

Five Sealed-bid Auction Models

Kun Peng, Colin Boyd, Ed Dawson and Kapali Viswanathan

Information Security Research Centre
Faculty of Information Technology
Queensland University of Technology,
2, George Street, Brisbane, QLD4001, Australia,
Email: k.peng, c.boyd, e.dawson, k.viswanathan@qut.edu.au

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 five 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 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 revealed to any 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 losing 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. Differences between privacy and confidentiality of bids include
 - 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 lead 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 values of the bids can be as precise as the seller or bidders require¹.
6. **Rule flexibility:** The choice of rules (e.g. first price or Vickery) makes no difference for the scheme. Especially the above properties must be satisfied for Vickery auction.

Copyright ©2003, Australian Computer Society, Inc. This paper is appeared at the Australasian Information Security Workshop (AISW2003), Adelaide, Australia. Conferences in Research and Practice in Information Technology, Vol. 21. C. Johnson, P. Montague and C. Steketee, Eds. Reproduction for academic, not-for profit purposes permitted provided this text is included.

¹Many auction schemes not only set a minimum and a maximum threshold for biddable prices, but also set a limited number of biddable prices. Price flexibility means any price between the minimum and maximum threshold is biddable

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. In regard to this property, auction schemes are classified in this section. Some auction schemes require each bidder to submit only one bid. This category of schemes are usually simple and efficient. Especially they support price flexibility. However they achieve weak or even no bid privacy. Model 1 and Model 2 below are in this category. Other schemes accept only a finite set of biddable prices and require each bidder to submit a bid at every biddable price. Auction schemes in this category are more complex and inefficient, but achieve stronger bid privacy. Model 3 and Model 4 below are in the second category.

Before introducing the models, the meaning of “sealing” is explained. Sealing is a function used to achieve confidentiality and privacy. Usually, there are two kinds of sealing.

1. Hash function sealing: Initially, a commitment for each bid is generated by a one-way and collision-resistant hash function. Each bidder first publishes his commitment of bid. After all the bidders have published their commitments, each bidder submits his bid (in plaintext or encrypted). This method aims to realize bid confidentiality and thus fairness—it is impossible for any bidder to know the bids of other bidders when his bid is committed no matter whether the bids are encrypted or not. Note that hash function is much more efficient than public-key encryption algorithm.
2. Encryption sealing: The bids are encrypted when submitted. Usually public-key encryption algorithms are employed. This method is usually employed to implement bid privacy. In the opening phase, only necessary decryptions are performed and the all the bids except the winning bid remain encrypted at the end of auction.

The role of hash function is not recognised in many auction schemes and encryption sealing is thought to be able to implement fairness and bid privacy. However bid confidentiality or bid privacy achieved by encryption is often conditional—trust on some auctioneer or third party is assumed while bid confidentiality and fairness achieved by hash function sealing is only based on the strength of the hash function. So hash function sealing is necessary to achieve strong bid confidentiality and fairness in some applications. Among the five models described in this section, Model 1 and Model 5 only employ hash function sealing, Model 4 employs only encryption sealing while Model 2 and Model 3 employ both types of sealing.

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 hash-sealed bid, which can be as precise as desired. After the bids are unsealed by the bidders, 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 uses a hiding and binding operation². 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 (Mu & Varadharajan 2000) and (Viswanathan, Boyd & Dawson 2000).

3.2 Model 2: Simple Bid-encrypted Auction

In Model 2, each bidder first commits his encrypted bid by a hash function. After all the commitments are published, the bidders submit their encrypted bids to one or more auctioneers. Then the auctioneer(s) decrypts all the bids and determines the result. As explained in Model 1, fairness is achieved if the hash function sealing uses hiding and binding operation. Price flexibility is permitted and any auction rules are supported. In the opening phase. 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 every auctioneer is trusted. However this involves quite a strong trust relationship and thus only weak privacy is achieved.

A frequently quoted scheme by Franklin and Reiter (Franklin & Reiter 1996) is in this category, in which threshold secret sharing is employed for several auctioneers to open all the bids. If the decrypted losing bids are published by the auctioneers, public verifiability is achieved, but bid privacy is lost. If the auctioneers keep the losing bids secret and each of them is trusted, absolute bid privacy is achieved. But it is achieved on a very strong assumption (no auctioneer reveals the losing bids) and at the cost of losing public verifiability.

To achieve bid privacy and public verifiability simultaneously, a question must be answered: how can an observer be convinced that the auction result is correct while the bids are secret to him. This leads to Model 3.

3.3 Model 3: Threshold Bid-encrypted Auction

Model 3 is upgraded from Model 2 and the only difference is that Model 3 employs homomorphic encryption and shares the trust needed for bid privacy among several auctioneers, so that a stronger absolute privacy can be achieved than in Model 2, while public verifiability can also be obtained. Adopting homomorphic encryption algorithm means only a finite set of prices are biddable and each bidder must

²Here bid sealing is realized by a hash function. Hiding means no information about the bids is revealed from the commitment, so that no bidder has any knowledge about other bidders' bids when he submits the commitment. Binding means no bidder can find two different bids with the same commitment. Obviously these two requirements can be obtained if the hash function is one way and collision-resistant.

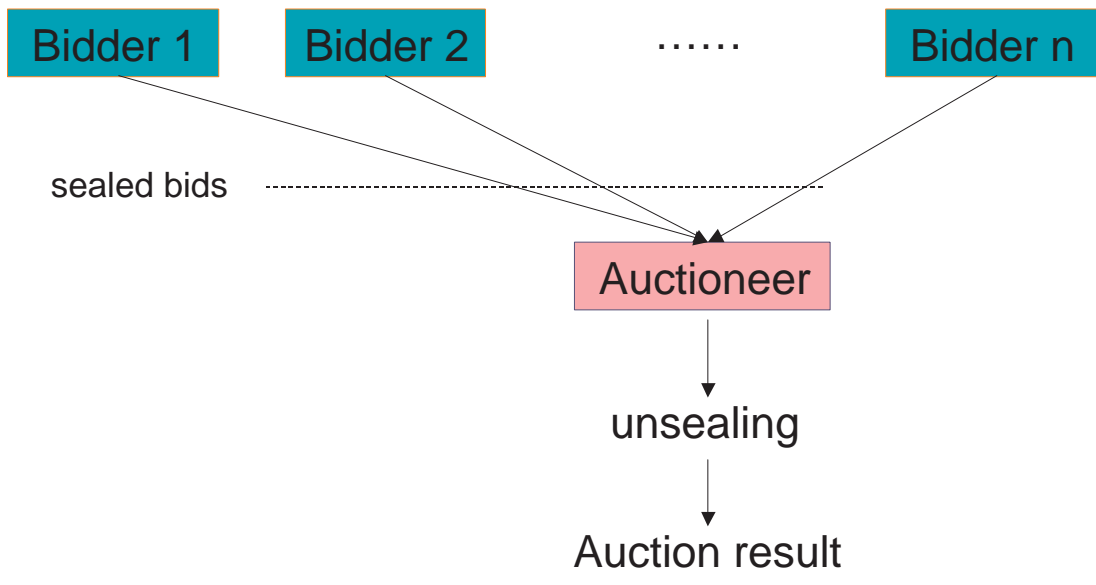


Figure 1: Plaintext Bid Auction

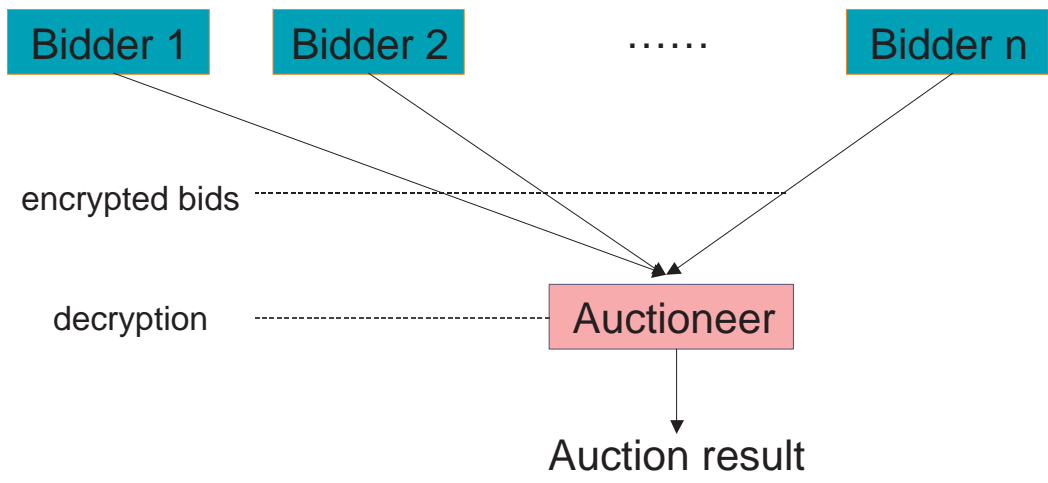


Figure 2: Simple Bid-encrypted Auction

submits a bid at every biddable price³ and the scheme no longer achieves price flexibility. Each bid is shared among the auctioneers and requiring their cooperation to reconstruct the bids. Therefore a number over a threshold of auctioneers 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 auctioneers 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, both types of sealing are used; fairness is achieved if the hash function sealing uses hiding and binding operation; 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. In the opening phase binary search strategy can be employed by the auctioneer to search for the winning bid. 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 for $k > 1^4$, 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, verification of bid validity is not included. In a first bid auction scheme, if more than one malicious bidder collude, invalid bids may also compromise the auction scheme. The lack of bid validity check breaches robustness.

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

- Secure share distribution and share validity verification are needed for secret sharing solution.
- Distributed decryption and verification of decryption validity in 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 sharing. (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) employs only two auctioneers and is 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 from Model 3, although again a finite set of biddable prices are accepted. In this model only encryption sealing is used. However the encrypted bids 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 by performing a downward search, cooperation of the bidders is not available. Therefore a losing bidder's bid is kept private without trust on anybody else. So very strong absolute privacy is achieved. This model is illustrated in Figure 4.

Fairness is achieved if the encryption algorithm is a hiding and binding operation. Published schemes 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 in that scheme bid privacy is still based on some kind of trust in the non-interactive category in Model 4.

³With a homomorphic encryption algorithm (e.g. the homomorphic encryption algorithm by Paillier (Paillier 1999)) 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.

⁴In an k^{th} bid auction, the bidder with the highest bid wins, and he pays the k^{th} highest bid for the goods.

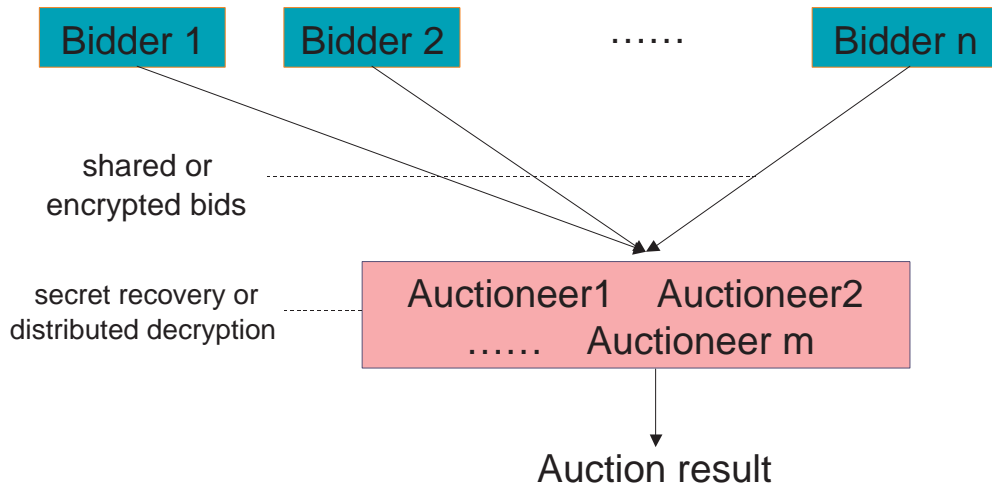


Figure 3: Threshold Bid-encrypted Auction

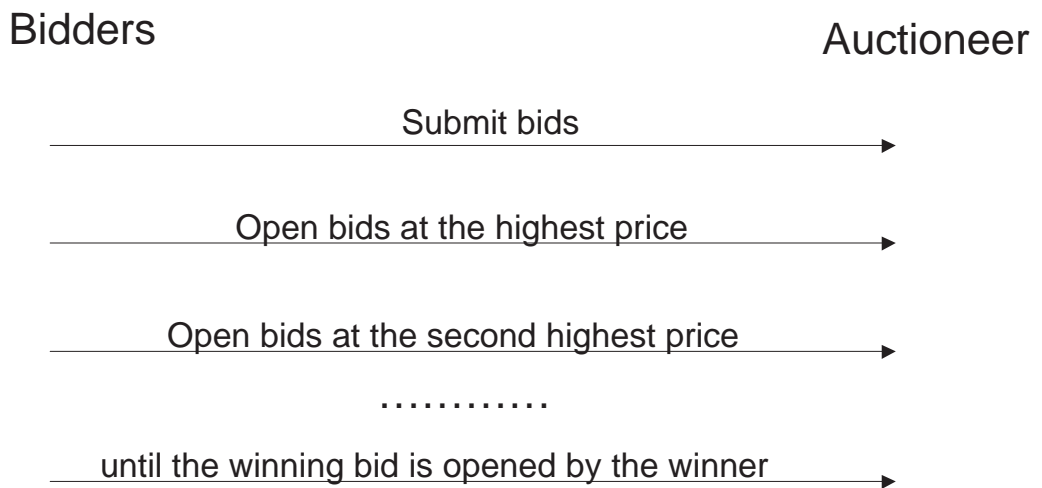


Figure 4: Dutch Style Sealed-bid Auction

A new scheme was proposed by Peng *et al* (Peng, Boyd, Dawson & Viswanathan 2002), which overcomes this requirement and achieves strong bid privacy non-interactively.

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 achieve 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 optimisation.

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.

4.2 Model 5: Untraceable Auction

Model 5 is a new model only achieving relative bid privacy. In this model, each bidder only need to submit one bid. Only hash function sealing is employed. The bids are submitted anonymously after their commitments are published and become in plaintext after being unsealed by the bidders. 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 signatures, 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 (Chaum 1981).

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

At the same time anonymity is desired.

Our solution requires 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 (e.g. Chaum's blind RSA signature scheme (Chaum & Pedersen 1992)) 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 labelled by his signature generated with 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 strong bid privacy is achieved.

	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	Absolute Very Weak	Absolute Medium	Absolute Unconditional	Absolute Weak
Public Verifiability	Yes	No	Yes	Yes	Yes
Robustness	Yes	Yes	No	yes	yes
Price Flexibility	Yes	Yes	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

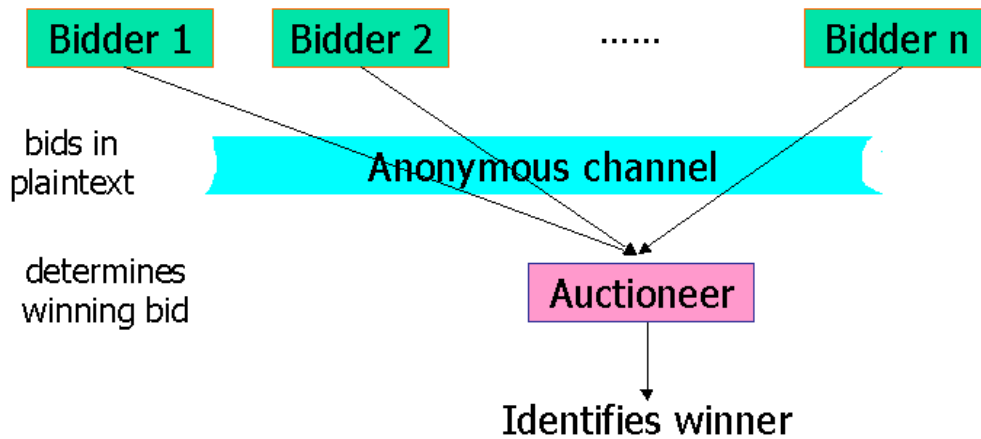


Figure 5: Untraceable Auction

In the case where the winner refuses to claim the winning bid, the cooperation of all the innocent bidders and the registration authority is needed to identify this person. However the innocent bidders need not reveal their own bids in order to do this. The solution for this problem is for each bidder to prove he submits a losing bid in a zero-knowledge way using a *1 out of n* verification protocol⁵. After all the innocent bidders prove their innocence, the short-term public key unlinkable to any losing bids belongs to the cheating winner. The registration authority can link this short-term public key to its owner's identity and verify to anybody the validity of this link since its owner's long-term signature on his short-term public key can be published. In this fashion, the cheating winner is recovered by the cooperation of all the other bidders and the registration authority while the losing bids are still kept secret. Therefore strong bid privacy for honest bidders and recoverable bid privacy of dishonest winner 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 innocence, the registration authority is accused of distributing more than one pseudonym to the winner.

The drawback of this technique is when the number of bidders involved is large, it is quite inefficient to recover bid privacy. For example if there are n bidders, the computation cost is $O(n^2)$ exponentiations. Since the cheater can be identified, 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 a hiding and binding hash function is employed to seal the bids, it is fair.

Relative bid privacy of a losing bidder is achieved if at least one other participant of the auction (a co-bidder or the registration authority) is honest, the blind signature protocol is secure (no information about a message is revealed from its blind signature) and the anonymous channel is secure (at least one server in the mixed network is honest). This is due to the following reasons.

- If the blind signature protocol is secure (it is impossible for the signer to recover the signed message), the pseudonyms cannot be linked to the bidders.
- If the anonymous channel is secure (the identity of the sender is unknown to the receiver), the bids cannot be traced through the channel.
- Therefore the only feasible attack to bid privacy of a bidder is
 1. all the other bidders collude to identify the anonymous bid belonging to the attacked bidder (e.g. they can prove in a zero knowledge way that each of their bids is one of the other bids);
 2. the registration authority publishes a list containing all the bidders' identities;

⁵Each participant must prove one losing bid is labelled by his short-term signature without indicating which bid belongs to him. This is in fact a *1 out of n* verification of equality of logarithms if the undeniable signature scheme by M Michels and M Stadler (Michels & Stadler 1997) is employed to label the bids. Implementation of *1 out of n* verification of equality of logarithms is based on paper by Cramer *et al* (Cramer, Damgård & Schoenmakers 1994), in which a protocol for *1 out of n* verification of knowledge is provided.

3. the identified bid must belong to the only bidder who is in the list and does not take part in the collusion.

So only weak trust is needed. The auction itself is quite efficient. 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 future improvements are needed in Model 5.

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. Model 5 can be optimised to achieve absolute bid privacy and rule flexibility.
2. Extend batch verification to improve the efficiency of verification of distributed decryption in Model 3.
3. Explore possible new models.

References

- Abe, M. & Suzuki, K. (2002), M+1-st price auction using homomorphic encryption, *in* 'Public Key Cryptology 2002', Springer-Verlag, Berlin, pp. 115–124. Lecture Notes in Computer Science Volume 2288.
- Chaum, D. (1981), Untraceable electronic mail, return address and digital pseudonym, *in* 'Communications of the ACM, 24(2)', pp. 84–88.
- Chaum, D. & Pedersen, T. P. (1992), Wallet databases with observers, *in* E. F. Brickell, ed., 'Advances in Cryptology - Crypto '92', Springer-Verlag, Berlin, pp. 89–105. Lecture Notes in Computer Science Volume 740.
- Chida, K., Kobayashi, K. & Morita, H. (2001), Efficient sealed-bid auctions for massive numbers of bidders with lump comparison, *in* 'Information Security, 4th International Conference, ISC 2001', Springer-Verlag, Berlin, pp. 408–419. Lecture Notes in Computer Science Volume 2200.
- Cramer, R., Damgård, I. B. & Schoenmakers, B. (1994), Proofs of partial knowledge and simplified design of witness hiding protocols, *in* Y. Desmedt, ed., 'Advances in Cryptology - Crypto '94', Springer-Verlag, Berlin, pp. 174–187. Lecture Notes in Computer Science Volume 839.
- Franklin, M. K. & Reiter, M. K. (1996), The design and implementation of a secure auction service, *in* 'IEEE Transactions on Software Engineering', Vol. 5, pp. 302–312.

- Kikuchi, H. (2001), $(m+1)$ st-price auction, *in* 'The Fifth International Conference on Financial Cryptography 2001', Springer-Verlag, Berlin, pp. 291–298. Lecture Notes in Computer Science Volume 2339.
- 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.
- Michels, M. & Stadler, M. (1997), Efficient convertible undeniable signature schemes, *in* '4th Annual Workshop on Selected Areas in Cryptology', pp. 231–244.
- Mu, Y. & Varadharajan, V. (2000), An internet anonymous auction scheme, *in* 'International Conference on Information Security and Cryptology 2000', Springer-Verlag, Berlin, pp. 171–182. Lecture Notes in Computer Science Volume 2015.
- Omote, K. & Miyaji, A. (2002), A second-price sealed-bid auction with the discriminant of the p -th root, *in* 'Financial Cryptography 2002', Springer-Verlag, Berlin.
- Paillier, P. (1999), Public key cryptosystem based on composite degree residuosity classes, *in* 'Eurocrypt'99', Springer-Verlag, Berlin, pp. 223–238. Lecture Notes in Computer Science Volume 1592.
- Peng, K., Boyd, C., Dawson, E. & Viswanathan, K. (2002), A non-interactive auction scheme with strong privacy, Springer-Verlag, Berlin. To appear in the proceedings of International Conference on Information Security and Cryptology 2002.
- Sako, K. (2000), An auction scheme which hides the bids of losers, *in* 'Public Key Cryptology 2000', Springer-Verlag, Berlin, pp. 422–432. Lecture Notes in Computer Science Volume 1880.
- 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, Hong Kong, pp. 180–187.
- Suzuki, K., Kobayashi, K. & Morita, H. (2000), Efficient sealed-bid auction using hash chain, *in* 'International Conference on Information Security and Cryptology 2000', Springer-Verlag, Berlin, pp. 183–191. Lecture Notes in Computer Science 2015.
- Viswanathan, K., Boyd, C. & Dawson, E. (2000), A three phased schema for sealed bid auction system design, *in* 'Information Security and Privacy, 5th Australasian Conference, ACISP'2000', Springer-Verlag, Berlin, pp. 412–426. Lecture Notes in Computer Science 1841.
- Watanabe, Y. & Imai, H. (2000), Reducing the round complexity of a sealed-bid auction protocol with an off-line ttp, *in* 'STOC 2000', ACM, pp. 80–86.