacy concern and the most information gain. We assume privacy concerns that are sufficiently small with respect to the expected utility of participating in the game. Note that the seller does not have any information utility.

Auction Utilities. Suppose o^r denotes the vector of outputs received by all participants at the end of run r and t denotes the vector of types of the different participants. The seller obtains a corresponding vector $o^{r,s}$ at the end of the run r. The auction utility of a rational player P_i is expressed by the function u_i^{auc} such that: $u_i^{auc}(o^r, t) > 0$ if o_i^r is the contract; else $u_i^{auc}(o^r, t) = 0$. On the other hand, the rational adversary has the following utilities: $u_A^{auc}(o^r, t) = 0$ if it does not win the auction i.e. o_A^r is not the contract or if he does not have to buy the item he won whereas $u_A^{auc}(o^r, t) < 0$ if o_A^r is the contract and it must buy the item he won. In fact, $u_A^{auc} = -p$ where p is the winning price for the item. The auction utility of a seller is expressed as follows: $u_S^{auc}(o^{r,s}, t) > 0$ when at least one of the participants in the auction is a rational player with positive auction utility when it wins. The overall utility of a participant P_i (which is either a rational adversary A or a rational party) for run r in the unmediated auction mechanism is given by:

$$u_i(r, t) = u_i^I(Info_i^r, Info_{-i}^r) + u_i^{auc}(o^r, t)$$

We can write the overall utility for a rational party simply as $u_R = u_R^I + u_R^{auc}$ and that of a rational adversary as $u_A = u_A^I + u_A^{auc}$. The seller's utility is simply represented as u_S which is the same as his auction utility. Suppose the suggested strategy i.e. the secure protocol for the unmediated auction mechanism for each party P_i is $\sigma_{i,s}$. Then, the utility of a participant to follow this protocol is $u_i(\sigma_{i,s}, \sigma_{-i,s}) = u_i^I(Info_i^{\sigma_{i,s},\sigma_{-i,s}}, Info_{-i}^{\sigma_{i,s},\sigma_{-i,s}}) + u_i^{auc}(o^{\sigma_{i,s},\sigma_{-i,s}}, t)$.

2.4 Secure Online Auction

The security of an auction protocol in the presence of rational adversary, rational parties and the seller with information and auction utilities as described in the last section must address 1) privacy concerns of the rational players from themselves (because of conflicting interest in information gain and privacy-consciousness) as well as the rational adversary; 2) prevention of 'throwing away' of contracts by rational adversaries and 3) prevention of sellers from obtaining their copy of the contract while winners do not receive theirs. The secure protocol must be such that it is in the best interest of all participants to follow the protocol i.e. the suggested strategy should be an equilibrium strategy. We define a computationally secure auction protocol in the following way:

Definition 2. *(Computationally Secure Auction Protocol.) An auction protocol π^{auc} which is a suggested strategy $\sigma_s = (\sigma_{i,s}, \sigma_{-i,s})$ in an unmediated auction*

game Γ^{auc} is said to be computationally secure against a rational adversary with overall utility $u_A = u_A^I + u_A^{auc}$, a rational party with overall utility $u_R = u_R^I + u_R^{auc}$ and a seller with utility u_S if the following conditions are satisfied:

1. *σ_s is a computational strict Nash equilibrium for the rational players for every deviating strategy σ_{dev} i.e. $u_R(\sigma_{dev}) < u_R(\sigma_s) + negl(k)$.*
2. *The rational adversary bids a value $b_A < u_A^I$. In addition, σ_s is a computational strict Nash equilibrium for the rational adversary for every deviating strategy σ_{dev} i.e. $u_A(\sigma_{dev}) < u_A(\sigma_s) + negl(k)$.*
3. *It is beneficial for the seller to participate in the protocol i.e. $u_S(\sigma_s) > 0$ and σ_s is a computational strict Nash equilibrium for the seller for every deviating strategy σ_{dev} i.e. $u_S(\sigma_{dev}) < u_S(\sigma_s) + negl(k)$. Here k is a security parameter and $negl(k)$ is a negligible function in k and the above conditions hold for infinitely many values of k.*

3 Secure Auction Protocol

For a second price auction bidding infinity becomes the dominant strategy whenever the contract is not enforced. Even in the ideal/mediated setting that does not allow reject (and ends in distributing the contract to the bidders), presence of the rational adversary in addition to the rational players has the same effect as the mediated setting with reject where only rational players participate. This implies that simply associating monetary utility of players with the contract does not solve our problem. Instead, we must enforce the contract. For a player who has no monetary utility for the item on auction, enforcement of the contract acts as a deterrent to bid arbitrarily. If players are allowed to reject or if they come to know that they have obtained the required information in the contract in the revealing epoch itself then for the rational adversary who assigns no monetary value to the contract itself but only to the information in the contract this epoch then is the point where one can deviate or to reject the contract after having a look at it. To avoid this problem, rejection should not be allowed.

We define the contract obtained as the outcome of the auction to be a legal document containing the information about the winner, the price the winning bidder has to pay and the item it has won if different items are being auctioned by the same seller. It has a seller's copy and a winner's copy. So, the seller can claim an amount of money equal to the winning price of an item by showing his copy of the contract to an appropriate authority, say a bank. On the other hand the winner of a contract gets information about the item he won and the price he has to pay for it from the contract and can also legally claim the item by showing the contract to the appropriate person i.e. the seller. Since the contract has legal validity, the winner can also seek compensation if the seller does not honor his commitment to sell the item won. Thus, when the seller obtains his copy of the contract it can be assumed to be as good as obtaining the payment for the item the particular winner has won. Similarly when the winner has obtained the contract it is as good as obtaining the item he has won. Each winner reconstructs his share of the contract from sub-shares obtained from each of the bidders using

the principles of rational secret reconstruction. This share is meaningless until it is used to reconstruct the contract along with the seller's share. Therefore, at the end, each winner has a contract and the seller also has a contract corresponding to each winner. The main idea is that the contract and the information in the contract are obtained simultaneously. If a party aborts the protocol at any stage before the last, it has to forgo both the contract and the information. Therefore we allow abort. This takes into account technical failures, such as, problems in network connectivity while the transaction occurs. But it ensures that no party (neither the seller nor the rational players nor the rational adversary) interested in the result of the auction intentionally aborts at any stage. Our protocol is thus the real world implementation of an ideal world that allows abort but not reject. Each players share is signed with information theoretic MAC so that a player cannot send a false share undetected. So, in each round, a player can either send the designated share or keep silent.

Choice of β. Following the general method of rational secret reconstruction [4, 5, 7, 9] the contract can be reconstructed only at a randomly chosen epoch so that it is possible to correctly guess the contract revelation round with a probability of β. Since there are three types of players (rational adversary, rational participant and seller), the choice of β must be made depending on the utility of obtaining the contract alone for each. When the rational adversary wins and obtains the contract alone, it need not buy the item it won and hence its overall utility is $u_A = u_A^I = p_A$ where p_A is its valuation of the information in the contract. When the rational participant wins and obtains the contract alone, its overall utility is $u_R = u_R^I + u_R^{auc} = p_R + v_w$. Note that the rational player does not pay the winning price p_w for the item. When the seller obtains the contract alone, its overall utility for each winner is $u_S = u_S^{auc} = p_w + v_S$ where v_S is the sellers personal valuation of the item he is selling (it is most likely that $v_S \leq p_w$). Therefore, β must be chosen such that $\beta.Max(\alpha_A p_A, \alpha_R(p_R + v_w), p_w + v_S) < Min(\alpha_A(p_A - p_w), \alpha_R(p_R + v_w - p_w), p_w)$ where the RHS denotes the minimum of the utilities when not deviating and α_A and α_R denote the probabilities that the rational adversary wins and the rational player wins respectively. We assume here that the protocol designer has an idea about the winning price of the item on auction.

3.1 Our Protocol

The Mediated Setting without Abort and without Reject. Let $C_{med}^{non-adv}$ be the communication device that also acts as the mediator.
Input: Obtain as input the bid b_i from each bidder P_i and the identity sel_{id} from the seller S.
Compute result: Compute $(o_1, \ldots, o_n) = Mec(b)$.
Send contract: Each bidder P_i is given its contract o_i and the seller S is given a copy of the contract for each P_i. The recommended strategy $\pi_{med}^{non-adv}$ for each bidder P_i is to input a bid $b_i \leftarrow B_i(t_i)$ and for the seller is to input the correct sel_{id}.

We next consider mediation with abort to account for undesired protocol abortion by rational parties/adversaries.

The Mediated Setting with Abort and without Reject. Here we want to have a protocol that is secure against following deviations. First, privacy conscious rational parties may abort at appropriate points in the protocol so as to prevent other parties from receiving their contract and hence any information about types of the aborting parties. Secondly, the rational adversary is only interested in the information about the winner. So, it may prevent the seller from receiving his contract and other parties from receiving their outputs. Such deviations are not allowed in our protocol. Lastly, a seller may want to receive his copy of the contract alone and hence abort early. Therefore, the mediated setting only allows aborts that do not allow any of the parties or the adversary to receive any output, i.e., the ideal world allows either everybody to receive the output or nobody to receive the output. This takes into account unintentional aborts over Internet like communication medium.

Input

The input of each bidder P_j is his bid b_j and that of the seller his identity sel_{id}. The trusted mediator does the following:

Computation Phase

Computes the winning bidder using an auction mechanism Mec as $(o_1, \ldots, o_n) = Mec(b)$.

Pre-processing Phase

1. Choose an i_I^* according to a geometric distribution with parameter β.
2. For each output o_j corresponding to each party P_j do the following for $i \in 1, \ldots, m$:
   - For $i < i_I^*$, set $o_{ij}^p \leftarrow D_p$ and $o_{ij}^s \leftarrow D_s$.
   - For $i \geq i_I^*$, set $o_{ij}^p = o_i$ and $o_{ij}^s = o_i$.

Abort phase

- During any of the above phases, the trusted mediator can receive an $abort_j$ instruction from any party P_j. In that case the trusted mediator must inform all the bidders and the seller that the protocol has been aborted and then quit.

Communication Phase

- In rounds $1 \leq i \leq m$, corresponding to party P_j, send o_{ij}^p to party P_j.
- In rounds $1 \leq i \leq m$, corresponding to party P_j, send o_{ij}^s to the seller.

Each rational party P_j does the following:

- Outputs o_{ij}^p as received from the trusted mediator.
- If an abort message is received from the trusted mediator then output a special symbol denoting failed transaction and quit.

The seller does the following:

- Outputs o_{ij}^s corresponding to each party P_j as received from the trusted mediator.
- If an abort message is received from the trusted mediator, then output a special symbol denoting failed transaction and quit.

The Unmediated Setting
Functionality ShareGen
Input
Each bidder P_j inputs his bid b_j and the seller his identity sel_{id}.
Computation Phase
Computes the winning bidder using an auction mechanism Mec as $(o_1, \ldots, o_n) = Mec(b)$.
Pre-processing Phase I

1. Choose an i_I^* according to a geometric distribution with parameter β.
2. For each output o_j corresponding to each party P_j do the following for $i \in 1, \ldots, m$:
   - For $i < i_I^*$, set $o_{ij}^p \leftarrow D_p$ and $o_{ij}^s \leftarrow D_s$.
   - For $i \geq i_I^*$, set $o_{ij}^p = o_i$ and $o_{ij}^s = o_i$.
3. Set A_{ij}^p and B_{ij}^p to be the random shares of o_{ij}^p and A_{ij}^s and B_{ij}^s to be the random shares of o_{ij}^s.

Pre-processing Phase II

1. Choose an i_{II}^* according to a geometric distribution with parameter β.
2. For each share A_{ij}^p corresponding to each party P_j do the following for $i \in 1, \ldots, m$:
   - For $i < i_{II}^*$, set $a_{ij}^b \leftarrow f(x_b^{'})$ for $b \in 1, \ldots, n$ where following Shamir's secret sharing f is an $(n-1)$ degree polynomial with A_{ij}^{fake} as the free coefficient.
   - For $i \geq i_{II}^*$, set $a_{ij}^b \leftarrow f(x_b)$ for $b \in 1, \ldots, n$ where following Shamir's secret sharing f is an $(n-1)$ degree polynomial with A_{ij}^p as the free coefficient.

Output
Send shares to bidder:

- Send the shares a_{ij}^k to player P_k corresponding to the output of player P_j.
- Send the shares a_{ik}^k and B_{ik}^s to player P_k corresponding to its own output.

Send shares to seller:

- Send shares A_{ij}^s and B_{ij}^p to seller corresponding to the output of player P_j.

Protocol π_I^{auc}
Stage 1
Players use their inputs to execute a secure protocol for *ShareGen* and obtains outputs as specified by functionality *ShareGen*.
Stage 2
Using the outputs of the previous stage each player P_k does the following:

1. In round $r = i$, epoch j sends the shares a_{rj}^k to each player P_j.
2. In round $r = i$, epoch k remains silent and receives the shares a_{rk}^j from each player P_j.
3. Reconstructs all A_{rj}^p.
4. In each round $r^{'} = i$, epoch 1, each player P_k sends his share B_{rk}^s to the seller. Similarly, in each round $r^{'} = i$, epoch 2, each player P_k receives the share A_{rk}^s from the seller.
5. Reconstructs o_{ik}^p.

The seller does the following:

1. In each round $r^{'} = i$, epoch 1, the seller receives the share B_{rk}^s from P_k. Similarly, in each round $r^{'} = i$, epoch 2, the seller distributes the share A_{rk}^s to each player P_k.
2. Reconstructs o_{ik}^s for each player P_k.

Outputs
For each player P_k

- If some other party aborts before any o_{ik}^p can be reconstructed, then output a special symbol denoting failed transaction and quit.
- If the seller or some other player aborts after at least one o_{ik}^p is recontsructed, then output the last reconstructed o_{ij}^p.

For the seller

- If a bidder aborts before any o_{ik}^s can be reconstructed, then output a special symbol denoting failed transaction and quit.
- If the bidder P_k aborts after at least one o_{ik}^s can be reconstructed, then output the last reconstructed o_{ik}^s.

3.2 Analysis

Theorem 1. *Protocol* π_I^{auc} *is computationally secure.*

Proof. We shall prove that our auction protocol π_I^{auc} is computationally secure (according to Definition 3) in three steps. First, we show for rational adversaries, $b_A < u_A^I$. Next we show that for sellers it is always beneficial to participate in the protocol. Lastly, we show that for each participant (rational adversary/ rational player/ seller) it is in computational strict Nash Equilibrium to follow the protocol.

In our protocol π_I^{auc}, each winner and the seller obtains a contract at the end of the protocol. No information related to the contract is released in any intermediate step. Also, the contracts are enforced causing each winner to pay for the item it has won. For a first price auction where a winner has to pay an amount equal to its bid value for the item it won, the rational adversary can only bid an amount less than its valuation of the information gained from the contract in order to gain a positive utility, if it wins, by participating in the protocol. So, for a first price auction, $b_A < u_A^I$. For a second price auction, the rational adversary's overall utility gain from the auction i.e. u_A will depend on the second highest bid value. However, this is not known to the rational adversary. For it to be beneficial for the rational adversary to participate in the auction, $(u_A^I - p) > 0$. But, since p is unknown beforehand, the rational adversary's overall utility from participating in the auction (u_A) is less than 0 whenever $u_A^I \leq p$. So participation in the auction does not guarantee a positive utility. On the other hand if the rational adversary bids $b_A \leq u_A^I$ then 1) if it does not win then $u_A = 0$ and 2) if it wins then $u_A > 0$ since $p < u_A^I$. So the rational adversary finds it beneficial to bid a value less than u_A^I. Since contracts are enforced, a winner always pays for the items it wins. Therefore the seller always has a utility $u_S(\sigma_s) > 0$ so that it is beneficial to participate in the protocol. In each round, each participant can either send the designated message or keep silent. Since messages are signed by information theoretic MACs, a participant cannot send a false message undetected. Now suppose a participant quits at the qth round. For a rational adversary or a rational player to benefit from quitting in this round: 1) it must have won the auction and 2) this is the round where the contract is reconstructed. With probability β, this is the round where the participant wins and the contract is revealed whereas with probability $(1-\beta)$ it is not so. Then expected utility of a rational adversary on quitting in round q is βu_A^I. But, by our choice, $\beta p_A < \alpha_A(p_A - p_w)$ where p_A is the rational adversary's valuation of the information in the contract, p_w is the winning price of the item and α_A is the probability that the rational adversary wins the auction. Therefore, it is in computational strict Nash Equilibrium for a rational adversary to follow the protocol. Similarly we can show that for rational parties and the seller, it is in computational strict Nash Equilibrium to follow the protocol.

4 Conclusion

We introduce a new problem scenario for online auctions where rational adversaries 'throw away' the contracts they win because they only value the information in the contract but do not want to buy the item they won. Other participants in such an auction scenario are referred to as rational players who buy the item if they win but are selfish and privacy-conscious. The seller can also misbehave by trying to obtain the legal contract alone and then exercising it. We propose a new auction protocol that is computationally secure in this scenario.

Acknowledgement. We would like to thank the anonymous reviewers for their useful comments and suggestions that helped us improve our work.

References

1. Bogetoft, P., Damgård, I.B., Jakobsen, T., Nielsen, K., Pagter, J.I., Toft, T.: A practical implementation of secure auctions based on multiparty integer computation. In: Di Crescenzo, G., Rubin, A. (eds.) FC 2006. LNCS, vol. 4107, pp. 142–147. Springer, Heidelberg (2006)
2. Bradford, P.G., Park, S., Rothkopf, M.H., Park, H.: Protocol completion incen-tive problems in cryptographic Vickrey auctions. Electronic Commerce Research 8(1-2), 57–77 (2008)
3. Franklin, M.K., Reiter, M.K.: The design and implementation of a secure auction service. IEEE Transactions on Software Engineering 22(5), 302–312 (1996)
4. Fuchsbauer, G., Katz, J., Naccache, D.: Efficient rational secret sharing in standard communication networks. In: Micciancio, D. (ed.) TCC 2010. LNCS, vol. 5978, pp. 419–436. Springer, Heidelberg (2010)
5. Gordon, S.D., Katz, J.: Rational Secret Sharing, Revisited. In: De Prisco, R., Yung, M. (eds.) SCN 2006. LNCS, vol. 4116, pp. 229–241. Springer, Heidelberg (2006)
6. Groce, A., Katz, J., Thiruvengadam, A., Zikas, V.: Byzantine agreement with a rational adversary. In: Czumaj, A., Mehlhorn, K., Pitts, A., Wattenhofer, R. (eds.) ICALP 2012, Part II. LNCS, vol. 7392, pp. 561–572. Springer, Heidelberg (2012)
7. Halpern, J., Teague, V.: Rational secret sharing and multiparty computation: extended abstract. In: Proceedings of the Thirty-Sixth Annual ACM Symposium on Theory of Computing, STOC 2004, pp. 623–632. ACM, New York (2004)
8. Juels, A., Szydlo, M.: A two-server, sealed-bid auction protocol. In: Blaze, M. (ed.) FC 2002. LNCS, vol. 2357, pp. 72–86. Springer, Heidelberg (2003)
9. Kol, G., Naor, M.: Games for exchanging information. In: Proceedings of the 40th Annual ACM Symposium on Theory of Computing, STOC 2008, pp. 423–432. ACM, New York (2008)
10. Miltersen, P.B., Nielsen, J.B., Triandopoulos, N.: Privacy-enhancing auctions using rational cryptography. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 541–558. Springer, Heidelberg (2009)
11. Naor, M., Pinkas, B., Sumner, R.: Privacy preserving auctions and mechanism design. In: Proceedings of the 1st ACM Conference on Electronic Commerce, pp. 129–139. ACM (November 1999)
12. Parkes, D.C., Rabin, M.O., Thorpe, C.: Cryptographic combinatorial clock-proxy auctions. In: Dingledine, R., Golle, P. (eds.) FC 2009. LNCS, vol. 5628, pp. 305–324. Springer, Heidelberg (2009)
13. Suzuki, K., Yokoo, M.: Secure generalized Vickrey auction using homomorphic encryption. In: Wright, R.N. (ed.) FC 2003. LNCS, vol. 2742, pp. 239–249. Springer, Heidelberg (2003)