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

**Abstract**

*The auction is one of the most famous form market mechanisms for collecting the market value of any good. Auction formats such as English and Dutch, which are variants of open cry auction, where the bid value of each bidder is available to each of the auction participants, suffer from many issues such as bid repudiation, false valuation, and bid privacy concerns so to tackle such problems sealed bid second priced auction have been proposed where the submitted bid values are in encrypted form. Only the auctioneer has the authority to open these bids. Based on comparing these results, the auctioneer declares the highest winning bidder. Still, the constraint with sealed bid auctions is the bid value of each bidder is collected in one round and, based on the 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 during the auction. In this paper, we propose a blockchain-based hybrid privacy-preserving auction scheme that preserves the privacy of the bid values and allows a bidder to change the bid valuation on finding someone else is the highest bidder. Our privacy-preserving auction scheme achieves the benefits of both open-cry and sealed-bid auctions.*

**1 Introduction**

Auctions are the best way to gather the actual market value of the product, and rich literature proves it. E-auctions (electronic auctions) have brought traditional auctions to a broader level, and many commercial websites are open to the general public, thus providing a wide range of auctioned apparel; users can act as buyers or sellers of this product. Auctions are not only limited to the apparel’s various other domains, such as electricity trading, spectrum allocation, cloud computing, etc., have adopted auctions to gather a reasonable valuation of the auctioned product in the market. Classical auctions were open cry auctions where each participant knows the bid value of each bidder in its true form; thus, these auctions suffered from tempered bidding, and in solution to these issues, authors proposed sealed bid auctions where the bid is submitted in encrypted form and are only open to the auctioneer, but this also suffers from problems such as bid repudiation, …... and to tackle such issues, privacy-preserving auctions (PPA) were introduced. Sealed bids and privacy-preserving auctions require the submission of all the bid values in one round, and based on these values, the auctioneer declares the results. Even though the earlier issues have been resolved, there is a tradeoff to bidders who may want to change the bid valuation, knowing they are not the highest bidders. Bidders tend to win the auction; if allowed, they change the valuation, knowing they are not the highest bidder. Changing the bid valuation is similar to the classical open-cry auction. Still, to ensure that the scheme does not suffer from bid temptation and to maintain transparency, we propose a blockchain-based hybrid privacy-preserving auction scheme where the bidders can know if they are the highest bidder and can change their bid valuation based on it. During the whole process of the auction, no actual bid value is revealed to any of the auction participants, and the auction preserves the privacy of the losing bids.

Previous privacy-preserving auctions depend on the third party or require threshold trust to satisfy the PPA (ref some of the earlier works in brief……………………….). There is always a possibility that the third party colludes with the auctioneer, and the privacy of the bids is lost; another issue that can hamper auction results is the bidder’s collusion. Our proposed hybrid privacy-preserving auction scheme ensures that the collusion of a third party with the auctioneer or bidder to bidder does not impact the auction results. We also provide the concept of distrust among the colluding participants so that these participants can never be sure whether or not they are getting correct input from the other colluding participants. Thus, distrust can be seen as a significant advantage, which works as an emotional factor among the colluding agents to never believe in their other colluding agents. We also claim that in our auction scheme, bid anonymity is maintained by each of the auction participants during the whole auction procedure. After the auction, the privacy of the losing bids is preserved.

Our hybrid auction scheme uses secure multiparty computation (SMPC), homomorphic encryption (HE), and blockchain. SMPC is an excellent tool with a lower overhead than the other PPA techniques (reference). HE, on the other hand, can perform mathematical operations on ciphertext, which again gives us the advantage of sharing the secure information among the unsecured channel and getting the required output on that data without disclosing the real information together with lower computational overhead in comparison to other secret sharing techniques and last blockchain provides us two fundamental properties which are necessary for privacy-preserving auction, i.e., trust over each transaction done during the whole auction procedure and verifiability to the auction results. Public blockchain ensures trust to the participants[reference], and each publicly stored transaction helps verify the auction results. This blockchain-based hybrid auction scheme is a novel contribution that allows the bidders to change the bid value they previously submitted upon knowing they are not the highest bidder while maintaining all the necessary properties of a privacy-preserving auction.

Our scheme requires four entities: an Auctioneer, a certifier, a losing bidder, and the highest bidder; a discussion of job roles and work is in the methodology section. The paper consists of a literature review in section 2, the preliminaries discussed in section 3, and the methodology discussed in section 4. The experimental evaluation and conclusion are given in sections 5 and 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 and bidder generate bid values  and . bidder and 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 valuecollaboratively, and then it is padded to both and , thus generating the expressions and . 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**

This section introduces the entities involved in the proposed hybrid privacy-preserving auction scheme and then discusses the working of the various phases to complete the whole auction. Phase-by-phase manner architecture is used to make the scheme work, and the information flow can be verified. To avoid maliciousness, every phase has its timeout, before which each participant has to ensure the completion of the phase from its side. Those unable to complete in the given time bound will be discarded from the auction, and a penalty will be levied on them.

**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.

**4.2 High level overview of HARAN**

Following subsection consist of overview of the working of HARAN, different phases and working of those phases has been covered in this subsection**.** Each of the bullets represents the phases in the HARAN and discuss what are the job roles perform by the entities during the HARAN.

* *Registration phase*: In this phase, the auctioneer and bidder register for the auction, and the auctioneer shares the auction details, rules, and protocols of the auction, these details and rules are listed as a transaction on the blockchain. whereas the willing bidders register for the auction through the certifier and, in return, certifier provides the public and private keys to all the participants all these transaction on the blockchain and entity registration is performed by the smart contract Registration phase is shown in Figure 2.
* *Bid submission phase*: This phase works in two halves. In the first half, the bidders submit their bid value to the auctioneer in the form of a random number added to their bid value (Random numbers are generated by bidders and auctioneer at their node and are always kept secret), further encrypted with the public key of other bidders, i.e., destination bidder. In the next half, the auctioneer homomorphically adds a fraction of its random number to the submitted bid value and forwards it to the destination bidder. In the end, destination bidders decrypt the message, add its random number, and resend this information to the auctioneer for STPC.
* *Bid comparison phase*: In this phase, the auctioneer compares the bid values via STPC and declares the highest bidder among all other bidders. The bidders who want to change their valuation after knowing they are not the highest can again perform the bid submission phase with the highest bidder and try to make a higher valuation to win the auction.
* *Market clearing phase*: when no bidder is willing to change the valuation, auctioneer declare the highest winner of the auction got from the last bid comparison phase and that highest bidder connects to the seller to purchase the auctioned good. This phase has been demonstrated in the Figure 3.

|  |
| --- |
| **Protocol:**   1. Interested entities submit their unique identities . 2. Certifier generates and Keys.   gets  gets   1. Bidders and auctioneer publish their to blockchain.   **Smart contract ():**  For every request for new registration ***userReg*** function is triggered.   1. Check if already not present in the database. 2. Call the ***depst*** function to make the early deposit. 3. Input the user information to database and return the key value pairs. |

**Figure 2**: Registration protocol & smart contract.

|  |
| --- |
| **Market Clearance Protocol:**   1. encrypts with ’s public key and propagates to the network. 2. is only able to decrypt this message from auctioneer. 3. declares himself winner and contacts the seller to purchase the good. |

**Figure 2: Market clearance phase protocol.**

**4.3 Bid submission phase**

This phase works with the bidders generating bid value which is their current valuation of the product and pad it with their own generated large random number. The padded value of bidder is than encrypted with the targeted bidder public key and further this ciphertext is encrypted with the RSA public key of the auctioneer. Auctioneer decrypts the encrypted information and recovers encrypted upon which adds a random fraction of its own large random number and keeps other fraction of the random number secret to itself. A than forwards to . After receiving , decrypts the information with its private key and adds its random number . After addition forward back the updated to

**Algorithm 1**: Bid Submission Phase

**Input**:

**Output**: STPC pair.

1. *generates bid value for bidder*
2. *decrypts and adds .*
3. *A forward this information to*
4. *decrypts and again pads with*
5. *forwards updated to*
6. *after decryption adds and keeps the information with itself.*

**4.4 Bid comparison phase**

This phase contains the steps through which the highest bidding bidder is declared to other bidders and opportunity is given to increase their valuation and compete with the highest bidder. compares the collected and declares the highest bidder . Upon declaration of the highest bidder call is open to all remaining bidder if any of them wants to change their bid valuation and if some bidder wants to do so than again Algorithm 1 is followed. This phase continues until no bidder is willing to change their bid valuation and the final highest bidder is the auction winner. Algorithm 2 demonstrates the bid comparison phase.

**Algorithm 2**: Bid Comparison Phase

*Input: ,*

*Output: Highest Bidder*

1. *compares the received &*
2. *A declares highest bidder and waits for a call to raise valuation.*
3. *Declare as the winner.*

**5 Experimental Evaluation**

**6 Threat Model**

In this section we analyze possible threats that our proposed model can face and we also provide proof that our proposed model will be safe against such type of threats.

Theorem 1: *A cannot gather any true bid from the data that has been collected during the auction*.

Proof: the data collects with respect to is and these both can be represented as

(4)

(5)

As equation 4 and 5 contain total 4 unknown variables, and the number of equations is 2 only then no exact value of any variable can be calculated from this much information.

The above theorem proves that bidders’ data is safe with the auctioneer and no real bid value can be revealed with the help of STPC pairs collected by the auctioneer.

Another threat that can arise in our scheme is the concern of collusion of the certifier and the auctioneer.

Theorem 2: *and on collusion can never get .*

Proof: on collusion with can get the private keys of and thus, can open the encryption of the bidders. This encryption can be opened at bid submission phase and on decryption auctioneer can get the information sent by . The information will be

(7)

(6)

In both the equation the bids are padded by the random number of the bidders and they are secret to them only so we can claim that auctioneer can never disclose the bid values are safe till the bid submission phase and cannot be disclosed from collusion A and C.

Discuss with sir about shifting key generation to the bidders and certifier being the bulletin board.

Another threat that is crucial from the perspective of the proposes auction scheme is the safety from the collusion of bidder to other bidder. IN this aspect we show that our scheme cannot totally avoid this treat but we prove the condition of distrust in such situation, where a participant will be reluctant to believe blindly on the information provided by the other participants and solely relying on the information of others may lead them too losing the auction.

Theorem 3*: Collusion of to will always result in distrust situation and no one of them will be able to verify truthfulness of the shared information.*

Proof: On collusion *&*  they can share their information too each other. We will see the proof from the side of *to*  and from other side it will be same so no need to prove. On collusion shares its *to .* can put this information in the data that it receives from in the bid submission phase, it can be represented as

= (8)

recovers m1 from this information upon putting the values of *to .* Upon the completion of the auction result gets the public information

(9)

(10)

and if it tries to validate the information that was shared by than it can verify this information by equation 9 and 10. From equation 9 it can know the auctioneer random number by adding and further from equation 10 if it need to verify the data of it has to rely again on to share the correct value of which can be easily change because for any sum such as x + y their always exits x’ + y’ and both expression yield equal results so can always fake by and will have no way to verify the correctness of these shared information.

**6 Security Evaluation**

Proposed auction scheme is secure and the safety of the proposed auction scheme is evaluated in total of …. Aspects.

*1)Anonymity*: Here anonymity refers to the bidders whose real id is completely anonymous and it can not be traced by the other participants except certifier and other entities who come in contact to the blockchain can also not recover the original IDs of the bidders. In registration phase bidders submit the UID which is their unique ID which is encrypted with the certifier public key. So, the encryption can only be opened by the C only. We can claim that bidder’s anonymity is maintained even after the end of the auction. For more safety certifier can be considered in distributed manner.

*2) Bid Privacy:* our proposed auction scheme achieves another security parameter which is bid privacy, from each of the participants as well as from the auctioneer too, as proved in the threat model neither the auctioneer, nor the bidders can discover the true value of the bid submitted but the bidders.

*3) Non-repudiation:* In the proposed hybrid auction scheme the bidders are not allowed to change their bid submitted in single iteration of bid submission phase, bidders are only allowed to change their valuation upon declaration of the highest bidder as a challenge to the highest bid. Each bid submission is registered as transaction on the blockchain thus we can say that our proposed hybrid auction scheme satisfies the non-repudiation of the bid.

**7 Conclusion**