**Conference Paper for Hybrid Auction (HARAN)**

**Abstract**

*The auction is one of the most famous form market mechanisms for collecting market value of any good. Auction format such as English and Dutch which are variants of open cry auction, where the bid value of each bidder is open to each of the auction participant suffer from many issues such as bid repudiation, false valuation and bid privacy concerns so to tackle such issues sealed bid second price auction have been proposed where the bid values are submitted in encrypted form and only auctioneer has the authority to open these bids, and based on the comparison of these results auctioneer declares the highest winning bidder. But the constraint with these auctions is the bid value of each bidder is collected in one round and on the basis of submitted bid result is declared, thus removing the opportunity for the bidders to change their valuation if they think that the value of the auction good can be of higher value for them after a certain period in the auction. In this paper we propose a hybrid privacy preserving auction which preserves the privacy of the bid values of the bidders and gives the possibility of changing the valuation after a period of time.*

**1 Introduction**

Auctions are best way to gather the true market value of the product and a rich literature can be seen as to support this statement, privacy preserving auctions (PPA) sealed bid auctions were introduced to remove the chances of bidder’s temptation by knowing the other bidders bid values but sealed bid auctions come with a condition of submission of all the bid values in one round and on the basis of these values the auctioneer declares the results. In sealed bid auctions the possibility of the bidder’s temptation was removed, but the new problem was later recognized that auctioneer on behaving maliciously can get incentives upon having the control over bidders’ data and to preserve the bid privacy of losing bidders PPA were proposed. In PPA we try to limit the openness the bid value of the losing bidders and prevent any maliciousness. In PPA the bid values are sealed and are expected to be submitted in a single round of auction upon which computation are performed to declare the winner but the major drawback of sealed bid auctions is that these auctions totally remove the chances of changing the bid value if certain bidder changes its mind and want to give different valuation to the auctioned good. In this paper we design a hybrid auction scheme based on secure multiparty computation (SMPC), homomorphic encryption (HE) and blockchain which allow the bidders to change the bid value that they previously submitted upon knowing they are not the highest bidder and they can increase their value of the product to win the auction. During this whole auction procedure, the privacy of bid value is preserved and the auctioneer never knows any of the original bid value of the bidders during or after the auction. In this paper the auction format is a type of hybrid auction which achieves two goals one is achieving the privacy of the bid from auctioneers and other auction participant and the second is the possibility of changing the bid valuation upon knowing that this bid is not the highest bid. This hybrid auction format is a novel contribution of ours is a novel contribution that we are giving in this paper.

Our scheme requires total four entities Auctioneer, certifier and a losing bidder and highest bidder, job roles and working of them will be discussed in the model working section. The paper consists literature review in section 2, the preliminaries are discussed in section 3 and methodology is discussed in section 4. Experimental evaluation and conclusion are given in section 5 and section 6 respectively.

**2 Literature Review**

PPA has been greatly considered in literature with emphasis on issuing public verifiability of the results and avoiding auctioneer’s maliciousness, various trust models have been considered to do so. Table 1 presents the comparison of different models based on the trust model used and the necessary auction properties satisfied by them.

In one of the early works [[ref](https://people.eecs.berkeley.edu/~tygar/papers/Multi-round_anonymous_auction_protocols/IEIC_multiround_anonymous_auction_protocols.pdf)], a multiple-round-based auction protocol was proposed with the concept of multiple () auctioneers, making the system safe with the threshold of () such that these numbers of auctioneers are not colluding with each other till then the system is safe. In the initial phase, prices are shared for the auction goods and the bidders generate bid vectors for these prices. For the interested price, they put their , and for the non-interested price they put 0, together with the random padding generated through the sum of random polynomials. These bid vectors are then input to an SMPC algorithm, and the winning-price number of present at the winning price is revealed this is made by the auctioneer using the La-Grange scheme to solve the simultaneous equations and obtain the free variable, which gives the sum of the identities of bidders who are willing to bid at that price. If a single bidder is interested in the highest price, then only a single is present and if the sum of multiple is found then multiple bidders are interested at that price which is a case of a tie, and again subsequent rounds are performed with more refined price list near to highest price to get a single winner at the wining price. If the value of is very small then many subsequent rounds of auction will be required increasing the computation cost and dependency on the threshold of auctioneers also increases communication cost, this work doesn’t ensure the verifiability of the auction results by each participant.

Further, this work was improved in [[ref](https://ieeexplore.ieee.org/document/884610)] by using the masking of bids in random polynomials which are generated for each bid by the set of distributed servers to ensure trust in the system. The winner was detected in the same way as earlier but this time the are masked by the random polynomials. When the auctioneer declares a winning price all the distributed servers collaborate and remove the noise from these IDs to know the exact winner ID no other information is revealed to the auctioneer. This work improved the shortcomings of earlier work in terms of privacy, and security, and the second highest bid is kept secret from the winner in comparison to the previous work through the masking step by the servers. But in this work also auctioneer can also know the highest winning price and verifiability by each auction participant is not ensured. The threat model has been shifted to servers from auctioneer in comparison to previous work. Instead of an auctioneer threshold here server threshold has been used such that servers should be honest to complete the auction safely. Another work that was presented in succession by the same authors is given in[[ref](https://sci-hub.se/https:/link.springer.com/chapter/10.1007/3-540-46088-8_27)] a auction scheme is proposed where result verifiability has been assured by the side of the auctioneers which can be considered as partial verifiability, also it does not prevent the anonymity of the winning bidder from the auctioneers, and it requires a larger number of auctioneers to fulfill the auction as mentioned in [[ref](https://sci-hub.se/10.1007/3-540-45664-3_8)].

Authors in [[ref](https://sci-hub.se/10.1007/3-540-45664-3_8)] use ElGamal encrypted bidder-generated bidding vectors consisting of bids encrypted by a public key which is handled by a set of distributed authorities in a threshold manner. For each bid bidders submit a differential of their bid values as proof of their casted bid. auctioneer publicly computes the integrals of these differential bids submitted by the bidders to verify the bids. Mix and match. Later auctioneer declares the winner. In this protocol, the highest bid is revealed to the auctioneer after completion of the auction.

The work in [reference12] is similar work that we are proposing It proposes a first price auction protocol where the concept of distributing the bid value to multiple shares is used thus distributing the trust to the bidders itself is considered. In this work role of auctioneer is played by the seller, so no auctioneer is involved during the whole process of the auction thus shifting the threat model from auctioneer to seller, this paper explored bidder’s collusion possibility and a threshold of bidders being dishonest is considered to avoid bidders’ collusion and resulting in colluding bidders knowing the bid value of other bidders. Another threat is if the seller becomes malicious and colludes with the bidders then he has to collude with at least bidders to know other bids. This work also lacks in giving the auction results public verifiability to know whether or not bidders’ collusion or any corruption in protocol happened in between. If this work is applied in the second-price environment then it will be impossible to ensure that the seller changed the second-highest bid for his profit as this work doesn’t ensure verifiability of the auction results.

The works of [[ref](https://link.springer.com/chapter/10.1007/978-3-642-03549-4_20)] use multi-party computation based on secret sharing to develop a practical double auction. Their scheme uses verifiable secret sharing involving representatives of buyers, sellers, and the research project itself. Traders submit bids and ask representing how much they are willing to buy or sell at all possible prices. The bids and asks are then secretly shared among the three servers for aggregation. Each server verifies that their received share is correct by the verification property of verifiable secret sharing. The servers then aggregate the individual shares to construct demand and supply curve shares. The parties compute the market-clearing price using secure comparisons on secret shared values. After traders submit their offers, no interactivity is required (their representatives interact on their behalf), and traders can submit multiple offers. However, the protocol does not allow traders to verify the results independently, and corrupting two out of three parties renders the protocol insecure.

In the works [[ref](https://dl.acm.org/doi/abs/10.1145/3600160.3600190)] a double auction is proposed based on homomorphic encryption and zero-knowledge proof of consistencies and it satisfies major auction properties such as pseudonymity, unforgeability, traceability, and non-repudiation. The scheme is fulfilled by the assumption of a non-colluding third agent which helps in the computation of the auction results. This protocol ensures privacy preserving as well as public verifiability but the trusted third party can collude with the auctioneer and disclose the key resulting in the disclosure of the confidential data of the bidders.

Privacy-preserving auctions have found great importance in the domain of auction applications such as spectrum allocation, energy trading, data trading, etc.

One such work of [[ref]](https://ieeexplore.ieee.org/document/8384016) an application of privacy-preserving auction has been proposed through which trading of big data is completed. In the suggested protocol an intermediate platform is considered and a single auctioneer is considered with an assumption of both parties being independent of each other. Bidders bid their bidding price and forward it to the intermediate platform by encrypting it with the auctioneer's public key. The intermediate platform further adds a padding of common random number homomorphic to all gained bids and transfers these padded bids to the auctioneer and based on these padded bids winner is declared. Even though this model fulfilled the auction the assumption of independence between the auctioneer and intermediate platform doesn’t hold in real life, if they both collude then the auctioneer can easily gather all bids in the original form also public verifiability of the auction results is not ensured.

Another recent work in the domain of energy trading is [[ref](https://www.sciencedirect.com/science/article/abs/pii/S0306261923000284)] where a privacy-preserving model has been used to fulfill energy trading without disclosing any confidential information to the auctioneer about bidders. This proposed architecture is based on blockchain and it requires a certifier who certifies the participant and creates unique IDs and paillier homomorphic key pairs for the bidders and the auctioneer. Further, each bidder prepares padded information containing its original bid and a random number in the form of a product, further, this information is encrypted with the auctioneer’s public key. This information is not directly sent to the auctioneer rather it is propagated to each bidder present in the auction who further multiplies his random number to this information homomorphically and then forwards it to the auctioneer. The auctioneer collects all such padded bids and compares these padded bids with the help of a secure two-party comparison protocol (explained in section 3) and declares the winner. This model of PPA lacks public verifiability and fails when two bidders collude with each other. Even a single bidder can make the auction results incorrect and it will not be detectable.

**3 Preliminaries**

The section briefly introduces the tools considered in the proposed privacy-preserving auction scheme.

**3.1 RSA(Rivest–Shamir–Adleman) cryptosystems**

RSA [reference] is a type of asymmetric encryption that is based on the idea of the computational complexity of factorizing the product of large random prime numbers. it consists of two keys one public and the other private. The public key is used to encrypt the data and the private key is used to recover that data. One who holds the private key can decrypt any message encrypted with the private key of the same. Digital signature is a very famous example of an application based on such cryptosystems.

**3.1 Digital Signature**

A digital signature[reference] is a type of mathematical scheme where a recipient of the message can be sure that a particular message comes from a genuine source. For this purpose, a sender encrypts the message with the private key and the receiver can verify the legitimacy of the message by decrypting that message with the sender's public key. Let's say Ram sends a message to Shyam to know the genuineness of the message ram attaches a digital signature with the original message by encrypting the message with its private key and Shyam decrypts this encrypted text with Ram’s public key if the message and decrypted message are same then Shyam can be assured that message is authentic and comes from Ram.

**3.1 Paillier Homomorphic Encryption**

It is a probabilistic asymmetric algorithm for public key cryptography [reference]. The main advantage of Paillier homomorphic encryption is taking advantage of the mathematical operation that can be easily performed over the ciphertext without decrypting it. The encryption scheme is secure and is based on the nth residue problem, which is a computationally hard problem.

The main functions that are available in this scheme of cryptography are *KeyGeneration()*, *Encryption()*, and *Decryption()*.

*KeyGeneration()*: This function creates a pair of keys, that is, the *Public key (keyPub)* and a *Private key (keyPri)*. For creating this pair of keys, two large random prime numbers *(p, q)* are chosen such that their Greatest Common Divisor, i.e., *gcd(n, (p-1)(q-1))* is 1, where *n* is *p.q*. We find a *l = lcm(p-1, q-1)*. Now we select a random number *g* such that it belongs to [2, ]. We do so to ensure that *n* divides the order of *g* by checking the expression, *= (L() mod n*, where *L* is the function such that *L(x) = (x-1)/n*.

*Encryption()/E()*: For encryption of any text, we use the *Public key*, which is *(n, g)*. Let the plain text denoted by *m*, which belongs in [*0,n*). For encrypting this plain text, we select a random number *r* that belongs in *(0, n)*, and *gcd(r, n)* is 1. Then, we compute ciphertext *c* as c =  *mod*  .

*Decryption()/D()*: For decryption of the ciphertext, we use the Private key, which is *(l, )*. Let the ciphertext *c* be decrypted and compute the plaintext *m*, and then we do it with the help of the following expression *m = L( ) mod n*.

The following equations indicate the algebraic operation that can be performed over the ciphertext generated through this cryptosystem; the result after decrypting it will be the same as if we have done these operations on the plain text directly.

(1)

(2)

(3)

**3.2 Secure Multi-Party Computation**

Secure multi-party computation (SMPC) [reference] is an efficient way to know whose bid is the highest without disclosing the actual value of the bid. SMPC will help sort the ciphertexts of the bid values, and based on the result of sorting, the auctioneer will decide who is the winner.

**Secure Two-Party Comparison (STPC)**

In ARPAN, we have used a secure two-party comparison protocol to compare the bid values of two bidders. This protocol is performed between every bidder. Let's say bidder A and bidder B generate bid values b1 and b2. bidder A and B don’t want either the auctioneer or other bidders to know their bid value, and for this purpose, a mathematical formulation is performed, where both bidders generate a random value X collaboratively, and then it is padded to both b1 and b2, thus generating the expressions Xb1 and Xb2. Here, the auctioneer can easily compare both expressions, and no secret information is revealed to him or other bidders. The same mathematical formulation will be performed for each bidder, thus preserving the privacy of the bid and yet making it possible to compare the bid values. The notions that we have used throughout the paper have been described in Table 2.

|  |  |
| --- | --- |
| **Symbol** | **Meaning** |
|  | Id of bidder |
|  | Bidder i |
|  | The random number of the bidder |
|  | The bid value of the bidder |
|  | The public key of the auctioneer |
|  | The private key of the auctioneer |
|  | Public key of bidder |
|  | The private key of bidder |
|  | Message is homomorphically encrypted with the public key of the auctioneer |
|  | Message is homomorphically encrypted with the public key of bidder |
|  | The decryption of the ciphertext by the public key of bidder |
|  | Message encrypted with RSA public key of the bidder |
|  | The decryption of ciphertext with the RSA private key of bidder |

Table 2: Notations used in HARAN.

**4 The proposed hybrid auction scheme**

The section introduces the entities involved in the proposed action and then discusses the proposed model by discussing the various phases in the proposed auction scheme. The whole auction concludes in a phase-by-phase manner and each phase has its timeout before which each bidder has to ensure the completion of the phase through its side. Those unable to complete in the given time bound will be discarded from the auction.

**4.1 Entities involved in the proposed auction**

HARAN requires a total of four entities to fulfill the PPA. All four entities are described below

* Auctioneer: The auctioneer is a single party that provides the platform for conducting the auction. The auctioneer is also an active participant and calculates the auction result based on the received ciphertexts through the bidding phase. The auctioneer is interested to know true bid values of the bidders.
* Bidders: Bidders are the interested buyers of the seller’s product. In our setting, they are considered dishonest agents who may not follow the auction regulations and may try to collude with each other for the purpose of knowing other bidders bid value or to change the auction results.
* Seller: The seller is the entity here to sell an item to interested buyers and is considered an honest agent. The seller’s interest is only in selling the product at the best price that the seller can get from the auction.
* Certifier: It is an entity that has been considered to generate the unique IDs for Auction and pallier homomorphic key-value pairs for all the parties involved in the auction. The auctioneer may collude with the certifier to know real bid values; certifier has been considered a semi-honest entity in ARPAN.