SCIENCE CHINA
Information Sciences

• LETTER •

April 2022, Vol. 65 149102:1–149102:3
https://doi.org/10.1007/s11432-019-2666-8

Constant-round auction with insulated bidders

Jie MA[1,2,3*], Bin QI[1,2,3] & Kewei LV[1,2,3*]

[1]*State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing* 100093*, China;*
[2]*Data Assurance and Communication Security Research Center, Chinese Academy of Sciences, Beijing* 100093*, China;*
[3]*School of Cyber Security, University of Chinese Academy of Sciences, Beijing* 100093*, China*

Received 12 June 2019/Revised 23 July 2019/Accepted 29 September 2019/Published online 24 May 2021

Citation Ma J, Qi B, Lv K W. Constant-round auction with insulated bidders. Sci China Inf Sci, 2022, 65(4): 149102, https://doi.org/10.1007/s11432-019-2666-8

Dear editor,

In recent years, online auction has gained widespread popularity as a primary characteristic of electronic commerce among masses. It has also become a primary topic of research interest. Cryptographic primitives such as secure multiparty computation (MPC) [1], zero-knowledge proof (ZKP) [2] and commitment scheme [3] are being effectively utilized for the proposal of various schemes. Therefore, these schemes have become much more inefficient and complicated, thereby rendering them suitable only for auction with a small number of bidders. Efficiency needs to be considered as an important factor for a real auction, especially if it is conducted online.

Considering all these observations, we present a simple and efficient auction scheme to compare all bids under ciphertexts by a three-party protocol to prevent the extraction of bid information. Each of the parties is assumed to honestly execute the protocol, although it is done with a curiosity about others' bids (semi-honest adversary). Here, we improve and run a three-party integer comparison protocol (iICP) among the auctioneer and two bidders. Only the auctioneer learns about the result of the comparison, whereas the two bidders hold their private bids under ciphertexts to perform the required interactions. In this scheme, every bidder connects with the auctioneer as an intermediary to indirectly interact with all the other bidders to compare their bids in parallel. Finally, all the comparison results are merely revealed to the auctioneer, who will not disclose the order of bids to the public. The bid privacy is preserved despite the presence of any corrupted bidders. Because there is no direct communication among the bidders, all messages between the two bidders will be transferred through the auctioneer. The auctioneer will be unable to see the messages except for their ciphertexts and comparison results. Moreover, a commitment with deposits is required from the bidders. Thus, this measure will ensure that they are correctly performing and they do not have the permission to change or retract their bids. After obtaining the pairwise comparison results, the auctioneer determines and broadcasts a winner who is required to open his/her commitment to the public. If some bidder submits a complaint, he/she should open his/her commitment to the auctioneer (only), who verifies whether his/her complaint is correct or not. If the complaint is false, then the auctioneer confiscates the deposits of the complainant.

Blockchain is only used to publish commitments, complaint results, auction results, etc., in this scheme. The number of interaction rounds is constant, and it can be reduced to mere four rounds if a broadcast channel is present among all participants. The scheme can still determine a valid winner if a bidder quits the scheme during the execution phase regardless of his/her deposit.

Ideal functionality. Our scheme emulates a trusted third party (TTP). First, all the bidders present all bids y_i and randomness S_i used in commitment to the TTP via an authenticated channel. Then, the TTP computes the result $\mathrm{cmp}_{i,j}$ of the comparison between each bid. Finally, the TTP announces all the comparison results to the auctioneer and broadcasts the winner to the auctioneer, all bidders, and all other participants of the blockchain. If a bidder $\boldsymbol{B}$ submits a complaint toward $\boldsymbol{B}'$, then, the TTP receives the two bids, y and y', and the corresponding randomness, S and S', respectively. Thereafter, the TTP announces y, S to the auctioneer and presents the comparison result between y and y' to the public.

Adversary model. All bidders and the adversaries are modeled to function as the probabilistic polynomial time Turing machines. Here, the adversary $\mathcal{A}$ is assumed to be semi-honest and having two parts: $\mathcal{A}_1$ and $\mathcal{A}_2$. They cannot collude with each other in our protocol. $\mathcal{A}_2$ can control the auctioneer to eavesdrop on the bid privacy of the bidders. As shown in [4], $\mathcal{A}_1$ can adaptively control one or more bidders with "augmented" capabilities. Indeed, when a bidder is controlled by $\mathcal{A}_1$, he/she is required to obey the protocols irrespective of having curiosity about the bid privacy of his/her competitors. Besides, the controlled bidder also can make an inconsistent bid with his/her commitment to compare and timely submit a complaint toward the auction

* Corresponding author (email: majie@iie.ac.cn, lvkewei@iie.ac.cn)

result. Furthermore, a bidder controlled by $\mathcal{A}_1$ can quit the comparison and is allowed to abort the auction at any time.

Commitment scheme with deposit. A commitment scheme (CS) with deposit is provided in [5]. Roughly, a committer $\boldsymbol{C}$ commits to y by broadcasting the hash $h=\mathcal{H}(S\|y)$ on blockchain via a transaction CS.Commit, which contains a deposit of value v possessed by $\boldsymbol{C}$, where $\mathcal{H}$ is a predetermined hash function and S is a random string selected by $\boldsymbol{C}$. Then, $\boldsymbol{C}$ sends a signed transaction CS.Fuse to the recipient $\boldsymbol{R}$, who can claim the deposit v if $\boldsymbol{C}$ does not follow the protocol. Otherwise, $\boldsymbol{C}$ can redeem the deposit by opening his/her commitment $(S\|y)$ via a transaction CS.Open.

Improved integer comparison protocol (iICP). We adopt three public key encryption schemes to improve the protocol provided in [6]: (1) a semantically secure PKE, $\text{PKE}_1=(\mathbf{Gen}_1,\mathbf{Enc}_1,\mathbf{Dec}_1)$ [6] satisfying the condition that if $m_1+m_2<d$, then $\mathbf{Enc}_1(m_1)^{b^{m_2}}=\mathbf{Enc}_1(m_1+m_2)$, otherwise, $\mathbf{Enc}_1(m_1)^{b^{m_2}}=\mathbf{Enc}_1(0)$; (2) a multiplicatively homomorphic PKE like RSA, $\text{PKE}_2=(\mathbf{Gen}_2,\mathbf{Enc}_2,\mathbf{Dec}_2)$ with a message space $\mathcal{M}_2$; (3) a semantically secure and additively homomorphic PKE [7], $\text{PKE}_3=(\mathbf{Gen}_\oplus,\mathbf{Enc}_\oplus,\mathbf{Dec}_\oplus)$ with message space $\mathcal{M}_\oplus$ satisfying the condition: $\mathbf{Enc}_\oplus(\mathcal{M}_\oplus)\subseteq\mathcal{M}_2$.

P_1 and P_2 with private inputs, α and β, respectively, want to compare them and reveal the result of comparison to a third party: $\boldsymbol{A}$. Similar to the research of [4, 8], let us consider $\alpha=\alpha_{k-1}d^{k-1}+\alpha_{k-2}d^{k-2}+\cdots+\alpha_1 d+\alpha_0$ and $\beta=\beta_{k-1}d^{k-1}+\beta_{k-2}d^{k-2}+\cdots+\beta_1 d+\beta_0$, where $0\leqslant\alpha_i,\beta_i<d$. P_i $(i=1,2$ runs $\mathbf{Gen}_i(1^\lambda)$ to generate the key pair $(\mathcal{PK}_i,\mathcal{SK}_i)$, whereas $\boldsymbol{A}$ runs $\mathbf{Gen}_\oplus(1^\lambda)$ to get the key pair $(\mathcal{PK}_3,\mathcal{SK}_3)$. They publish their public key $\mathcal{PK}_i$, where $\mathcal{PK}_1=(n,b,d,g,h,u)$, $l=k-1,\ldots,0$ and perform the following three-party protocol (iICP).

(1) P_1 selects $r_{1,\ell}\leftarrow_\$\{1,\ldots,2^u-1\}$ and computes $C_\ell=g^{b^{(d-\alpha_\ell-1)}}h^{r_{1,\ell}}$. Then P_1 sends C to $\boldsymbol{A}$, where $C=(C_{k-1},\ldots,C_0)$. (2) $\boldsymbol{A}$ forwards C to P_2. (3) P_2 selects $r_{2,\ell}\leftarrow_\$\{1,\ldots,2^u-1\}$, $s_\ell\leftarrow_\$\{1,\ldots,b^d-1\}$, s.t., $s_\ell\not\equiv 0 \bmod b$ and computes $D_\ell=C_\ell^{b^{\beta_\ell}}g^{s_\ell}h^{r_{2,\ell}}$; $A_{2,k-1}=\mathbf{Enc}_2(\mathbf{Enc}_\oplus(s_{k-1}))$, $A_{2,k-2}=\mathbf{Enc}_2(\mathbf{Enc}_\oplus(\beta_{k-1}\|s_{k-2})),\ldots,A_{2,0}=\mathbf{Enc}_2(\mathbf{Enc}_\oplus(\beta_{k-1}\|\beta_{k-2}\|\cdots\|s_0))$. P_2 sends (D,A_2) to $\boldsymbol{A}$, where $D=(D_{k-1},\ldots,D_0)$ and $A_2=(A_{2,k-1},\ldots,A_{2,0})$. (4) $\boldsymbol{A}$ forwards (D,A_2) to P_1. (5) P_1 computes $w_\ell=\mathbf{Dec}_1(D_\ell)$; $A'_{1,k-1}=\mathbf{Enc}_2(\mathbf{Enc}_\oplus(-w_{k-1}))\cdot A_{2,k-1}$, $A'_{1,k-2}=\mathbf{Enc}_2(\mathbf{Enc}_\oplus(-(\alpha_{k-1}\|w_{k-2})))\cdot A_{2,k-2},\ldots,A'_{1,0}=\mathbf{Enc}_2(\mathbf{Enc}_\oplus(-(\alpha_{k-1}\|\alpha_{k-2}\|\cdots\|w_0)))\cdot A_{2,0}$. Then, P_1 blinds $A'_{1,\ell}$ by computing $A_{1,\ell}=(A'_{1,\ell})^{r_\ell}$ for $0\neq r_\ell\leftarrow_\$\mathcal{M}_\oplus$. P_1 gets $A_1=(A_{1,(k-1)'},\ldots,A_{1,0'})$ by shuffling $(A_{1,k-1},\ldots,A_{1,0})$ via a random permutation π_1. Thereafter, P_1 sends A_1 to $\boldsymbol{A}$. (6) $\boldsymbol{A}$ forwards A_1 to P_2. (7) P_2 computes $A'_{0,\ell}=\mathbf{Dec}_2(A_{1,\ell})$ and blinds $A'_{0,\ell}$ by computing $A_{0,\ell}=(A'_{0,\ell})^{r'_\ell}$ for $0\neq r'_\ell\leftarrow_\$\mathcal{M}_\oplus$. Then, P_2 shuffles $(A_{0,k-1},\ldots,A_{0,0})$ to $A_0=(A_{0,(k-1)'},\ldots,A_{0,0'})$ by a random permutation π_2. Afterwards P_2 sends A_0 to $\boldsymbol{A}$. (8) $\boldsymbol{A}$ computes $m_\ell=\mathbf{Dec}_\oplus(A_{0,\ell})$. If for all ℓ, $m_\ell\neq 0$, then output is **True** (i.e., $\alpha\geqslant\beta$), otherwise, output is **False**.

Theorem 1. The iICP is secure against the adversary $(\mathcal{A}_1,\mathcal{A}_2)$, where $\mathcal{A}_1$ may control P_1 or P_2 and $\mathcal{A}_2$ may corrupt $\boldsymbol{A}$, thereby, preserving the privacy, α and β, of P_1 and P_2, respectively.

Privacy-preserving auction. Our privacy preserving auction scheme operates in a constant number of rounds, in which, a commitment scheme (CS) with deposit [5] is used to bind bids and the ciphertexts with each of the respective bidders to incentivize an honest performance. On the contrary, the above improved integer comparison protocol (iICP), is used to preserve privacy of all bids because all of them are compared under ciphertexts.

Each bidder $\boldsymbol{B}_i$ commits to his bid y_i and its ciphertexts by broadcasting the transaction CS.Commit_i on blockchain with some deposit and sends CS.Fuse_i to the auctioneer $\boldsymbol{A}$ after signing it. $\boldsymbol{B}_i$ runs iICP with all other bidders $\boldsymbol{B}_j, j\neq i$ in parallel to compare his/her bid with other bidders. Then, $\boldsymbol{A}$ obtains all the comparison results to determine a winner. Once a winner $\boldsymbol{B}_w$ is determined, his/her bid information should be revealed on blockchain for other bidders to verify its soundness. The transaction CS.Open_i can help $\boldsymbol{B}_i$ to redeem the deposit, which leaks the bid privacy. So, an alternative transaction CS.Refund_i (which contains no information about y_i) signed by both $\boldsymbol{B}_i$ and $\boldsymbol{A}$ is adopted to redeem the deposit. If a bidder $\boldsymbol{B}$ submits a complaint toward $\boldsymbol{B}'$, $\boldsymbol{B}$ should open his/her bid information to $\boldsymbol{A}$ to ensure consistency. Afterwards, $\boldsymbol{A}$ runs iICP again with $\boldsymbol{B}$ and $\boldsymbol{B}'$ and penalizes the loser by broadcasting CS.Fuse. This punishment can avoid malicious comparisons by submitting a complaint to extract bid information of the honest bidder, because each comparison is likely to leak a lower or upper bound of the bid. Finally, $\boldsymbol{A}$ signs and broadcasts all the received CS.Refund from the honest bidders to return their deposits.

Specifically, all bidders and the auctioneer agree on a hash function $\mathcal{H}$ and the deposit value used in CS.Each $\boldsymbol{B}_i$ runs $\mathbf{Gen}_1(1^\lambda)$ and $\mathbf{Gen}_2(1^\lambda)$ to generate the key pairs $(\mathcal{PK}_i^1,\mathcal{SK}_i^1)$ and $(\mathcal{PK}_i^2,\mathcal{SK}_i^2)$, whereas $\boldsymbol{A}$ runs $\mathbf{Gen}_\oplus(1^\lambda)$ to get the key pair $(\mathcal{PK}_3,\mathcal{SK}_3)$. They all publish their public keys and then, run the following parallelized iICP.

(1) Each $\boldsymbol{B}_i$ encrypts y_i into C_i via PKE_1 and computes his/her commitment $H_{y_i}^{C_i}=\mathcal{H}(y_i\|C_i\|S_i)$ with a random string S_i. Then, he/she broadcasts $H_{y_i}^{C_i}$ on blockchain by a transaction CS.Commit_i with some deposit, and sends $(C_i,\text{CS.Fuse}_i,\text{CS.Refund}_i)$ to $\boldsymbol{A}$; (2) $\boldsymbol{A}$ forwards all $C_j, j\neq i$ to $\boldsymbol{B}_i$; (3) $\boldsymbol{B}_i$ computes $(D,A_2)_{i,j}$ for all $j\neq i$ and sends them to $\boldsymbol{A}$; (4) $\boldsymbol{A}$ forwards $(D,A_2)_{j,i}$ to $\boldsymbol{B}_i$ for all $j\neq i$; (5) $\boldsymbol{B}_i$ computes $(A_1)_{i,j}$ for all $j\neq i$ and sends them to $\boldsymbol{A}$; (6) $\boldsymbol{A}$ forwards $(A_1)_{j,i}$ to $\boldsymbol{B}_i$ for all $j\neq i$; (7) $\boldsymbol{B}_i$ computes $(A_0)_{i,j}$ for all $j\neq i$ and sends them to $\boldsymbol{A}$; (8) For $\ell=k-1,\ldots,0$, $\boldsymbol{A}$ computes $(m_\ell)_{i,j}=\mathbf{Dec}_\oplus((A_{0,\ell})_{i,j})$. If $\exists i$ for $\forall j\neq i,\forall\ell$, $(m_\ell)_{i,j}\neq 0$, then $\boldsymbol{A}$ broadcasts that $\boldsymbol{B}_i$ is the winner, who should open his/her commitment on blockchain; (9) If a bidder $\boldsymbol{B}$ submits a complaint toward $\boldsymbol{B}'$, $\boldsymbol{B}$ should open his/her $y\|C\|S$ to $\boldsymbol{A}$ to ensure consistency. Afterwards, $\boldsymbol{A}$ runs iICP again with $\boldsymbol{B}$ and $\boldsymbol{B}'$ and then penalizes the loser by broadcasting CS.Fuse on-chain. Finally, $\boldsymbol{A}$ signs and broadcasts all received CS.Refund of honest bidders to return their deposits.

Theorem 2. Our auction scheme is secure against the adversary $(\mathcal{A}_1,\mathcal{A}_2)$, where $\mathcal{A}_1$ may control one or more bidders, and $\mathcal{A}_2$ may corrupt the auctioneer $\boldsymbol{A}$, thereby preserving the privacy of honest bidders.

Conclusion. In this study, we present a constant-round auction scheme via a commitment scheme and an integer comparison protocol. The time cost is comparable compared to DGK [3] and Fischlin [9] protocols which are secure against semi-honest adversary, but the round complexity and communication overhead are much lower than DGK and Fischlin, even strain [1]. Furthermore, future studies are required to make the scheme secure by using ZKP against malicious adversaries.

Acknowledgements This work was supported by National Key R&D Program of China (Grant No. 2017YFB0802500) and the 13th Five-Year National Cryptographic Development Foundation (Grant No. MMJJ20180208).

References

1 Blass E O, Kerschbaum F. Strain: a secure auction for blockchains. In: Proceedings of European Symposium on Research in Computer Security. Belrin: Springer, 2018. 87–110

2 Galal H, Youssef A. Verifiable sealed-bid auction on the ethereum blockchain. In: Proceedings of International Conference on Financial Cryptography and Data Security, Trusted Smart Contracts Workshop. Berlin: Springer, 2018. 265–278

3 Damgård I, Geisler M, Krøigaard M. Efficient and secure comparison for on-line auctions. In: Proceedings of Australasian Conference on Information Security and Privacy. Berlin: Springer, 2007. 416–430

4 Ma J, Qi B, Lv K W. Fully private auctions for the highest bid. In: Proceedings of the ACM Turing Celebration Conference. New York: ACM, 2019. 64

5 Andrychowicz M, Dziembowski S, Malinowski D, et al. Secure multiparty computations on Bitcoin. Commun ACM, 2016, 59: 76–84

6 Carlton R, Essex A, Kapulkin K. Threshold properties of prime power subgroups with application to secure integer comparisons. In: Topics in Cryptology—CT-RSA 2018. Berlin: Springer, 2018. 137–156

7 Schoenmakers B, Tuyls P. Practical two-party computation based on the conditional gate. In: Proceedings of International Conference on the Theory and Application of Cryptology and Information Security. Berlin: Springer, 2004. 119–136

8 Carlton R A. Secure integer comparisons using the homomorphic properties of prime power subgroups. Electronic Thesis and Dissertation Repository, 2017. https://ir.lib.uwo.ca/etd/4833

9 Fischlin M. A cost-effective pay-per-multiplication comparison method for millionaires. In: Topics in Cryptology—CT-RSA 2001. Berlin: Springer, 2001. 457–472