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:
Bingyu Liu, Shangyu Xie, and Yuan Hong. 2020. PANDA: Privacy-Aware Double Auction for Divisible Resources without a Mediator. In *Proc. of the 19th International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2020), Auckland, New Zealand, May 9–13, 2020,* IFAAMAS, 3 pages.

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 maximum payoffs. Then, auction mechanisms have been extensively studied for exchanging such divisible resources to achieve the Nash Equilibrium [8, 12]. Since auctions request all the potential buyers to propose bid prices [2, 8] (in particular, double auction [10] requests both potential buyers and sellers to simultaneously submit their prices), a trusted-third party is established as the *market mediator* to coordinate the bidding and resource allocation in the auctions. The establishment of the mediator may result in high operational costs, extra charges to buyers/sellers, high computation burden, and high demand of trust on the mediator.

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

Proc. of the 19th International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2020), B. An, N. Yorke-Smith, A. El Fallah Seghrouchni, G. Sukthankar (eds.), May 9–13, 2020, Auckland, New Zealand.

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.

2 DOUBLE AUCTION

We denote a set of buyers as $\mathcal{B}$ and sellers as $\mathcal{S}$ in the auction, where each buyer/seller submits a two-dimensional bid profile (bid price, and the maximum amount to buy/sell) as follows: 1) buyer $m \in \mathcal{B}$: $b_m = (\alpha_m, d_m)$, and 2) seller $n \in \mathcal{S}$: $s_n = (\beta_n, h_n)$. Aslo, we denote the valuation function of each buyer m as $\widehat{V}_m(A_m)$ with its amount to buy A_m and the cost function of each seller n as $\widehat{C}_n(A_n)$ with its amount to sell A_n. Moreover, the valuation function $\widehat{V}_m$ follows a generic setting [11, 16]: (1) $\widehat{V}_m$ is differentiable and $\widehat{V}_m(0) = 0$, and (2) $\widehat{V}'_m$ 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:

$$\rho_m(r) = \sum_{m \neq i} \alpha_m [A_m(0; r_{-i}) - A_m(r_i; r_{-i})] \tag{1}$$

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

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

$$f_m(r) = \widehat{V}_m(A^*_m(r)) - \rho_m(r), \forall m \in \mathcal{B} \tag{3}$$

$$f_n(r) = -\widehat{C}_n(A^*_n(r)) - \rho_n(r), \forall n \in \mathcal{S} \tag{4}$$

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

$$\forall m \in \mathcal{B}, f_m(b^*_m, r^*_{-m}) \geq f_m(b_m, r^*_{-m}) \tag{5}$$

$$\forall n \in \mathcal{S}, f_n(s^*_n, r^*_{-n}) \geq f_n(s_n, r^*_{-n}) \tag{6}$$

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 C 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.

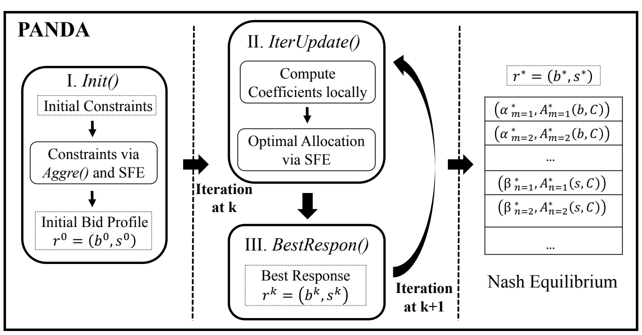

Figure 1: PANDA Framework

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 all the agents follow the protocol but may curious to 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 response.

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 $\{\alpha_m\}_{max} < \{\beta_n\}_{min}$: 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 (which 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 $\widetilde{C}(r, C)$ with the following equation:

$$\widetilde{C}(r, C) = Q(r, C) + \frac{p_b(r, C) - p_s(r, C)}{\omega_{max} + \sigma_{max}} \tag{7}$$

ω_{max} and σ_{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 $p_b(r, C) = \min\{\alpha_i, A_i \geq 0\}$ and $p_s(r, C) = \max\{\beta_j, A_j \geq 0\}$ can be known to the other agents. Note that $\frac{p_b(r,C) - p_s(r,C)}{\omega_{max} + \sigma_{max}}$ 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:

$$A^*_m(b, C) = \min\{d_m, \max\{[C - \sum_{i \in \mathcal{T}_m} d_i], 0\}\} \tag{8}$$

$$A^*_n(s, C) = \min\{h_n, \max\{0, [C - \sum_{j \in \mathcal{T}_n} h_j]\}\} \tag{9}$$

where $\mathcal{T}_m = \{i \in M; s.t.\ \alpha_i > \alpha_m\} \cup \{\alpha_i = \alpha_n \wedge i < m\}$ and $\mathcal{T}_n(s) = \{j \in N; s.t.\ \beta_j > \beta_n\} \cup \{\beta_i = \beta_m \wedge j < n\}$.

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

$$b^*_m = \arg\max\{f_m(b_m, b_{-m})\} \tag{10}$$

$$s^*_n = \arg\max\{f_n(s_n, s_{-n})\} \tag{11}$$

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

[1] Dou An, Qingyu Yang, Wei Yu, Xinyu Yang, Xinwen Fu, and Wei Zhao. 2018. SODA: Strategy-Proof Online Double Auction Scheme for Multimicrogrids Bidding. *IEEE Trans. Systems, Man, and Cybernetics: Systems* 48, 7 (2018), 1177–1190. https://doi.org/10.1109/TSMC.2017.2651072

[2] José R. Correa, Andreas S. Schulz, and Nicolás E. Stier Moses. 2013. The Price of Anarchy of the Proportional Allocation Mechanism Revisited. In *Web and Internet Economics - 9th International Conference, WINE 2013, Cambridge, MA, USA, December 11-14, 2013, Proceedings*. 109–120. https://doi.org/10.1007/978-3-642-45046-4_10

[3] Zhiyong Feng, Chen Qiu, Zebing Feng, Zhiqing Wei, Wei Li, and Ping Zhang. 2015. An effective approach to 5G: Wireless network virtualization. *IEEE Communications Magazine* 53, 12 (2015), 53–59.

[4] Craig Gentry. 2009. *A Fully Homomorphic Encryption Scheme*. Ph.D. Dissertation. Stanford, CA, USA. Advisor(s) Boneh, Dan. AAI3382729.

[5] Oded Goldreich. 2019. On the foundations of cryptography. In *Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali*. 411–496. https://doi.org/10.1145/3335741.3335759

[6] Oded Goldreich, Silvio Micali, and Avi Wigderson. 2019. How to play any mental game, or a completeness theorem for protocols with honest majority. In *Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali*. 307–328. https://doi.org/10.1145/3335741.3335755

[7] Yuan Hong, Han Wang, Shangyu Xie, and Bingyu Liu. 2018. Privacy Preserving and Collusion Resistant Energy Sharing. In *ICASSP*. IEEE, 6941–6945.

[8] Ramesh Johari and John N Tsitsiklis. 2004. Efficiency loss in a network resource allocation game. *Mathematics of Operations Research* 29, 3 (2004), 407–435.

[9] Vijay Krishna. 2009. *Auction theory*. Academic press.

[10] Volodymyr Kuleshov and Adrian Vetta. 2010. On the efficiency of markets with two-sided proportional allocation mechanisms. In *International Symposium on Algorithmic Game Theory*. Springer, 246–261.

[11] Aurel A Lazar and Nemo Semret. 2001. Design and analysis of the progressive second price auction for network bandwidth sharing. *Telecommunication Systems* 13 (2001).

[12] Rajiv T Maheswaran and Tamer Başar. 2003. Nash equilibrium and decentralized negotiation in auctioning divisible resources. *Group Decision and Negotiation* 12, 5 (2003), 361–395.

[13] Gregor Matvos and Amit Seru. 2014. Resource allocation within firms and financial market dislocation: Evidence from diversified conglomerates. *The Review of Financial Studies* 27, 4 (2014), 1143–1189.

[14] Tatsuaki Okamoto and Shigenori Uchiyama. 1998. A New Public-Key Cryptosystem as Secure as Factoring. In *Advances in Cryptology - EUROCRYPT '98, International Conference on the Theory and Application of Cryptographic Techniques, Espoo, Finland, May 31 - June 4, 1998, Proceeding*. 308–318. https://doi.org/10.1007/BFb0054135

[15] Simon Parsons, Juan A. Rodríguez-Aguilar, and Mark Klein. 2011. Auctions and bidding: A guide for computer scientists. *ACM Comput. Surv.* 43, 2 (2011), 10:1–10:59.

[16] Bruno Tuffin. 2002. Revisited Progressive Second Price Auction for Charging Telecommunication Networks. *Telecommunication Systems* 20, 3-4 (2002), 255–263. https://doi.org/10.1023/A:1016545228543

[17] Shangyu Xie, Yuan Hong, and Peng-Jun Wan. 2019. A Privacy Preserving Multiagent System for Load Balancing in the Smart Grid. In *AAMAS*. International Foundation for Autonomous Agents and Multiagent Systems, 2273–2275.

[18] Shangyu Xie, Yuan Hong, and Peng-Jun Wan. 2019. Pairing: Privately Balancing Multiparty Real-Time Supply and Demand on the Power Grid. *IEEE Transactions on Information Forensics and Security* 15 (2019), 1114–1127.

[19] Qingyu Yang, Dou An, Wei Yu, Xinyu Yang, and Xinwen Fu. 2015. On stochastic optimal bidding strategy for microgrids. In *34th IEEE International Performance Computing and Communications Conference, IPCCC 2015, Nanjing, China, December 14-16, 2015*. 1–8. https://doi.org/10.1109/PCCC.2015.7410289

[20] Andrew Chi-Chih Yao. 1986. How to Generate and Exchange Secrets (Extended Abstract). In *27th Annual Symposium on Foundations of Computer Science, Toronto, Canada, 27-29 October 1986*. 162–167. https://doi.org/10.1109/SFCS.1986.25

[21] Zhichao Zhao, Fei Chen, T-H Hubert Chan, and Chuan Wu. 2017. Double Auction for Resource Allocation in Cloud Computing.. In *CLOSER*. 273–280.

[22] Suli Zou, Zhongjing Ma, and Xiangdong Liu. 2018. Resource Allocation Game Under Double-Sided Auction Mechanism: Efficiency and Convergence. *IEEE Trans. Automat. Contr.* 63, 5 (2018), 1273–1287. https://doi.org/10.1109/TAC.2017.2737579