Ambiguity Resistant Privacy-Preserving Auction (ARPAN)

- dubiety

Abstract

Auctions have become very popular for trading a good, primarily when the actual value of that particular good is unknown in the market, and with the internet era, auctions have seen tremendous growth in terms of accessibility and conductibility; therefore, many online platforms have come into the picture. However, the primary concern with these platforms was that information such as bid values shared by the bidders with these platforms are open to the platform holder, i.e. the auctioneer and major threats such as data privacy and using bidders' data to manipulate the results of the current or future auctions have been found. To ensure safety from these issues, privacy-preserving actions (PPA) have been proposed for such environments so that bidders' privacy is preserved. Ensuring verifiability together with anti-collusion is a challenge in PPA environments, the possibility of bidders' collusion to manipulate auction results and make them ambiguous is an issue that is lacking in past works. Verifiability and anti-collusion become a major challenge because privacy-preserving auctions hide most of the information to preserve privacy and there may be ambiguity in the auction result which again is undetectable till the auction holds verifiability. In this paper, an ambiguity-resistant privacy-preserving auction (ARPAN) is proposed which ensures safety from bidders' collusion together with the verifiability of the auction results and all other necessary properties. ARPAN is based on secure multi-party computation and homomorphic encryption; ARPAN enables us to perform an auction without disclosing the bid information of buyers to the auctioneer, even the highest bid is not revealed to the auctioneer, it also ensures that bidders' collusion to change the auction result will be identified before the declaration of the results, and the auction results will be publicly verifiable to each participant of the auction. Thus, ARPAN preserves the bidders' privacy, removes ambiguity in the auction result, and makes the auction results publicly verifiable.

1 Introduction

Auctions have emerged as one of the most excellent tools to gather the actual value of any product. For this purpose, various auction methods have been proposed in the past [reference]. Popular auction types, such as English and Dutch [Reference], are frequently used. Most auctions prefer open bidding, i.e., bid value is open to each participant of the auction, and everybody knows what value a specific bidder is willing to pay for the auctioned good. The drawback with such auctions is that the bidders' data is easily accessible to everyone, ultimately leading to unfair auctions having bid repudiation, false valuation, fake bidding, etc. [reference]. The second price auction [reference], where the highest bidder pays the second highest price, was proposed to solve many such issues, and the concept of sealed bidding was introduced. Due to the sealed bid, only the auctioneer can open and compare all the bids and then declare the winner. Sealed bidding removes the issue of price changes and the temptation to raise the price by limiting the openness of bid values to the auctioneer only. Still, the problem is that we must consider the auctioneer as a trusted entity and trust the auctioneer not to misuse bid information.

Modern internet-based auctions, i.e., e-auctions, platforms, [reference] are generally privately owned and led by the auctioneer itself, thus creating great opportunities to gain profit from using bidder's data, for example, maliciously using it for upcoming auctions, in case of second priced sealed bid auctions auctioneer may change the second highest bid and make it too close to the highest bid and earn the difference as his profit, and it will be undetectable because the bids are sealed. In case the bids are not hampered by the auctioneer and a certain bidder wins the auction and pays the second price as a winning price, another threat that is formed is on the subsequent auction of the same good; the auctioneer sets the reserve price of the good as the last auction's winning price thus securing his gain. The auctioneer may sell this data to third-party retailers, and they may use this information while selling the same good to the bidders [reference]. They may not sell goods lower than that bid price. The cases of auctioneers performing malicious behavior are not only on paper there is real-life proof in the domain of energy trading where auctioneers misused the bidder data maliciously for financial incentives [reference]. Another major threat in a privacy-preserving auction environment is to ensure anti-collusion, two or more bidders may collude with each other and try to change the auction results or may try to know the bid values of other honest bidders and in most of the PPA's bids are in encrypted form and detecting such maliciousness by bidders is not easily detectable and during the literature review we have found this research gap in past works and we propose ARPAN which enables us to detect any such bidders collusion before the declaration of the auction results, ARPAN also prevents all the issues mentioned above together with bidders collusion, in ARPAN during and after the auction the completion of the auction no real bid value is revealed to the auctioneer. Experimental evaluation of ARPAN shows that this scheme is practical in real life and execution time for 500 number of bidders is …... which is very less and shows practical applicability of ARPAN for real time privacy preserving auctions. ARPAN holds all other major properties significant for PPA and these properties are listed below.

- Privacy: Privacy refers to preserving the bid values from the auctioneer and all other participants before and after the auction.
- Accountability: This means a malicious bidder can't disrupt the integrity of the auction results by submitting a deceitful bid value and can bypass the system's safety.
- Integrity: The Bidders can submit the bids within an allocated time frame, thus preventing the false submission after the time frame.
- Non-Repudiation: Bidders cannot deny the bid that they have submitted to the system; protocol should be able to map the bids to original bidders.
- Fairness: The bidder has the same power and authority as other bidders to check the authenticity of the results.
- Verifiability: Each bidder must be able to verify the auction results securely.
- Transparency: The winning bid's origin, authenticity, and legitimacy must be guaranteed by all the bidders.
- Anti-Collusion: Two or more bidders must not be able to collude with each other and try to disrupt the auction results or maliciously know the bid value of other bidders.

ARPAN satisfies all the above-mentioned properties. The rest of the paper is organized as follows. Related works have been concluded in section 2. Section 3 provides the background of tools used to fulfill our work. The working of the proposed scheme is shown in section 4. Section 5 consists of the experimental evaluation. Section 6 concludes the work. Next, we present a case study proving the algorithm's safety.

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], a multiple-round-based auction protocol was proposed with the concept of multiple (n) auctioneers, making the system safe with the threshold of $(t-1)$ such that these number of auctioneers are not colluding with each other till then the system is safe. In the initial phase, k prices are shared for the auction goods and the bidders generate bid vectors for these prices. For the interested price, they put their ID, 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 ID present at the winning price is revealed this is done by the auctioneer using the La-Grange scheme to solve the simultaneous equations and obtain the free variable, which gives the sum of 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 ID is present and if the sum of multiple IDs 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 k 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] 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 IDs 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 $n-1$ servers should be honest to complete the auction safely. Another work that was presented in succession by the same authors is given in[ref] a $M+1$ 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].

Authors in [ref] 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 $m-2$ 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 $2m$ 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] 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] 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] 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] 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.

We have incorporated [ref] the PPA model in our proposed work ARPAN and further extended it to satisfy all necessary auction properties together with anti-collusion and verifiability and in the whole process of doing so no bid value is revealed to the auctioneer during or after the auction. The auctioneer declares the winner based on the submitted encrypted padded bids only and the results are publicly verifiable to both the auctioneer and bidders.

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, n^2]. We do so to ensure that *n* divides the order of *g* by checking the expression, μ= *(L(*g^l $mod\ \ n^2\ )^{-1}$ *) 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 $= g^m\ r^n\ \ mod\ n^2$.

Decryption()/D(): For decryption of the ciphertext, we use the Private key, which is *(l,* μ*)*. 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(* $c^{l\ mod\ n^2}$ *)*μ *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.

$$D\ (E(m1)|KeyPub\ \ E(m2)|KeyPub\ mod\ \ n^2)|KeyPri\ = (m_1 +\ m_2)\ mod\ n \tag{1}$$
$$D(\ E(m1)|KeyPub\ \ g^{m2} mod\ \ n^2)|KeyPri\ = (m_1 + m_2)\ mod\ n \tag{2}$$
$$D\ (\ (E(m)|KeyPub)^k\ mod\ \ n^2)|KeyPri\ = km\ mod\ n \tag{3}$$

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
BID_i	Id of bidder B_i
B_i	Bidder i
r_i	The random number of the bidder B_i
b_i	The bid value of the bidder B_i
$pubKey_{Auc}$	The public key of the auctioneer
$priKey_{Auc}$	The private key of the auctioneer
$pubKey_i$	Public key of bidder B_i
$priKey_i$	The private key of bidder B_i
$E(\ x)\|pubKey_{Auc}$	Message x is homomorphically encrypted with the public key of the auctioneer
$E(\ x)\|pubKey_i$	Message x is homomorphically encrypted with the public key of bidder B_i
$D(\ y)\|priKey_i$	The decryption of the ciphertext y by the public key of bidder B_i
$E^{RSA}(x)\|pubKey_i^{RSA}$	Message x encrypted with RSA public key of bidder B_i
$D^{RSA}(x)\ \|priKey_i^{RSA}$	The decryption of ciphertext y with the RSA private key of bidder B_i

Table 2: Notations used in ARPAN.

4 The Proposed Privacy-Preserving Auction

The section introduces the entities involved in the proposed auction and then discusses the proposed model by discussing 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.

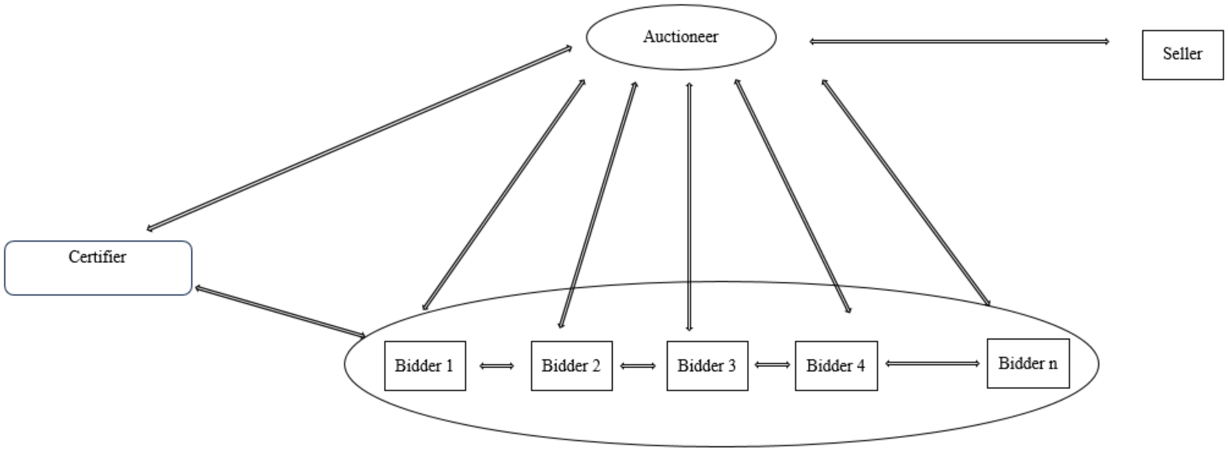

Figure 1: Architectural overview of ARPAN

4.1 Entities involved in the proposed auction

ARPAN 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. Auctioneer may collude with the certifier to know real bid values; certifier has been considered a semi-honest entity in ARPAN.

A major concern of previous PPAs was the dependency on the central authority to avoid dependency on a central authority we have introduced the certifier and the data that is shared with the certifier is only the unique IDs of the participants to generate homomorphic encryption and RSA key pairs and if certifier colludes with the auctioneer, then also ARPAN ensures privacy of bidders' data will be preserved. Here, the auctioneer can be any online auction platform service provider responsible for conducting the auction. We aim to achieve an auction where no sensitive information can be disclosed, thus preventing bid privacy from the auctioneer and externally interested parties, nor can bidders submit fake data during SMPC to win the auction or disrupt the auction's legitimacy thus making the auction bidders collusion-proof. In our model, we consider both the bidders and the auctioneer dishonest. They are both interested in their benefit; bidders can try to submit false data and win the auction or to know the bid value submitted by other bidders, and the auctioneer wants to know the original value of the bids to earn benefit from this data in the future. The seller is considered an honest party only interested in selling the goods at the best price. The certifier is considered to make the scheme work, but the information shared with the certifier is kept to a minimum and no confidential information is shared with it so that it cannot disturb the auction.

The architectural overview of ARPAN has been shown in Figure 1.

4.2 High-level overview of the phases

The protocol consists of a total of 4 phases, as depicted in Figure 2. Following is the high-level overview of the proposed protocol

1. Registration Phase: Each participant registers with the certifier using its unique ID and ensures their entry to the database. The certifier issues the public and private keys to each bidder and the auctioneer.

2. Bid Submission Phase: Bidders generate a large secret random number for themselves, which will be used to fulfill the STPC protocol. Each bidder encrypts its bid value padded with its random number by the auctioneer's public key, together with the digital signature, and then forwards this data to each bidder by encrypting it with their public keys. Each bidder adds its random number to the received information homomorphically and then forwards the same to the auctioneer for STPC.
3. Ambiguity Removal Phase: In this phase, ambiguity removal takes place; before the declaration of the results auctioneer analyzes all collected data from the bid submission phase to check if no collusion or wrong entry has been made through the bidders. If ambiguity is found the auction is rejected by the auctioneer.
4. Market Clearance This phase is for the declaration of the winner, the winner is declaration is based on of STPC protocol applied on the padded bids submitted by the bidders in the bid submission phase. Later auctioneer makes this auction data public so that each participant can verify the auction results.

The in-depth discussion of each phase will be made in the following subsections. In ARPAN, we present a secure two-party comparison-based PPA where the possibility of bidders' collusion can easily be detected together with a proper method to verify the auction results by both bidders and auctioneer, and no actual bid value of a bidder is revealed to any of the participants of auction other than the bidder itself.

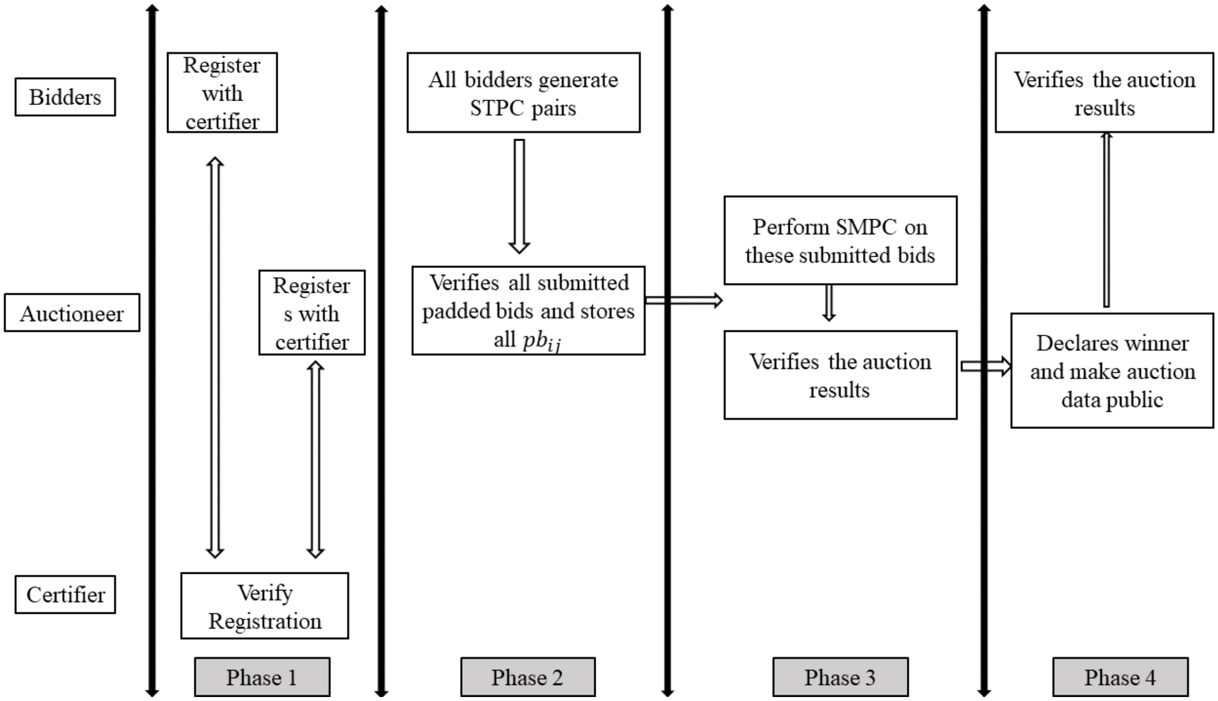
Bidders
Auctioneer
Certifier
Register with certifier
Registers with certifier
Verify Registration
All bidders generate STPC pairs
Verifies all submitted padded bids and stores all pb_{ij}
Perform SMPC on these submitted bids
Verifies the auction results
Verifies the auction results
Declares winner and make auction data public
Phase 1
Phase 2
Phase 3
Phase 4

Figure 2: High-level overview of ARPAN

4.3 Phase 1: Registration Phase

This phase is the preliminary phase, where an auctioneer submits the auction issue request to the certifier and submits the auction details to the issuer. Details can be time frames of the auctions, rules, protocols of the auction, date, and goods to be auctioned. The certifier issues a set of public and private keys of pallier homomorphic encryption and RSA encryption to the auctioneer and all the bidders willing to participate on the auction date in exchange for a unique ID. Here, the certifier works as the bulletin board, and no confidential information is shared with the certifier except a unique ID to generate the keys.

4.4 Phase 2: Bid Submission Phase

Bidders submit their bid as the sum of their own generated random number and their actual bid. Further, this data with digital signature is submitted to other bidders as represented in equation 4.

$$\{\ E(E(\ r_i + b_i)|pubKey_{Auc})|pubKey_j,\ \ DS_i\big(E(E(\ r_i + b_i)|pubKey_{Auc})\big|pubKey_j\big)\ \ \} \tag{4}$$

Here, the first part of equation 4 is the bid b_i of bidder B_i padded with its random number r_i, and this information has double encryption, one with auctioneer public key $pubKey_{Auc}$ and then further with the bidder to whom this information is sent for STPC i.e., to bidder B_j. The Second part is the digital signature of B_i on the sent information to maintain the authenticity of the sent information.

In the next step B_j decrypts the information and adds its random number r_j to the ciphertext homomorphically; together with this, bidder B_j also adds its digital signature and submits this data to the auctioneer. The data submitted to the auctioneer by bidder B_j that was gained to him from bidder B_i is shown in equation 5.

$$\{\, E(\,r_j + r_i + b_i)|pubKey_{Auc},\ DS_i\big(E(E(\,r_i + b_i)|pubKey_{Auc})\big|pubKey_j\big), DS_j\big(E(\,r_j + r_i + b_i)\big|pubKey_{Auc}\big)\,\} \qquad (5)$$

The information from equation 5 is verified by the auctioneer with the help of digital signatures and then saved in the auctioneer's database.

Algorithm 1 is the demonstration of the protocol that is followed during the bid submission phase.

Algorithm 1

1. For a set of n bidders $B = \{B_1, B_2, \ldots \ldots .. B_n\}$,each bidder B_i generates padded bids information I_{ij} at own end and shares with, each bidder B_j.

$$\forall i, j \in (2, n], i \neq j \ \ I_{ij} = E(E(\,r_i + b_i)|pubKey_{Auc})|pubKey_j$$

2. Bidder B_j decrypts and adds its random number to received I_{ij} at their node and then updates the information which is represented by I'_{ij}

$$D\big(E(E(\,r_{+i}b_i)|pubKey_{Auc})\big|pubKey_j\big)|priKey_j$$
$$I'_{ij} \ = E(\,r_j + r_i + b_i)|pubKey_{Auc}$$

3. Auctioneer decrypts received I'_{ij} represented as pb_{ij} and stores it to use in upcoming phases.

$$pb_{ij} = \ D\big(I'_{ij}\ \big)|priKey_{Auc}$$
$$pb_{ij} = r_j + r_i + b_i$$

Bid submission prevents non-repudiation and privacy of the bids. Digital signature prevents any hampering to the data ensuring non-repudiation together with the authenticity of the sent messages, while the padding of random numbers ensures that no privacy of bids is leaked to the auctioneer when the bids get finally submitted to the auctioneer. As in the bid submission phase bids privacy is preserved and non-repudiation is prevented and the auctioneer can declare the winner using secure two-party comparison protocol upon all gathered pb_{ij} and papers such as [reference] have used the above same approach to declare the winner but this protocol doesn't ensures anti-collusion if two bidders collude they can easily make the results of the auction incorrect or may gather the information of bid submitted by other bidders and that's why concluding auction results by phase 2 solely doesn't guarantees that no such maliciousness has occurred in between, and neither provides any way to detect such maliciousness. Phase 3 proposed in this paper is to ensures the system safety from the above-described issue of bidder's collusion and a method to publicly verify the auction results.

4.5 Phase 3: Ambiguity Removal Phase

In this phase before the declaration of the winner auctioneer checks for anti-collusion due to the bidders. The auctioneer follows algorithm 2 to find the bidder's collusion that can took place in between. If the auctioneer finds any collusion, then auctioneer rejects the auction and if no collusion happened then declares the winner in market clearance phase. Following is the description of algorithm 2.

Algorithm 2

1. Auctioneer collects all pb_{ij} and checks the following expression for every iteration of an arbitrary k from the range $[1, N)$.
   $for\ (k\ \leq k + n;\ k + +)$

$$SUM_k = \sum_{i=1}^{n} \begin{cases} if\ \ k + i \leq n & r_{k+i} + r_i + b_i \\ else & r_{k+i\,mod\,n} + r_i + b_i \end{cases}$$

2. Auctioneer checks each SUM_k on the basis of following conditions

$$\begin{cases} if\ SUM_k = SUM_{k-1} = SUM_{k-2} = \cdots = SUM_n & auction\ is\ accepted \\ else & reject\ the\ auction \end{cases}$$

The first step of the algorithm 2 arranges all pb_{ij} in a specific order of matrix (shown in case study) based on an arbitrary stepping value k. Here k is used to change the arrangements of the elements of the matrix in such a way that the sum of each row collected in the variable SUM_k is same in every iteration of the for loop. If each iteration of the loop yields same value of SUM_k then auctioneer can be assured that no collusion happened in between by the side of bidders. A proof of algorithm 2 has been presented in the case study section and the proof confirms that ARPAN will detect any possible bidder's collusion even if a single bidder will create ambiguity in between the bid submission.

This phase removes any ambiguity happened in between the earlier phases; this phase bounds the bidders to submit true input during the bid submission otherwise it gets detected in ambiguity removal phase using algorithm 2. Earlier works which used these approaches lacked detection of such ambiguity and if such ambiguity goes unnoticed then it is guaranteed that the auction results will not be correct. Two colluding bidders can easily take the auction offtrack of the auction rules. They can also extract bid values of other bidders. But by the use of the algorithm 2 the auctioneer can find any such ambiguity present in the collected bid data.

4.6 Phase 4: Market Clearence Phase

After the ambiguity removal phase auctioneer compares all collected pb_{ij} via STPC protocol and finds the winning bidder. For declaration of the winning bidder the auctioneer encrypts the winning bidder's BID with the winning bidders RSA public key and propagates it to the network. Each bidder tries to decrypts this message by the auctioneer and only the winner bidder can decrypt it thus knowing he is the winner and can communicate with the seller to further buy the auctioned good. The procedure of market clearance phase has been demonstrated in Algorithm 3.

Algorithm 3

1. Auctioneer compares all pairs of pb_{ij}.

$$\forall i, j \in (2, n], i \neq j \qquad pb_{ij}\ compared\ with\ pb_{ji}$$

2. Auctioneer encrypts the winning bidder BID_{winner} and forward it to the network

$$E^{RSA}(BID_{winner})|pubKey^{RSA}_{winner}$$

3. Winner bidder decrypts the message and knows itself being the winner of auction**.**

$$D^{RSA}(E^{RSA}(BID_{winner})|pubKey^{RSA}_{winner})|pubKey^{RSA}_{winner}$$

5 Security Analysis and Evaluation

Security of the proposed model ARPAN will be judged on the properties that are necessary for the auction and we will evolution of the proposed model is holding against such properties.

5.1 Privacy

As bids are padded by the random number of two bidders the original information of the bid to be recovered by the auctioneer is not possible without knowing the random numbers of the two bidders. Thus, we can claim that the bids are safe till both bidders don't share their random numbers with the auctioneer, and as the bidders are concerned about their bid privacy, they will not be willing to disclose their bid to the auctioneer and if they do so then also, they will only disclose only their bid values to the auctioneer.

5.2 Accountability

Accountability is property when no bidder can submit fake deceitful bids and diverge the auction from the real path, ARPAN ensures that all the bids that go to the auctioneer have a digital signature with them, and faking one own bid by any bidder is not possible, the only way that a bidder can fake the bid is when the bidder submit fake random values, but as shown in ambiguity removal phase no any such maliciousness will go unnoticed, the auctioneer can detect such maliciousness with algorithm 2 and can exactly know whether or not any such deceitful fake bid has been submitted by any bidder in between.

5.3 Integrity

In ARPAN each phase concludes in a fixed period and each bidder is authenticated via the digital signature made by the key which has been provided by the certifier. The time slots have been allotted in each phase in which each participant has to conclude their role otherwise, the participant is rejected from the auction so only authenticated bidders are allowed to submit bids within a given period thus integrity of the auction holds in ARPAN.

5.4 Non-Repudiation

The bidders are not allowed to change the bids that they cast once, in the bid submission phase they cast their bids by generating secure two-party comparison pairs, together with a digital signature with the help of a key that is provided to them by the certifier and these key pairs are mapped with the bidders and certifiers issue only one such key to each bidder so no bidder can deny once submitted bid to the auctioneer.

5.5 Verifiability

The verifiability of the auction result that we have discussed in literature reviews as the lack of some previous works has been addressed in ARPAN. As in the end auctioneer makes all data public any of the interested participants can verify the result with the help of Algorithm 2 of the ambiguity detection phase thus ARPAN guarantees that no malicious behaviors will not go unnoticed and the winner of the auction is the highest bidder only which can be publicly verified by each participant of the auction.

5.7 Fairness

By watching the working of all phases, the proposed auction schemes can be seen as fairness assuring, in each phase each bidder gets an equal set of opportunities, and in the end, no biasedness is shown in the declaration of the winner thus, we can say that fairness is greatly achieved in proposed privacy-preserving auction ARPAN.

5.8 Transparency

Here transparency is maintained as all bidders can check the authenticate the legitimacy and origin of the winning bid. As the data of the bid submission phase is made public by the auctioneer, each bidder can conclude the winning bid is greater than its bid and the results of the auction are authentic and transparent.

5.9 Anti-collusion

Phase by-phase structure of our proposed scheme guarantees that no bidder-to-bidder collusion will go unnoticed, if some group of bidders try to perform such maliciousness, then this maliciousness will easily be detected by the auctioneer in the ambiguity detection phase with the help of algorithm 2. ARPAN ensures anti-collusion through the side of bidders and guarantees that no bidder's collusion will go unnoticed and will be detected before the declaration of the winner.

6 Threat Model

This section will analyze the threat model and possible threats that can be confidently identified in ARPAN, possible threats that our proposed privacy-preserving scheme can effortlessly tackle, provides solution to them are following.

6.1 Malicious Bidder

This threat occurs when a bidder is malicious and may deviate from the auction rules. The maliciousness that it can show is by submitting fake random numbers either to change the auction results or may be intending to know other bidders' bid value. But in both cases our model will identify such threats with the help of the ambiguity removal phase and such maliciousness will be detected before the result declaration of the auction.

6.2 Malicious Auctioneer

The malicious auctioneer may want to know the bid values of the bidder for its profit but as in our model we are using paillier homomorphic encryption and random padding to the bid value and the problem of finding the addends of a large number is computationally hard the possibility of finding the original bid value by bidder by removing the random number of the bidder is computationally not possible with the computation power currently the users possess. The auctioneer can receive a bid in two states one that is after the bid submission phase and one during the bid submission phase some bidder colludes with the auctioneer and open their private homomorphic key to the auctioneer but in both cases, the auctioneer will receive the padded bid which is a computationally hard problem for the auctioneer to recover the original bid value by removing random noise from the padded bids.

6.3 Bidders collusion

In the case of the bidder’s collusion two or more bidders try to collude to change the action results or may try to know other bidders' bid values but this can be easily detected with the help of algorithm 2 in the ambiguity detection phase, and finding such bidder collusion is possible till the number of dishonest bidders is $n-2$. A bidder may try to know the original bid value of the other bidder from the received bids in the bid submission phase but these values are encrypted with the auctioneer's public key and if this bidder colludes with the auctioneer, then also the value of the bid that he recovers is padded with the random number of the original bidder and as shown in just previous subsection recovering original bid by removing random noise is computationally not possible.

6.3 Corrupt Certifier

Another threat that can come to the picture in the PPA models is the dependency upon the central authority as it can result in a single point of failure but in our proposed model no confidential data is shared with the certifier only a unique ID of the interested participants is shared thus no bid values can be extracted by the auctioneer or central authority even if they both collude. If the certifier leaks the private key pairs, then also the bids that will be collected by the auctioneer will be in a padded state and the padding has been performed by the bidder itself who is unwilling to reveal its own bid value to the auctioneer.

7Conclusion

Case Study

In this case study we are going to give proof of the algorithm 2 that it will be working even if a single bidder submits false entry or even if two or more bidders collude and try to change the results of auction or try to recover bid values of other bidders.

Statement 1: "*even if a single bidder violates the protocol, then it will not go unnoticed*".

Let us consider n bidders and $n > 2$, let's say $B_1, B_2, \ldots, B_n$ where each bidder bids $b_1, b_2, \ldots, b_n$ respectively. In the bid submission phase for bidder B_1 the bid pairs that will be generated and submitted to auctioneer in respect to all other bidder for secure two-party comparison will be $r_2 + r_1 + b_1, r_3 + r_1 + b_1, \ldots, r_n + r_1 + b_1$. Let's suppose bidder B_1 submits different random numbers from the one it forwarded to all bidders in bid submission phase for the purpose to create ambiguity in the auction results and let the different message be $r_1' + r_2 + b_2$ and this fake random number is added by B_1 when it was adding its random number in the padded bid of bidder B_2. If the results of the auctions were only based on the bid submission phase, then this ambiguity has gone unnoticed and B_1 had altered the auction results, but due to the ambiguity detection phase B_1 submitted data will have to be passed through ambiguity detection phase. During the ambiguity detection phase the ambiguous padded bid will be detected by the auctioneer because auctioneer performs the ambiguity check on this data before declaring the winner.

To detect ambiguity created by B_1 auctioneer follows ambiguity removal protocol and arranges all pb_{ij} in following manner and for simplicity we have taken value of k which has been used in step 1 of algorithm 2 as 1.

$r_2 + r_1 + b_1,\ r_3 + r_2 + b_2,\ r_4 + r_3 + b_3,\ r_5 + r_4 + b_4$ --$r_1 + r_n + b_n$
$r_3 + r_1 + b_1,\ r_4 + r_2 + b_2,\ r_5 + r_3 + b_3,\ r_6 + r_4 + b_4$ ---$r_2 + r_n + b_n$
.   .   .
.   .   .
.   .   .
.   .   .
$r_n + r_1 + b_1,\ r_1' + r_2 + b_2,\ r_2 + r_3 + b_3,\ r_3 + r_4 + b_4$---$r_{n-1} + r_n + b_n$

As the sum of all these rows must be same which is $2r_1 + 2r_2 + \cdots + 2r_n + b_1 + b_2 + \cdots + b_n$,but as if bidder B_1 has submitted fake random value the last row will yield a different sum which is $r_1' + 2r_1 + 2r_2 + \cdots + 2r_n + b_1 + b_2 + \cdots + b_n$ and this sum will be different from all other rows thus if a single row yields different sum then it's a red flag for auctioneer to discard the auction.

Statement 2: "*If two or more bidders try to collude and disrupt the auction results then also the ambiguity will not go unnoticed"*

This ambiguity detection algorithm can be applied to the data collected from bid submission phase and ambiguity can be detected for a single bidder case but what happens when number of colluding bidders is more than 1, then these bidders can bypass the algorithm 2 by faking the random number in such differences so that the sum of rows comes exactly same. For example, let say the bidders B_1 *and* B_3 are colluding and they have faked random number as shown in equation 6.

$$r_1 + r_3 = r_1' + r_3' \tag{6}$$

Now the auctioneer arranges the bids of bid submission phase in following manner.

$r_2 + r_1 + b_1,\ r_3 + r_2 + b_2,\ r_4 + r_3 + b_3,\ r_5 + r_4 + b_4$ --$r_1 + r_n + b_n$
$r_3 + r_1 + b_1,\ r_4 + r_2 + b_2,\ r_5 + r_3 + b_3, r_6 + r_4 + b_4$ --$r_2 + r_n + b_n$
.   .   .
.   .   .

. . .

. . .

$r_n + r_1 + b_1,\ r_1' + r_2 + b_2,\ r_2 + r_3' + b_3,\ r_3 + r_4 + b_4$--$r_{n-1} + r_n + b_n$

Now in this case the sum of each row will yield same sum and auctioneer will be convinced that auction results are not ambiguous but in reality, two bidders have cleverly colluded but to prevent such maliciousness from happening auctioneer picks an arbitrary value of k in between $[1, N)$ which we call as stepping value, and due to this arbitrary value of k the above pattern of pb_{ij} will have a different arrangement but the result of sum of a row will be same and such maliciousness will be detected. To detect the exact value of k by colluding bidder in such large sample space will not be an easy task as the number of bidders will grow the probability to detect the arbitrary value of k will become less and less. Due to this reason bidder B_1 and B_3 have to add their real random numbers each time they are asked to do so otherwise this ambiguity will not go unnoticed.

As we can see from the above expression the arrangement of submitted bids knowing the exact value of k is nearly impossible and rows will yield different sum and the ambiguity will be detected.

The threshold till where Algorithm 2 will hold true is till the number of dishonest bidders is n-2. To be examined……