PANDA: Privacy-Aware Double Auction for Divisible Resources without a Mediator*

Extended Abstract

Bingyu Liu
Illinois Institute of Technology
Chicago, Illinois
bliu40@hawk.iit.edu

Shangyu Xie
Illinois Institute of Technology
Chicago, Illinois
sxie14@hawk.iit.edu

Yuan Hong
Illinois Institute of Technology
Chicago, Illinois
yuan.hong@iit.edu

ABSTRACT

Auction mechanism generally requires a trusted-third party as the market mediator to coordinate bidding and resource allocation via collecting private data from the agents, which may arouse severe privacy concerns and high computation overheads. To address such issues, we propose a novel privacy-aware double auction framework (namely PANDA) by designing an efficient cryptographic protocol to privately execute double auction for divisible resources among all the agents. To ensure privacy and truthfulness, PANDA delicately co-designs VCG auction and cryptographic protocol, which is equivalent to a mediator for sealed-bid auction of divisible resources.

KEYWORDS

Multi-agent System; Secure Computation; Resource Allocation;

ACM Reference Format:


1 INTRODUCTION

In the past decade, divisible resources have been frequently exchanged in the electricity markets (e.g., electricity [1, 7, 17, 19]), cloud markets (e.g., computation and storage resources [21]), financial markets (e.g., stock shares [13]), wireless networks (e.g., bandwidth [3]), among others. In such markets, each agent may sell resources with arbitrary amounts to any other buyers, and all the agents generally compete with each other by seeking for their aggregated valuation if such agent is in the auction [22]. We also denote the payoff function for buyer \( m \) as \( V_m(A_m) \) with its amount to buy \( A_m \) and the cost function of each seller \( n \) as \( C_n(A_n) \) with its amount to sell \( A_n \). Moreover, the valuation function \( V_m \) follows a generic setting \([11, 16]\): (1) \( V_m \) is differentiable and \( V_m(0) = 0 \), and (2) \( V_m \) is non-increasing and continuous.

We also denote the payoff function for buyer \( m \) and seller \( n \) as \( f_m(r) \) and \( f_n(r) \), respectively. In a VCG mechanism \([11, 16]\), transfer payment is defined as the difference between all the agents’ aggregated valuation if any agent is not in the auction minus the aggregated valuation if such agent is in the auction \([22]\). We denote the transfer payments for buyer \( m \) and seller \( n \) as \( \rho_m(r) \) and \( \rho_n(r) \), where \( r \) is the set of bid profiles. Thus, we have:

\[
\rho_m(r) = \sum_{n \in A_m} \alpha_m[A_m(0; r_{-i}) - A_m(r_j; r_{-j})] \tag{1}
\]

\[
\rho_n(r) = \sum_{m \in A_n} \beta_n[A_n(0; r_{-j}) - A_n(r_j; r_{-j})] \tag{2}
\]

If directly eliminating the mediator in the auction, severe privacy concerns may occur since all the agents should disclose their local private data for completing the auction. In addition, some agents may try to win more payoffs in the auction by reporting untruthful bids, especially in sealed-bid auctions [9]. Even worse, agents (aka. potential buyers or sellers) may collect such information from their competitors [18], and misuse such private data, e.g., reselling the data (a mediator may also do so).

In this paper, we propose a novel auction framework (namely PANDA) by designing an efficient cryptographic protocol among all the buyers and sellers to privately execute double auction for divisible resources. Specifically, we construct the cryptographic protocol with the fundamental cryptographic primitives: Homomorphic Encryption (HE) [4, 14] and Secure Function Evaluation (SFE) [5]. Then, the cryptographic protocol enables all the agents to securely communicate with each other and complete the transactions with limited information disclosure. Per the secure multiparty computation (MPC) theory \([6, 20]\), the cryptographic protocol can be proven to be equivalent to a mediator. Furthermore, we design a double auction \([22]\) based on the Vickrey-Clarke-Groves (VCG) \([11, 16]\) mechanism in PANDA to ensure truthfulness.


\*This work is partially supported by the National Science Foundation (NSF) under Grant No. CNS-1745894

Then, given the optimal allocation profile for buyers/sellers $A_m^*(r), A_n^*(r)$, we can get the payoff of the buyer/seller:

$$f_m(r) = \tilde{V}_m(A_m^*(r)) - \rho_m(r), \forall m \in B$$  \hspace{1cm} (3)

$$f_n(r) = -\tilde{C}_n(A_n^*(r)) - \rho_n(r), \forall n \in S$$  \hspace{1cm} (4)

**Definition 2.1 (Nash Equilibrium in PANDA).** Given the bid profiles $r$, a Nash Equilibrium $NE$ holds such that:

$$\forall m \in B, f_m(b_m^*, r_{-m}) \geq f_m(b_m, r_{-m})$$

$$\forall n \in S, f_n(s_n^*, r_{-n}) \geq f_n(s_n, r_{-n})$$

### 3 PRIVACY-AWARE DOUBLE AUCTION
#### 3.1 Overview of Framework

The proposed protocol ensures that all the bid profiles are encrypted and privately computed in multiple iterations to achieve the best responses for the Nash Equilibrium (NE). Figure 1 shows the major steps of the PANDA framework. In the initialization of each auction, PANDA first executes **Init()** to privately derive an initial bid profile while ensuring valid conditions for the auction via secure function evaluation (SFE) and **Aggre()**. Then, **IterUpdate()** is executed to privately update the potential amount and **BestRespon()** is sequentially executed to privately compute the best response in each (current) iteration $k$. Finally, the auction reaches Nash Equilibrium after iteratively updating the potential amount and the best response. The details of each algorithm will be illustrated in the following section.

**Figure 1: PANDA Framework**

**Properties of PANDA.** First, PANDA inherits the properties of auction [15], i.e., budget balance, Pareto efficiency, and existence of NE. Our proposed framework works under semi-honest model that may curiously infer others’ private information. [6, 20]). While addressing the above threats, PANDA has the following properties:

1. **Decentralized**: no central market mediator or operator to coordinate agents to finish the auction.
2. **Privacy**: each agent’s bid profile (the bid price and amount) is kept private; every pair of potential buyer and seller only know the amount in their transaction (and the clearing price).
3. **Truthfulness**: each agent truthfully participates in the auction would gain more payoff than the untruthful.

#### 3.2 Algorithms

**3.2.1 Init().** PANDA first executes **Init()** to privately generate valid initial conditions. Specifically, secure function evaluation (SFE) is executed to privately ensure $(\sigma_m)_{max} < \{\beta_m\}_{min}$: such bid profiles would result in a valid auction (if not evaluated to be true, then all the agents execute it again). This step also calls another algorithm **Aggre()**, which is used to securely sum up the amounts of all the buyers and sellers. **Aggre()** mainly uses the additive property of Homomorphic Cryptosystem for the aggregation. Thus, the potential amount $C$ (the common amount allocated in each side of the double auction) can also be determined. Note that $C$ is initialized before the auction is smaller than the total amounts. The auction moves to the next step once meeting the initial constraints.

**3.2.2 IterUpdate().** It privately updates the potential amount as $\overline{C}(r, C)$ with the following equation:

$$\overline{C}(r, C) = Q(r, C) + \frac{p_k(r, C) - p_l(r, C)}{\omega_{max} + \sigma_{max}}$$

$\omega_{max}$ and $\sigma_{max}$ are denoted as the upper bound of the gradients. With the gradients of buyers’ marginal valuations and sellers’ marginal costs, the potential amount can reach the NE more efficiently. The minimum aggregated amounts of buyers and sellers $Q(r, C)$ can be obtained by SFE. It is assumed that the matched prices $p_k(r, C) = \min(a_i, A_i \geq 0)$ and $p_l(r, C) = \max(b_j, A_j \geq 0)$ can be known to the other agents. Note that $\omega_{max} + \sigma_{max}$ is a private coefficient for the gradients of marginal valuations (costs). Then, in iteration $k$, each agent locally updates the best response w.r.t. the bid profile of the others, and then jointly finds the optimal allocation using the SFE as below:

$$A_m^*(b, C) = \min\{d_m, \max\{C - \sum_{i \in T_m} d_i, 0\}\}$$

$$A_n^*(s, C) = \min\{h_n, \max\{0, C - \sum_{j \in T_n} h_j\}\}$$

where $T_m = \{i \in M; s.t. \ a_i > a_m\} \cup \{a_i = a_m \land i < m\}$ and $T_n(s) = \{j \in N; s.t. \ b_j > b_n\} \cup \{b_j = b_m \land j < n\}$.

**3.2.3 BestRespon().** It is executed to derive the best response for buyer $m \in B$ and seller $n \in S$ (denoted as $b^*_m$ and $s^*_n$ respectively). Then, we can calculate the optimal profiles:

$$b^*_m = \arg \max \{f_m(b_m, b_m - m)\}$$

$$s^*_n = \arg \max \{f_n(s_n, s_n - n)\}$$

Recall that **IterUpdate()** iteratively returns the optimal allocation with SFE for every buyer/seller, then PANDA finally converges in the auction with the best responses of all the agents under Nash Equilibrium (NE). The matched prices from buyers and sellers eventually coverage to the clearing price.

### 4 CONCLUSION

In this paper, we have proposed a novel framework PANDA that securely executes double auction for divisible resources by integrating the VCG mechanism and cryptographic protocol, which is equivalent to a market mediator. PANDA ensures privacy and truthfulness in the distributed computation among all the agents.
REFERENCES


