Five Sealed-bid Auction Models

Kun Peng, Colin Boyd, Ed Dawson and Kapali Viswanathan

Abstract

Published sealed-bid auction schemes are classified into four models according to how they deal with bid privacy. The properties of each model are introduced and possible improvements in these models are suggested. A new model is proposed and its implementation is discussed. Application of different models is discussed, based on a comparison of the models.

1 Introduction

Sealed-bid auctions are an ideal method to distribute merchandise. In sealed-bid auctions each bidder seals his bid and submits it before a set time. After that time the bids are opened and the winning price and winner are determined according to a pre-defined auction rule. Compared to other types of auction, such as open-cry auction, sealed-bid auction is more suitable in network environment. Therefore sealed-bid auction has been attracting most attention in the research of e-auction.

In many auction applications it is desired to keep the losing bids private even at the end of the auction. This requirement is called bid privacy and is discussed in many papers. Bid privacy may have different meanings in different applications and may be implemented at different costs and on different assumptions. In this paper auction schemes are classified according to the method to implement bid privacy, so that comprehensive review of them, detailed analysis of them and possible improvements on them can be achieved.

Altogether fives models of sealed-bid auction are introduced. The first four models exist in the published schemes. The fifth model is novel and proposed by the authors to fit some certain applications. Properties and functionalities of the five models are analysed. Costs to achieve different degrees of bid privacy are compared. Possible improvements of the models are suggested.

2 Desired Properties in Sealed-bid Auction

There are several properties that are desired in an e-auction scheme. They include correctness, confidentiality, fairness, anonymity, privacy, public verifiability, robustness, price flexibility and flexibility. The first three properties are basic properties and are required in all sealed-bid e-auction schemes. The other six are optional properties and may be desired in some applications. Their definitions are as follows.

Basic properties:

1. **Correctness**: If every party acts honestly, the correct winning price and winner(s) are determined according to the auction rules.
2. **Confidentiality** (of sealed-bids): No bids are not revealed to any other parties (including the auctioneer) until the bid opening phase.
3. **Fairness** includes:
   - No bidder knows anything about other bidders' bids before he submits his own bid. This is actually included in Confidentiality.
   - After a bidder submits his bid, the bid cannot be modified.
   - No bidder can deny his bid after he submits it. This is sometimes called non-repudiation of bids.

Optional properties:

1. **Anonymity**: The identities of the bidders must be kept secret.
2. **Privacy** (of losing bids): The losing bids remain confidential until the end of the auction even to the auctioneer. Difference between privacy and confidentiality of bids includes
   - Privacy only deals with losing bids.
   - Privacy is confidentiality of the losing bids even after the bid opening phase.
3. **Public verifiability**: The validity of the result of the auction is publicly verifiable by anyone.
4. **Robustness**: Nobody is assumed to be honest and any malicious behaviour of any party cannot compromise the system or leads to an incorrect result. Robustness is a complement to correctness and guarantees that if there is a result, that result must be correct no matter what system failure or attack may occur.
5. **Price flexibility**: The bidding value should be as precise as the seller or bidders require.
6. **Rule flexibility**: What rules (e.g. first price or Vickery) are followed makes on difference for the scheme. Especially the above properties must be satisfied for Vickery auction.

The three basic properties are usually satisfied in the current auction schemes. The optional properties can be chosen to be satisfied according to the requirements of applications. It is also desired that auction schemes are efficient in both computation and communication. Usually more cost leads to better satisfaction of properties. So an appropriate trade-off between the desired properties and efficiency should be achieved.

3 Classifying and Modelling Auction Schemes

Bid privacy is a very important property. According to the manner in which bid privacy is dealt with, the published schemes are classified into four different sealed-bid auction models. In the following their principals, advantages and drawbacks are analysed.

3.1 Model 1: Plaintext Bid Auction

If bid privacy is not required, a simple model can be employed. Each bidder submits a sealed bid, which can be as precise as desired. After the bids are unsealed, they are published in plaintext and can be linked to the corresponding bidders without the cooperation of the bidders. Except for privacy and strong anonymity all the desired properties can be achieved in this model simply and efficiently. Fairness is achieved if the bid sealing is hidden and binding. There is no distinction between different auction rules and public verifiability is obviously obtained since all bids are public after unsealing phase. Anonymity is possible, but only with trust on the auctioneer or a third party, so is not strong. Bid privacy is ignored. However privacy and strong anonymity are sometimes required in many auction applications. Model 1 is illustrated in Figure 1.

Published schemes in this model include (Franklin & Reiter 1996), (Mu & Varadharajan 2000) and (Viswanathan, Boyd & Dawson 2000).

3.2 Model 2: Simple Bid-encrypted Auction

Each bidder submits an encrypted bid. Then the auctioneer decrypts all the bids and determines the result. Fairness is achieved if the bid sealing is hiding and binding. Price flexibility is permitted and any auction rules are supported. Binary search strategy can be employed to improve efficiency. The only difference with the first model is that the bids are encrypted, so that absolute bid privacy to sellers and observers can be obtained if the auctioneer is trusted. However this is quite a strong trust and thus only weak privacy is achieved. Moreover bid privacy raises a problem for public verifiability: how can an observer be convinced that the auction result is correct while the bids are secret to him. There is a solution: homomorphic encryption algorithm. But that means only a finite set of prices are biddable[1] and the scheme no longer achieves price flexibility. No strong and recoverable anonymity technique has been presented in this model so far. This model is illustrated in Figure 2.

3.3 Model 3: Threshold Bid-encrypted Auction

Model 3 employs more than one auctioneer and shares the trust needed for bid privacy among them, so that a stronger absolute privacy can be achieved than in Model 2. This is realized by sharing the bids among the auctioneers and requiring their cooperation to reconstruct the bids. Therefore a number over a threshold of bidders are trusted, which is a weaker trust. There are two implementations of this technology.

1. Secret sharing: Each bid is shared among the auctioneers. A number over a threshold of bidders can put their shares together to recover the bids.
2. Distributed decryption: Each bid is encrypted and the encrypted bid can only be decrypted by a number of auctioneers over the threshold.

This model is illustrated in Figure 3.

As in Model 2, fairness is achieved if the bid sealing is hiding and binding; rule flexibility can be satisfied; homomorphic secret sharing or homomorphic encryption can be employed to achieve public verifiability at the cost of losing price flexibility. Binary search strategy can be employed to improve efficiency. No strong and recoverable anonymity technique has been presented in this model so far.

Bid privacy in Model 3 is stronger than that in Model 2. But it is still not strong enough. Moreover, homomorphism of secret sharing and distributed decryption techniques have a side-effect—intolerant to invalid bid. Especially in k^{th} bid auction ($k > 1$), an invalid bid may compromise an auction scheme. That is why most auction schemes dealing with k^{th} bid auction (Abe & Suzuki 2002, Omote & Miyaji 2002) apply a bid validity checking function. However in all the known first bid auction schemes, bid validity checking or verification is not included. In a first bid auction scheme, if more than one malicious bidders conspire, invalid bids may also compromise the auction scheme. The lack of bid validity checking breaches robustness.

Model 3 is less efficient than Model 2 because the following additional computation is needed.

- Secure share distribution and share validity verification are needed for secret sharing solution.
- Distributed decryption and verification of its validity for distributed decryption solution are required.
- In both solutions to realize the verification protocols, more communication and computation cost are needed. Especially the verification protocol is a bottleneck in computation.
- In both solutions bid validity verification is highly costly in computation.

Several published schemes are in this model (Kikuchi, Harkavy & Tygar 1998, Kikuchi, Hotta, Abe & Nakanishi 2000, Chida, Kobayashi & Morita 2001, Kikuchi 2001, Abe & Suzuki 2002, Omote & Miyaji 2002). (Kikuchi et al. 1998, Kikuchi et al. 2000) employ standard threshold secret sharing technique. (Chida et al. 2001) employs a special $2-2$ secret shaing. (Kikuchi 2001) also employs threshold secret sharing, but uses the degree of polynomials to stand for a bid. (Abe & Suzuki 2002, Omote & Miyaji 2002) employ distributed decryption technique. (Abe & Suzuki 2002) employs standard threshold distributed decryption. (Omote & Miyaji 2002) employ onlys two auctioneers and are in fact 2-2 distributed decryption if bid decryption is defined as interpreting the meaning of bids in auction schemes.

3.4 Model 4: Dutch Style Sealed-bid Auction

Dutch style sealed-bid auction employs a totally different strategy. Like in Model 2, the bids are encrypted, but can only be opened with the cooperation of the bidders. At present, only first-bid auctions have been addressed in published schemes in this category. To protect bid privacy, the bids are opened from the highest downwards in these schemes. It is quite like the strategy in Dutch auction, so it is called Dutch style sealed-bid auction. In a first bid auction, after the winning bid is found in a downward search, cooperation from the bidders is not available. Therefore a losing bidder's bid is kept private without trust

[1] With a homomorphic encryption algorithm to encrypt the bids, the sum of bids from all bidders at a price can be obtained by directly decrypting the product of all their encrypted bids. To applying homomorphic decryption, each bidder must bid at a same set of prices.

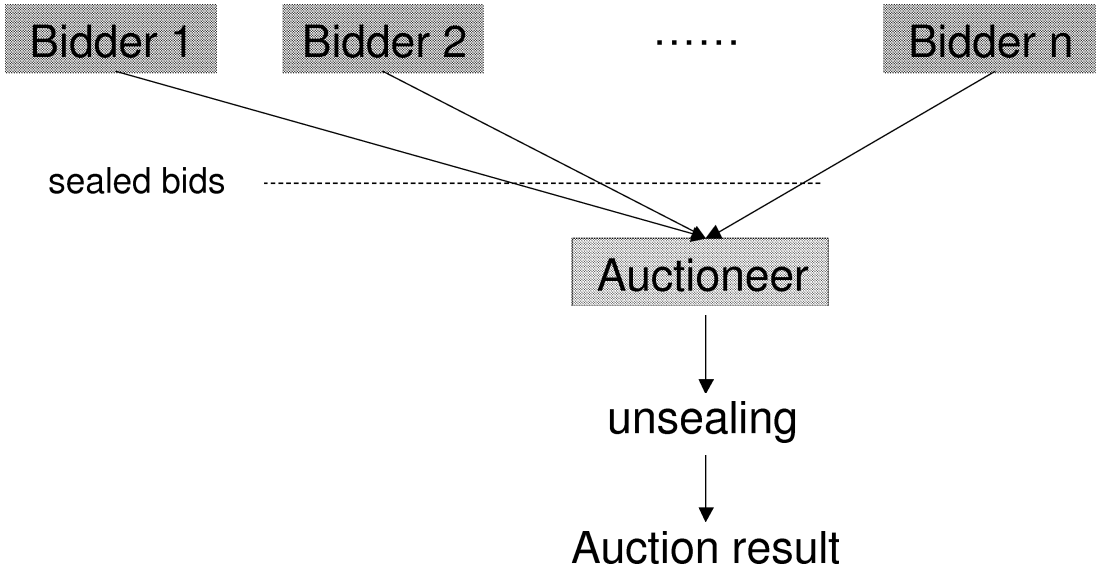

Figure 1: Plaintext Bid Auction

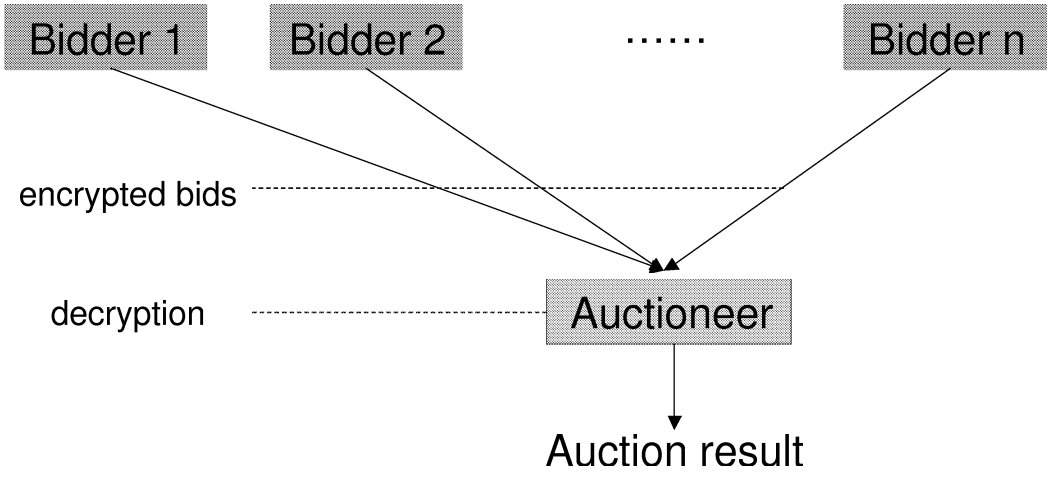

Figure 2: Simple Bid-encrypted Auction

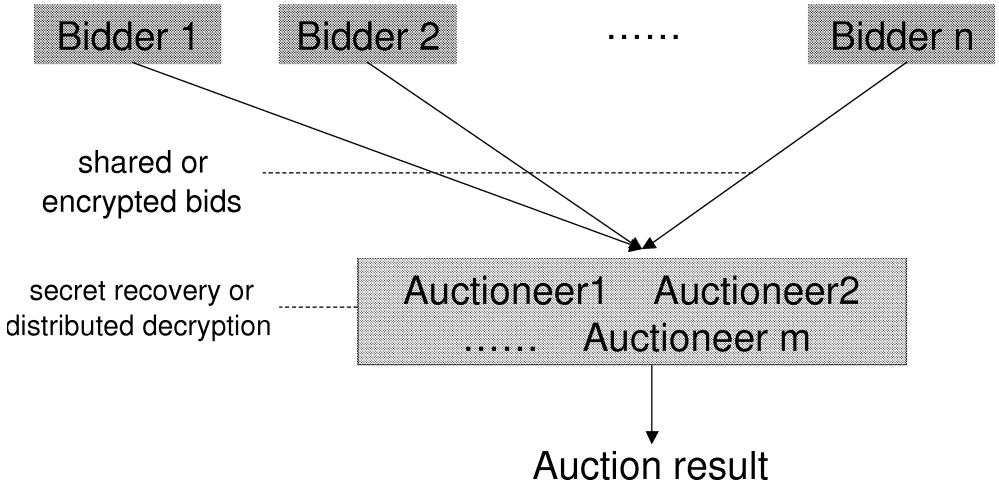

Figure 3: Threshold Bid-encrypted Auction

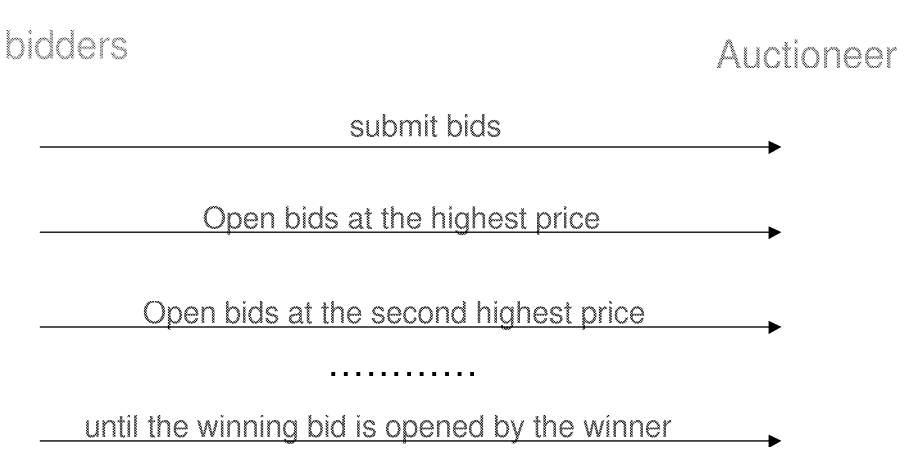

Figure 4: Dutch Style Sealed-bid Auction

on anybody else. So very strong absolute privacy is achieved. This model is illustrated in Figure 4.

Fairness is achieved if the bid sealing is hiding and binding. Published scheme in this category do not support price flexibility. No strong and recoverable anonymity technique has been presented in this model so far.

There are two different kinds of implementations of this model according to different kinds of cooperation provided by the bidders to open their bids.

1. Explicit cooperation: The bidders open their bids price by price interactively. One round of communication is needed for each biddable price no lower than the winning bid. Mature schemes have been proposed, which realize very strong absolute bid privacy. Computational efficiency can be quite high if a hash function is employed to process the bids. But the number of computation rounds is linear to the number of biddable prices, which is a high cost. Although not addressed in published research, rule flexibility should be possible if costly public key encryption is used instead of hash function in this implementation.

2. Implicit cooperation: The bidders do not take part in bid opening on-line. Instead, when submitting bids, they prepare a unique searching route (from the highest biddable price to the winning bid) for the auctioneer to follow. The computational cost is low since it is non-interactive. But costly public encryption algorithms must be employed. The number of exponentiation computations is linear to the number of biddable prices. So computational efficiency is low. No published scheme with this implementation achieves really strong bid privacy. Rule flexibility has not been achieved yet so far in this implementation.

Schemes employing explicit cooperation includes (Sakurai & Miyazaki 1999), (Sako 2000) and (Suzuki, Kobayashi & Morita 2000), while (Watanabe & Imai 2000) is a classic example of schemes employing implicit cooperation.

Model 4 achieves the strongest bid privacy. However in the only well-known non-interactive scheme (Watanabe & Imai 2000), privacy for a losing bid is obtained on the assumption that at least one bidder with higher bid or the auctioneer is trusted. So bid privacy is still based on some kind of trust in the non-interactive category in Modle 4.

3.5 Summary

Table 1 shows the best each model can achieve so far. It is easy to see that some desired properties are not satisfied. So certain auction applications cannot be realized. Therefore modifications are needed to obtain better auction schemes. The first two models are quite simple and achieves no bid privacy or very weak bid privacy. So improvement attempts are focused on Model 3 and Model 4.

In Model 3, one necessary improvement is to achieve robustness in first bid auction by bid validity checking or other mechanism. Another possible improvement is efficiency optimization.

In Model 4, one useful improvement is to remove the trust needed in the non-interactive category. Other possible improvements include price flexibility and rule flexibility.

4 A New Model

A new model is presented in this section. In this model relative bid privacy, instead of absolute bid privacy, is achieved. Anonymity is also achieved in this model.

4.1 Absolute Privacy and Relative Privacy

There are usually two motivations for bid privacy.

1. To protect the personal privacy of bidders. The losing bidders may hope to keep their behaviour unknown. So it is must be impossible to link the identities of bidders to their bids.

2. To conceal the losing bids from the auctioneer or seller so that the seller cannot take advantage of information when selling identical or similar items in some later time.

If both motivations exist, all the losing bids must be kept secret from anybody except the corresponding bidders. This kind of privacy is called absolute privacy. However we feel the first motivation is more common and widely desired. If in some circumstances the second motivation is not involved, it is only necessary to make the losing bids unlinkable to the corresponding bidders. This kind of privacy is called relative privacy and it may not protect the confidentiality of the losing bids after the bidding phase. It is more flexible to achieve relative privacy.

	Model 1	Model 2	Model 3	Model 4 Interactive	Model 4 Non-interactive
Correctness	Yes	Yes	Yes	Yes	Yes
Confidentiality	Yes	Yes	Yes	Yes	Yes
Fairness	Yes	Yes	Yes	Yes	Yes
Anonymity	Absolute Weak Recoverable	Absolute Weak Recoverable	Absolute Weak Recoverable	Absolute Weak Recoverable	Absolute Weak Recoverable
Privacy	No No	Absolute Very Weak	Absolute Medium	Absolute Unconditional	Absolute Weak
Public Verifiability	Yes	Yes	Yes	Yes	Yes
Robustness	Yes	Yes	No	yes	yes
Pricesness	Yes	No	No	No	No
Rule flexibility	Yes	Yes	Yes	No	No
Computation Efficiency	High	High	Medium	High	Low
Communication Efficiency	High	High	Medium	Low	High

Table 1: Properties and Efficiency

4.2 Model 5: Untraceable Auction

Modle 5 is a new model only achieving relative bid privacy. In that model the bids are submitted anonymously and become in plaintext after being unsealed. Anonymity can be implemented by pseudonyms generated by blind signature techniques. Namely at the beginning the bidders must register at a registration authority and get blind sigatures, from which their pseudonyms can be extracted. The bids must be submitted through an anonymous channel, which can be implemented by the mix network proposed by Chaum (**?**).

In Model 5, the unlinkability between losing bidders and their bids is achieved, assuming all the other bidders do not collude. Therefore relative privacy is always achieved in this model with a weak trust assumption. This model is illustrated in Figure 5.

4.3 Strong and Recoverable Relative Bid Privacy

To achieve strong relative privacy, the bids should be untraceable with weak trust. At the same time the scheme must provide non-repudiation, thus the winner must not be able to deny his bid. After the winning bid is found the winner is required to claim it. If he refuses to cooperate, there must be a bid privacy recovery mechanism to be applied to identify him. So the relative bid privacy must be strong and recoverable at the same time.

In all the previous schemes with bid privacy recovery, a third party (e.g. a registration authority) is trusted to recover bid privacy when the winner tries to deny his bid. The drawback of this solution is that relative bid privacy is only achieved with a trust on that third party. It is a quite strong assumption and leads to weak bid privacy.

Another solution is the registration authority and all the losing bidders cooperate to identify the dishonest winner by publishing their secrets. Namely every innocent bidder reveals his identity, indicates and proves which bid belongs to him and the registration authority publishes the list of identities of all the bidders. The bidder unable to prove his innocence is the cheater. This method is straightforward, but compromises anonymity and bid privacy completely when there is a dishonest winner, thus is not practical.

Here there is in fact a dilemma: strong (for honest bidder) and recoverable (for dishonest bidder) bid privacy. If a finite group of bidders are involved in an auction, it is desired:

1. Bids of honest bidders are untraceable with a weak assumption.
2. Malicious behaviors can be traced and linked to the identities of the bidders performing them.

At the same time anonymity is desired.

Our solution requirs each bidder to use two public keys. One is a long-term public key, which is based on PKI. Before being permitted to join, each bidder must register at a registration authority using verified identities. When registering, each bidder authenticates himself using the long-term private key and provides a short-term public key (signed using his long-term private key) so that the registration authority can link the short-term public keys to the true identities. As a result of successful registration, a bidder obtains a pseudonym from the registration authority. The pseudonym is extracted from a blind signature of the registration authority so that it is untraceable on its own. Each bidder submits his bid using his pseudonym. Each bidder's behaviour is labeled by his signature using his short-term private key. The signature algorithm is some kind of undeniable signature and signature verification needs cooperation of the signer. So neither the pseudonym nor the signature reveals any information about the bidder's identity. Namely the link between a bid to the short-term public key of the corresponding bidder is hidden. After the registration phase the registration authority publishes all the short-term public keys and keeps the bidders' identities secret. The untraceability for honest participants' behaviours is achieved based on the trust of all the other parties as a whole (at least one of them does not take part in a collusion). This is a weak trust, so a strong bid privacy is achieved.

It needs the cooperation of all the innocent bidders and the registration authority to identify a cheating bidder. However the innocent bidders need not reveal their bids in this course. When the winner refuses to claim the winning bid, each bidder is required to prove he submits a losing bid in a zero-knowlege way using a 1_out_of_n verification protocol[1]. After all the innocent bidders prove their innocence, the short-term public key unlinkable to any losing bids belongs to

[1]Each participant must prove one losing bid is labeled by his short-term signature without indicating which bid belongs to him

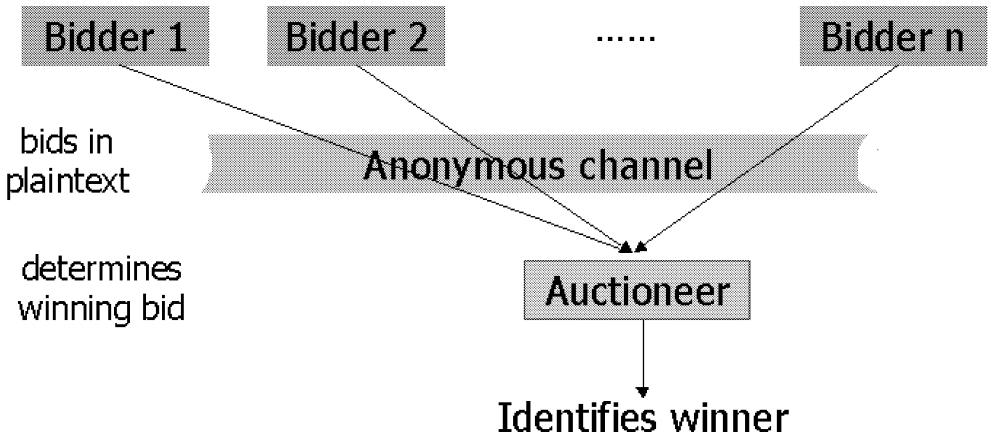

Figure 5: Untraceable Auction

the cheating winner. The registration authority can link this short-term public key to its owner's identity and verify anybody this link since its owner's long-term signature on his short-term public key can be published. In this method this cheating winner is recovered by the cooperation of all the other bidders and the registration authority in a zero knowledge way. Therefore strong bid privacy for honest bidders and recoverable bid privacy of dishonest bidder are achieved at the same time.

If the registration authority is honest, anonymity of the bidders can be achieved. If a dishonest winner appears but all the bidders can prove their innocense, the registration authority is accused of distributing more than one pseudonyms to the winner.

The drawback of this technique is when the number of bidders involved is great, it is quite inefficient to recover bid privacy. For example if there are n bidders, the computation cost is $O(n^2)$ exponentiations. Fortunately the identified cheater can be punished severely, which can discourage the bidders from cheating. So usually the recovery operation is avoided.

This method is illustrated in Figure 6.

4.4 Properties of Model 5

In Model 5 all the bids are in plaintext after being unsealed, so correctness, robustness and rule flexibility are achieved. If an appropriate sealing function is employed (e.g. secure hash function), it is fair. Relative bid privacy is achieved if at least one partipant of the auction (a bidder or the registration authority) is honest and the anonymous channel is secure (at least one server in the mixed network is honest). So only weak trust is needed. the auction itself is quite efficienct. Although the mixed network costs some computation, it is still efficient compared to Model 3 (with bid validity verification to achieve robustness) or Model 4. However it still has the following shortcomings.

1. Absolute privacy is not achieved.
2. Anonymity is based on the trust on the registration authority.
3. The bids must be submitted through an anonymous channel. Usage of anonymous channel may compromise the high efficiency.

So improvements are needed in Model 5. For example absolute privacy may be implemented by mixing the true bids with some dummy bids.

5 Conclusion

Four models are set up in the existing schemes and Model 5, a new model has been proposed. Table 2 shows what has been achieved. It can be noted that in this table the only negative item is the low communication efficiency of interactive schemes in Model 4. It is inevitable since low communication efficiency is a direct result of interactive solution. Future work can be performed in the following directions.

1. Optimizing Model 5 to achieve absolute bid privacy and ruls flexibility.
2. Extending batch verification to improve the efficiency of verification of distributed decryption in Model 3.
3. Exploring possible new models.

References

Abe, M. & Suzuki, K. (2002), M+1-st price auction using homomorphic encryption, *in* 'PKC 2002', pp. 115–124.

Chida, K., Kobayashi, K. & Morita, H. (2001), Efficient sealed-bid auctions for massive numbers of bidders with lump comparison, *in* 'LNCS 2200', p. 48.

Franklin, M. K. & Reiter, M. K. (1996), 'The design and implementation of a secure auction service', *IEEE Transactions on Software Engineering* **22**(5), 302–312.

Kikuchi, H. (2001), (m+1)st-price auction, *in* 'Proc. of The Fifth International Conference on Financial Cryptography '01, IFCA', pp. 291–298.

Kikuchi, H., Harkavy, M. & Tygar, J. D. (1998), Multi-round anonymous auction, *in* 'Proceedings of the First IEEE Workshop on Dependable and Real-Time E-Commerce Systems', pp. 62–69.

Kikuchi, H., Hotta, S., Abe, K. & Nakanishi, S. (2000), Distributed auction servers resolving winner and winning bid without revealing privacy of bids, *in* 'proc. of International Workshop on Next Generation Internet (NGITA2000), IEEE', pp. 307–312.

Mu, Y. & Varadharajan, V. (2000), An internet anonymous auction scheme, *in* 'LNCS 2015', ISISC 2000, p. 171.

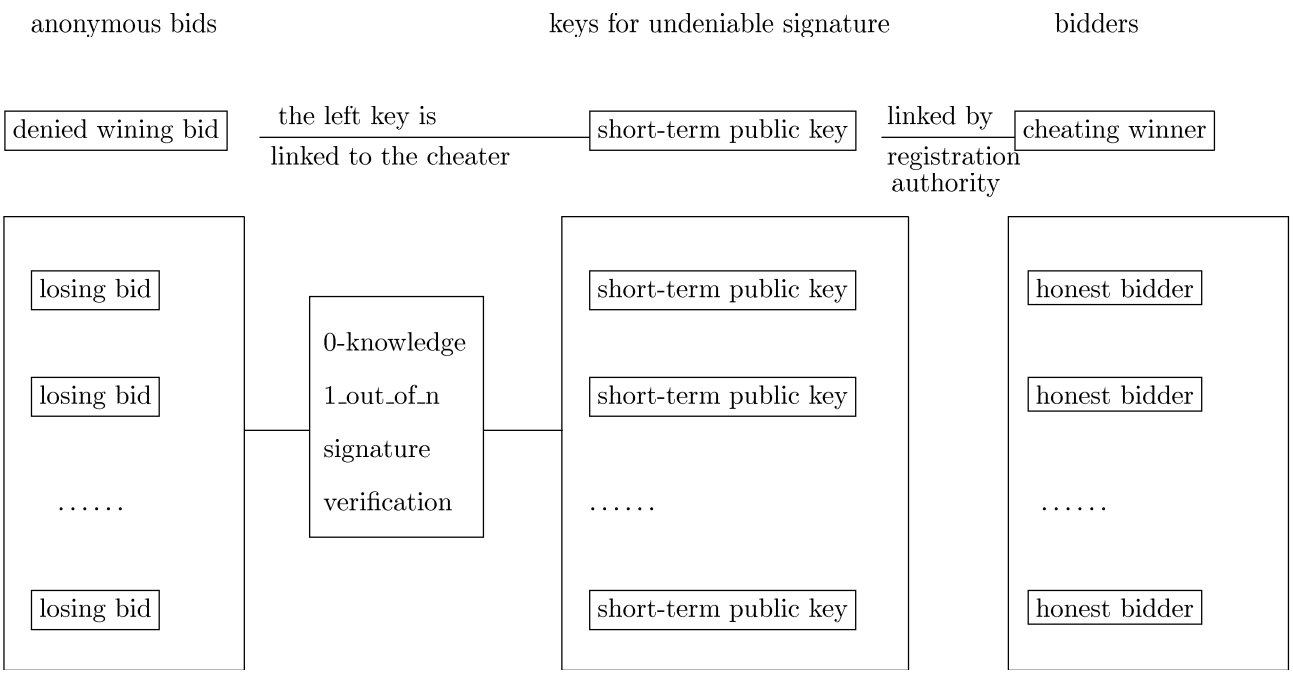

Figure 6: Strong and recoverable bid privacy

	Model 3	Model 4 Interactive	Model 4 Non-interactive	Model 5
Correctness	Yes	Yes	Yes	Yes
Confidentiality	Yes	Yes	Yes	Yes
Fairness	Yes	Yes	Yes	Yes
Anonymity	Strong Recoverable	Strong Recoverable	Strong Recoverable	Relative Strong Recoverable
Privacy	Absolute Medium	Absolute Unconditional	Absolute Unconditional	Absolute Strong
Public Verifiability	Yes	Yes	Yes	Yes
Robustness	Yes	Yes	Yes	Yes
Price Flexibility	No	Yes	Yes	Yes
Rule flexibility	Yes	No	Yes	Yes
Computation Efficiency	High	High	Improved	High
Communication Efficiency	Medium	Low	High	High

Table 2: Improvement

Omote, K. & Miyaji, A. (2002), A second-price sealed-bid auction with the discriminant of the p-th root, *in* 'Financial Cryptography 2002'.

Sako, K. (2000), An auction scheme which hides the bids of losers, *in* 'Public Key Cryptology, PKC'2000, Springer', pp. 422–432.

Sakurai, K. & Miyazaki, S. (1999), A bulletin-board based digital auction scheme with bidding down strategy -towards anonymous electronic bidding without anonymous channels nor trusted centers, *in* 'Proc. International Workshop on Cryptographic Techniques and E-Commerce', City University of Hong Kong Press, pp. 180–187.

Suzuki, K., Kobayashi, K. & Morita, H. (2000), Efficient sealed-bid auction using hash chain, *in* 'ICISC 2000, LNCS 2015', pp. 183–191.

Viswanathan, K., Boyd, C. & Dawson, E. (2000), A three phased schema for sealed bid auction system design, *in* 'ACISP'2000', Springer-Verlag, pp. 412–426.

Watanabe, Y. & Imai, H. (2000), Reducing the round complexity of a sealed-bid auction protocol with an off-line ttp, *in* 'ACM STOC 2000', ACM, pp. 80–86.