A Truthful, Privacy-Preserving, Approximately Efficient Combinatorial Auction For Single-minded Bidders

Extended Abstract

Sankarshan Damle
International Institute of Information Technology (IIIT)
Hyderabad, India
sankarshan.damle@research.iiit.ac.in

Boi Faltings
Ecole Polytechnique Fedeŕalé de Lausanne (EPFL)
Lausanne, Switzerland
boi.faltings@epfl.ch

Sujit Gujar
International Institute of Information Technology (IIIT)
Hyderabad, India
sujit.gujar@iiit.ac.in

ABSTRACT

Combinatorial auctions are widely used to sell resources/items. The challenges in such auctions are multi-fold. We need to ensure that bidders, the strategic agents, bid their valuations truthfully to the auction mechanism. Besides, the agents may desire privacy of their identities as well as their bidding information. We consider three types of privacies: agent privacy, the identities of the losing bidders must not be revealed to any other agent except the auctioneer (AU), bid privacy, the bid values must be hidden from the other agents as well as the AU and bid-topology privacy, the items for which the agents are bidding must be hidden from the other agents as well as the AU. In this paper, we address whether can we solve the allocation and payment determination problems, which are NP-hard, approximately for single-minded bidders while preserving privacy. In the literature, $\sqrt{m}$-approximation, where m is the number of items auctioned, and a strategy-proof mechanism is available for this, which we refer to as ICA-SM. To implement ICA-SM with privacy, we propose a novel cryptographic protocol TPACAS. We show that TPACAS achieves these privacy guarantees with high probability. To accomplish this, we use notaries who are semi-trusted third parties. We show that, in TPACAS, notaries do not learn any information about the agents and their bidding information.

KEYWORDS

Combinatorial Auctions; Privacy and Security; Truthful Mechanism Design

ACM Reference Format:
Sankarshan Damle, Boi Faltings, and Sujit Gujar. 2019. A Truthful, Privacy-Preserving, Approximately Efficient Combinatorial Auction For Single-minded Bidders. In *Proc. of the 18th International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2019), Montreal, Canada, May 13–17, 2019,* IFAAMAS, 3 pages.

1 INTRODUCTION

Auctions are mechanisms which facilitate the buying and selling of goods/items amongst a group of agents. In general, a combinatorial auction, where the agents can bid for combination(s) of items, yields a higher revenue than selling the goods/items individually. For example, different governments across the globe use combinatorial auctions to lease out wireless spectrum [7] or allocate airport landing take-off slots to interested agents [11].

Using auctions directly is a security risk on each agent's bid and its combination of items. Disclosure of an agent's public identity reveals its interest in acquiring the items auctioned. The revelation of an agent's *bidding information* (bid value and the combination of preferred items) to an auctioneer or other participating agents may expose its profits, economic situations and preferences for specific items to its contemporaries. An auctioneer (AU) may further exploit this information in future auctions. In consequence, an auction protocol should be such that only the winning agents' combination of preferred items is made public while preserving the privacy of the identities and the bidding information of the other agents.

Auction protocols which preserve the privacy of bidding information are called *secure auction* protocols. In this paper we define these desirable privacies of a secure auction in three types [4]: (i) *Agent privacy*, an agent's participation in an auction must be hidden from all the other agents; (ii) *bid privacy*, the bid values must be hidden from the other agents as well as the auctioneer; and (iii) *bid-topology privacy*, the items for which the agents are bidding must be hidden from the other agents as well as the auctioneer.

Furthermore, if the bidding information is hidden from the agents as well as the auctioneer, we need a *trustworthy* implementation of a secure auction. That is, anybody should be able to verify the correctness of the allocations and that the payments are in alignment with the described rules. Besides, the implementation must preserve all the three types of privacies with high probability. Motivated by these challenges, our focus in this paper is on the preservation of privacy of all agents' bidding information in an instance of a combinatorial auction.

Typically, the goal in such auctions is to maximize the social welfare, i.e., to allocate these resources to those who value them most. Strategic agents may misreport their valuations to maximize their profits. Thus, we look for auctions which, through appropriate payment rules, ensure that the agents bid their true valuation. In game theory, such auction protocols (allocation rule along with payment rule) are called *dominant strategy incentive compatible* (DSIC). In addition to this, auction protocols must also be *individually rational* (IR) i.e., protocols wherein the agents have a non-negative payoff.

Combinatorial auctions have an exponential number of possible valuations for each agent and are NP-Complete [12]. Hence, we focus on a *single-minded* case. In this, the agents are interested in a single specific bundle of items and obtain a particular value if

Proc. of the 18th International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2019), N. Agmon, M. E. Taylor, E. Elkind, M. Veloso (eds.), May 13–17, 2019, Montreal, Canada.

they get the whole bundle (or any superset) and zero otherwise. Even single-minded combinatorial auctions, being NP-Hard [13], are solved approximately. In particular, Lehmann et al. [5] proposes a strategic proof mechanism for such auctions, which gives $\sqrt{m}$-approximate allocation and payment rule, which we refer to as ICA-SM (Incentive Compatible Approximate auctions for Single-minded bidders), given in Algorithm 1. In this paper, we propose TPACAS (Truthful, Privacy-preserving, an Approximately efficient Combinatorial auction for Single-minded bidders), which solves a single-minded combinatorial auction, preserving the cryptographic and game theoretic properties mentioned earlier i.e., TPACAS is a trustworthy implementation of ICA-SM.

Algorithm 1: ICA-SM Algorithm

```
Notations: Let $B = \{b_1, \ldots, b_{\hat{n}}\}$ be the set of agents with $\vartheta_{b_i}$ as their
           bid valuation, $S_{b_i}$ as their preferred bundle of items and $\sigma_{b_i}$
           as their payment. Here, $W$ is the set of winners.
    (1) Initialization:
        • Sort the agents according to the order :
          $\vartheta^*_{b_1} / \sqrt{|S^*_{b_1}|} \geq \vartheta^*_{b_2} / \sqrt{|S^*_{b_2}|} \geq \cdots \geq \vartheta^*_{b_{\hat{n}}} / \sqrt{|S^*_{b_{\hat{n}}}|}$
        • $W \leftarrow \emptyset$
    (2) For $i : 1 \longrightarrow \hat{n}$, if $S^*_{b_i} \cap (\cup_{b_j \in W} S^*_{b_j}) = \emptyset$ then $W \leftarrow W \cup \{b_i\}$
    (3) Output:
        • Allocation: The set of winners is $W$.
        • Payments: $\forall b_i \in W, \sigma_{b_i} = \vartheta^*_{b_j} / \sqrt{|S^*_{b_j}| / |S^*_{b_i}|}$ where $j$ is the
          smallest index such that $S^*_{b_i} \cap S^*_{b_j} \neq \emptyset$, and for all $k < j$,
          $b_k \neq b_i, S^*_{b_k} \cap S^*_{b_j} = \emptyset$. If no such $j$ exists then $\sigma_{b_i} = 0$.
```

Related Work. Our work is closely related to [8] and [9]. Micali and Rabin [8] use *homomorphic* property of commitments while Parkes et al. [9] also uses *time-lapse cryptography* to achieve winner determination while preserving the privacy of the agents and their bidding information. However, these protocols expose the bidding information to the auctioneer after the bidding phase is over. We overcome these issues by proposing the use of *notaries*. We assume there are approved cryptographic notaries in the system and the auctioneer can appoint them in assisting in the auction. In TPACAS, the auctioneer assigns a signed random *id* for each agent and a set of randomly chosen notaries. The agents commit their bid values and the size of the bundle in which they are interested similar to [8]. The challenge remains to sort the bids or to check if two agents have any item in common while keeping the values and bid-topology private. In the literature, this challenge is similar to Yao's Millionaires' problem [14] of securely determining the richer among two different parties and has been extensively studied.

The first solution to the problem, Yao [14], needs exponential time and space. Thereafter, several protocols with great improvement have been proposed [1, 2, 6]. However, each comparison through these protocols is at best linear in order of the length of the binary representation of these numbers and may also involve multiple rounds of computation. This makes the process computationally expensive for applications such as auctions. Further, these protocols require the continuous involvement of agents which is not desirable.

2 TPACAS PROTOCOL

TPACAS uses the ICA-SM algorithm to solve a single-minded combinatorial auction. To provide the cryptographic properties, we require the agents to encrypt their bidding information, towards which we make use of Pedersen commitment [10]. Notaries are used as semi-trusted third parties to act as a communication link between the agents and AU.

Secure Comparison of Two Integers. To securely sort the agents as well as compare their item bundles, we introduce a method for comparing two integers x and y securely. For this, we require $x, y < q/2$ where q is a large prime. Procedure 1 describes the method. We achieve secure comparison in constant time and in one execution of Procedure 1. For the comparison, we make use of notaries which are semi-trusted third parties. We show that notaries do not learn any information about the values, x and y. Further, we make use of the Pedersen commitments of each agent's bidding information to provide zero-knowledge proofs for the verifiability of the winner and payment determination. The proofs are presented in the complete version of the paper.

Procedure 1: *Compare*$\big(b_i, E(R(x)), b_j, E(R(y))\big)$

```
Notations: Procedure for the secure comparison of two values $x$ and $y$,
           of agents $b_i$ and $b_j$ for $R(x) = (u_i, v_i)$ where
           $x = (u_i + v_i) \bmod q$ and $R(y) = (u_j, v_j)$ where
           $y = (u_j + v_j) \bmod q$, with $E(R(x))$ and $E(R(y))$ as their pair
           of Pedersen commitments. For this, let $(n^1_{b_i}, n^2_{b_i})$ and
           $(n^1_{b_j}, n^2_{b_j})$ be the notaries assigned to $b_i$ and $b_j$, respectively.
    Input: The pair of encryptions given by $E(R(x))$ and $E(R(y))$.
   Output: $x \overset{?}{\geq} y$
           Steps
       (1) AU asks the assigned notaries to exchange amongst each
           other the values for the commitments for
           $E(R(x)) = \big(E(u_i), E(v_i)\big)$ and $E(R(y)) = \big(E(u_j), E(v_j)\big)$ in
           the following manner: $n^1_{id_{b_i}}$ receives the value $u_j$ from $n^1_{b_j}$
           and $n^2_{b_i}$ receives the value $v_j$ from $n^2_{b_j}$ securely [3, 15].
       (2) $n^1_{b_i}$ calculates $(u_i - u_j) \bmod q$ as $val_1$ and $n^2_{b_i}$ calculates
           $(v_i - v_j) \bmod q$ as $val_2$.
       (3) $n^1_{b_i}$ sends $val_1$ and $n^2_{b_i}$ sends $val_2$ to the AU, securely.
       (4) AU then checks the following,
           if $(val_1 + val_2)$ mod $q = 0$ return “equal"
           if $(val_1 + val_2)$ mod $q < q/2$ return “>"
           else return “<"
```

THEOREM. *TPACAS is a trustworthy implementation of ICA-SM.*

Discussion. We show that TPACAS preserves agent, bid and bid-topology privacy with high probability – the probability of guessing improves only by $O\left(\frac{1}{2^m}\right)$ – and is non-repudiate and verifiable. Since the protocol also solves the winner and payment determination problem through ICA-SM, it is DSIC and ex-post IR. Thus, TPACAS is a trustworthy implementation of ICA-SM. □

REFERENCES

[1] Ian F Blake and Vladimir Kolesnikov. 2004. Strong conditional oblivious transfer and computing on intervals. In *International Conference on the Theory and Application of Cryptology and Information Security*. Springer, 515–529.

[2] Ivan Damgård, Matthias Fitzi, Eike Kiltz, Jesper Buus Nielsen, and Tomas Toft. 2006. Unconditionally secure constant-rounds multi-party computation for equality, comparison, bits and exponentiation. In *Theory of Cryptography Conference*. Springer, 285–304.

[3] Roger Dingledine, Nick Mathewson, and Paul Syverson. 2004. *Tor: The second-generation onion router.* Technical Report. Naval Research Lab Washington DC.

[4] Thomas Léauté and Boi Faltings. 2013. Protecting privacy through distributed computation in multi-agent decision making. *Journal of Artificial Intelligence Research* 47 (2013), 649–695.

[5] Daniel Lehmann, Liadan Ita Oćallaghan, and Yoav Shoham. 2002. Truth revelation in approximately efficient combinatorial auctions. *Journal of the ACM (JACM)* 49, 5 (2002), 577–602.

[6] Hsiao-Ying Lin and Wen-Guey Tzeng. 2005. An efficient solution to the millionairesâĂŹ problem based on homomorphic encryption. In *International Conference on Applied Cryptography and Network Security*. Springer, 456–466.

[7] John McMillan. 1994. Selling spectrum rights. *Journal of Economic Perspectives* 8, 3 (1994), 145–162.

[8] Silvio Micali and Michael O Rabin. 2014. Cryptography miracles, secure auctions, matching problem verification. *Commun. ACM* 57, 2 (2014), 85–93.

[9] David C Parkes, Michael O Rabin, Stuart M Shieber, and Christopher Thorpe. 2008. Practical secrecy-preserving, verifiably correct and trustworthy auctions. *Electronic Commerce Research and Applications* 7, 3 (2008), 294–312.

[10] Torben Pryds Pedersen. 1991. Non-interactive and information-theoretic secure verifiable secret sharing. In *Annual International Cryptology Conference*. Springer, 129–140.

[11] Stephen J Rassenti, Vernon L Smith, and Robert L Bulfin. 1982. A combinatorial auction mechanism for airport time slot allocation. *The Bell Journal of Economics* (1982), 402–417.

[12] Michael H Rothkopf, Aleksandar Pekeč, and Ronald M Harstad. 1998. Computationally manageable combinational auctions. *Management science* 44, 8 (1998), 1131–1147.

[13] Tuomas Sandholm. 1999. An algorithm for optimal winner determination in combinatorial auctions. (1999).

[14] Andrew C Yao. 1982. Protocols for secure computations. In *Foundations of Computer Science, 1982. SFCS'08. 23rd Annual Symposium on*. IEEE, 160–164.

[15] Tatu Ylonen. 1996. SSH–secure login connections over the Internet. In *Proceedings of the 6th USENIX Security Symposium*, Vol. 37.