# Security and Privacy of Online Sealed Bid Auction

Amita Chakraborty
Assistant Professor
Department of CSE
Shaikh Burhanuddin College, Dhaka, Bangladesh.

Md. Golam Moazzam
Associate Professor
Department of CSE
Jahangirnagar University
Savar, Dhaka-1342, Bangladesh.

Md. Nazrul Islam
PhD Student
Department of CSE
Jahangirnagar University
Savar, Dhaka-1342, Bangladesh.

Mohammad Zahidur Rahman, PhD.
Professor
Department of CSE
Jahangirnagar University, Savar, Dhaka-1342, Bangladesh.

## ABSTRACT
This paper provides a robust method for solving the question of security and privacy of online sealed bid auction. The Internet is now playing an important role in changing how we interact with other people and how we do business today. As a result of the internet, Electronic commerce allows business to more effectively interact with their customers. The challenges that oppose electronic communication are concern of security and privacy of information. This paper will first discuss online sealed bid auction. Secondly it will talk about the concerns about security and privacy issue.

## Keywords
Internet, E-commerce, Online auction, Online sealed bid auction, Security and privacy.

## 1. INTRODUCTION
An auction is a process of buying and selling goods or services by offering them up for bid, taking bids, and then selling the item to the highest bidder. In economic theory, an auction may refer to any mechanism or set of trading rules for exchange [1].

There are several variations on the basic auction form, including time limits, minimum or maximum limits on bid prices, and special rules for determining the winning bidder(s) and sale price(s). Participants in an auction may or may not know the identities or actions of other participants [2], [3]. Depending on the auction, bidders may participate in person or remotely through a variety of means, including telephone and the internet. The seller usually pays a commission to the auctioneer or auction company based on a percentage of the final sale price.

The players in an auction include [4], [5]:

- Seller, who has one or more items (also called goods) to sell;
- The bidder who submit the bid;
- Auctioneer, who acts on behalf of the seller to determine a winning price (clearing price) and a bidder as the winner.
- Winner, the bidder chosen by the auctioneer(s) to pay the seller the clearing price and get the goods.

## 2. SEALED BID AUCTION

### 2.1 Sealed First-price Auction
Sealed first-price auction also known as a First-Price Sealed-Bid Auction (FPSB). In this type of auction all bidders simultaneously submit sealed bids so that no bidder knows the bid of any other participant. The highest bidder pays the price they submitted. This type of auction is distinct from the English auction, in that bidders can only submit one bid each. Furthermore, as bidders cannot see the bids of other participants they cannot adjust their own bids accordingly. This kind of bid produces the same outcome as Dutch auction. Sealed first-price auctions are commonly used in tendering, particularly for government contracts and auctions for mining leases [6].

### 2.2 Vickrey Auction
Vickrey auction also known as a sealed-bid second-price auction. This is identical to the sealed first-price auction except that the winning bidder pays the second highest bid rather than their own. This is very similar to the proxy bidding system used by eBay, where the winner pays the second highest bid plus a bidding increment (e.g., 10%). In a network environment, sealed-bid auction is preferred not only because of its convenience and quickness but also because of its potential ability to protect bid confidentiality and bidders' privacy [7].

Two kinds of models are discussed here to be understandable our proposed model.

***Model 1: Auction with Simple Encryption***

In Model 1, each bidder submits his encrypted bid to one or more auctioneers. Then the auctioneer(s) decrypts all the bids and determines the result. Price flexibility is permitted and any auction rules are supported. In the bid opening phase, absolute bid privacy to the seller and observers can be obtained if the auctioneer is trusted and public verification of his operation is not required. However, this involves quite a strong trust and thus only weak privacy is achieved. Confidentiality and fairness in this model is based on the trust on the auctioneer(s) [8], [9].

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.

### *Model 2: Auction with Homomorphic Bid-Opening*

Model 2 is designed to achieve absolute bid privacy and public verifiability simultaneously. The only difference from Model 1 is that Model 2 employs homomorphic bid opening, so that absolute privacy and public verifiability can be achieved. Adopting homomorphic bid opening means that each bidder must submit a bid at every biddable price. For the sake of acceptable computation and communication cost, the number of biddable prices cannot be very large. That means price flexibility cannot be achieved and the schemes in this model cannot be applied to accurate auction applications. Each bid is shared among the auctioneers, who can cooperate to recover the bids. However, they do not recover any single bid. Instead, they recover the sums of all the bids at a number of biddable prices on a searching route. Usually, binary search is employed and the number of prices on the searching route is the 2-base logarithm of the number of biddable prices. Therefore a publicly verifiable auction result can be determined without revealing the bids A number over a threshold of auctioneers are trusted, which is weak trust. Confidentiality and fairness in this model is based on the trust on the auctioneer(s). There are two implementations of this technology [7], [10].

**I.** Secret sharing: Each bid is shared among the auctioneers. A number over a threshold of auctioneers can put their shares together to recover the sums of bids.

**II.** Distributed decryption: Each bid is encrypted and the sums of bid can only be recovered by threshold decryption involving a number of auctioneers over the threshold.

In this model 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.Bid privacy in Model 2 is strong (stronger than that in Model 1).

Although no current first bid auction schemes adopt bid validity verification in their auction protocols, it is necessary in first bid auction if more than one bidder may conspire.

## 3. PROPOSED ONLINE SEALED BID AUCTION

Secure and practical sealed-bid auction is a useful cryptographic application and its requirements for security and efficiency are challenging. Especially, it is not easy to achieve strong and absolute bid privacy efficiently. Various auction schemes have been designed to satisfy different requirements and suit different applications. The name of our proposed auction for online sealed-bid auction is Online Sealed Bid Auction (OSBA). It is based on Model 1 and Model 2. The architecture is shown in Fig. 1.

Like as Model 1 each bidder submits his/her encrypted bid to one auctioneer. Then like Model 2 each encrypted bid is shared among the n file servers through auctioneer. The auction server can cooperate to recover the bids. The auction server can recover the bid of every bidder. To find out the winning bid (max value) a simple algorithm FindMaxValue can be applied. Therefore, a publicly verifiable auction result can be determined without revealing the bids. Like Model 1 price flexibility is permitted and any auction rules are supported.

As a bid from a bidder is distributed among n file servers there is an n-point of failure and the advantage is that for a intruder to know the actual bid, n shared encrypted bid are needed from n file servers.

As a bid from a bidder is distributed among n file servers there is an n-point of failure and the advantage is that for a intruder to know the actual bid, n shared encrypted bid are needed from n file servers.

Confidentiality and fairness in this model is based on the trust on the auctioneer and Registration Server which is acts as a TTP. During the bid opening phase if auction server or any file server flips the bid, then trusted party can detect it.

If the decrypted losing bids are published by the auctioneer, public verifiability is achieved, but bid privacy is lost. If the auctioneer keeps the losing bids secret and auctioneer 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.

OSBA has the following phases:

1. Registration Phase
2. Bidding Phase
3. Bid Distribution
4. Time Checking
5. Winner Selection Phase
6. Winner Verification

## Steps Followed in Application Level

### *Registration Phase*

1) A dedicated **registration Server** (i.e. **auction bid service manager** i.e. **time keeper**) starts biding protocol by registering each bidder.

2) For registration bidder must submit his information (Such as Bid deposit/Bank account/ Tax return papers, etc.) to registration Server.

3) Registration Server sends a **certificate** to bidder.

4) An Independent private channel will be established between Auction server and client bidder through which they communicate with each other.

***5)*** After a pre-defined time **registration process**, maintained **by time keeper**, will time out. Then **bidding process** starts.

Say, there are four **bidders**, labeled $\mathbf{ID_0}$, $\mathbf{ID_1}$, $\mathbf{ID_2}$, $\mathbf{ID_3}$ registered in this auction. The ***seller*** publishes the ***price vector*** **V = (5, 10, 15, 20, 30, 35, 40)** and ***security parameter*** **m = 2**. The random number generator is set to generate 8-bit numbers randomly.

### *Bidding Phase*

1) ***Auction server*** starts it's ***bidding service*** and must close after a predefined time maintained by time keeper.

2) Bidder generates his personal ***session key*** and ***ticket*** for specific bid.

3) For this bidder choose auction item, price quote, auction ID (auction identifier) which form his ***secret bid***.

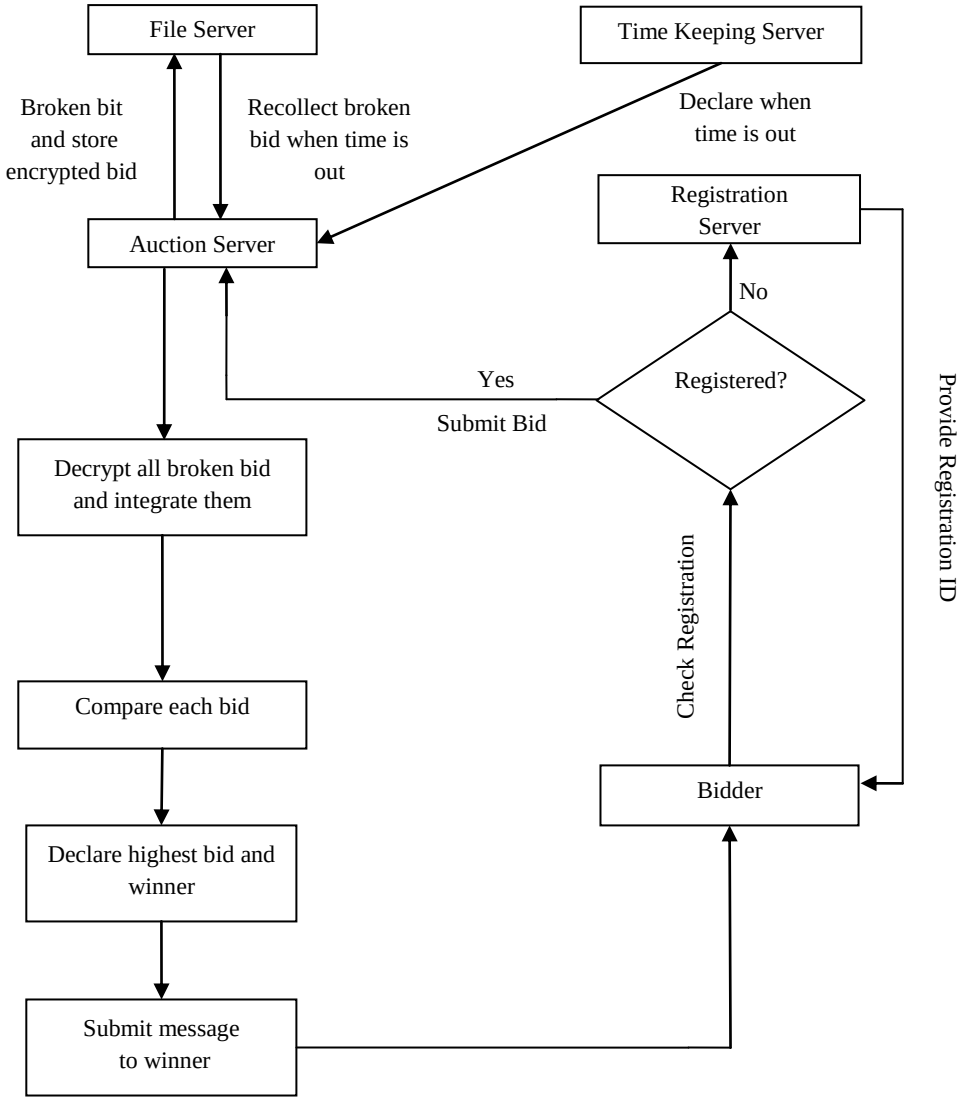



Fig. 1: Proposed Online Sealed Bid Auction (OSBA) Architecture

4) Bidder then randomly chooses a ***polynomial f(x)*** of degree ***t*** with a free term equal to ***secret bid***.

5) Then she/he computes the share of the secret bid from a pair of values of the two polynomials $\alpha_i$ = *f(i)* and $\rho_i$ = *r(I*) based on the algorithm of the polynomial chosen, where ***i*** is for ***n*** participating auction services.

6) Before sending to the $\boldsymbol{i}_{th}$ auction servers via private channel bidder encrypt his/her own bid.

7) According to the protocol, the commitment of a share is the one way hash of that share.

We summarize the information associated with the participants in the following fields. Table 1 contains the *price bid* by each participant, their *random number value* and their *commitment*. Table 2 contains the modified *vectors* for each participant. Each vector is sliced in two, since m = 2. Table 3 contains the *sliced and summed components* held by each bidder.

**Table 1. Price bid, Random number value, and Commitment**

| ID | Bid | Random Number | $R_{ID}$ | $C_{ID}$ |
|---|---|---|---|---|
| 0 | 15 | 150 | H(15+*150*) | $E_{PKS}(Sig_0(ID_0 \| H(15+150)))$ |
| 1 | 30 | 130 | H(30+*130*) | $E_{PKS}(Sig_0(ID_0 \| H(30+130)))$ |
| 2 | 35 | 180 | H(35+*180*) | $E_{PKS}(Sig_0(ID_0 \| H(35+180)))$ |
| 3 | 5 | 220 | H( 5+*220*) | $E_{PKS}(Sig_0(ID_0 \| H( 5+220)))$ |

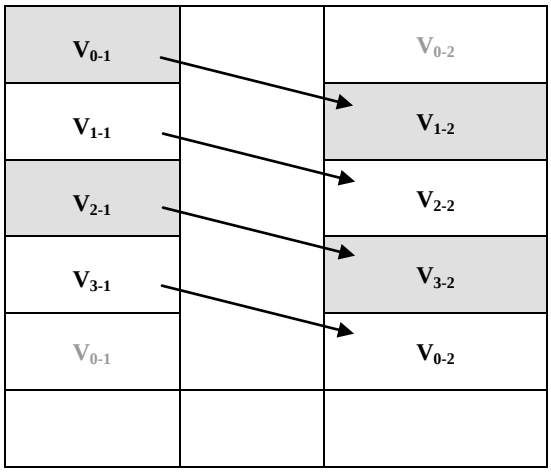
**Table 2. Modified Vectors for Each Participant**

| ID | Bid | $V_{ID}$ |
|---|---|---|
| 0 | 15 | H(15+*200*), H(15+*142*), H(15+*150*), 20, 25, 30, 35, 40 |
| 1 | 30 | H(30+*157*), H(30+*187*), H(30+*165*), H(30+*132*), H(30+*172*), H(30+*130*), 35, 40 |
| 2 | 35 | H(35+*133*), H(35+*145*), H(35+*215*), H(35+*232*), H(35+*211*), H(35+*147*), H(35+*80*), 40 |
| 3 | 5 | H(5+*133*), 10, 15, 20, 25, 30, 35, 40 |

**Table 3. Sliced and Summed Components Held by Each Bidder**

| ID | V | $V^{prime}$ |
|---|---|---|
| **0** | $V_{0-1} + V_{0-2}$ | $V_{3-1} + V_{0-2}$ |
| **1** | $V_{1-1} + V_{1-2}$ | $V_{0-1} + V_{1-2}$ |
| **2** | $V_{2-1} + V_{2-2}$ | $V_{1-1} + V_{2-2}$ |
| **3** | $V_{3-1} + V_{3-2}$ | $V_{2-1} + V_{3-2}$ |

**Table 4. Bid value transformation**




### *Share Compare, Check Validity and Broadcast Integrity*

- Compares the received pair of each encrypted $\alpha_i$ and $\rho_i$ with corresponding broadcast commitment.
- Each auction server (1, 2…n) also verifies that the broadcasted polynomial lie within a committed polynomial.
- If validity failed bidder then informed.
- When bidder receives any complaint from $i_{th}$ auction server, then he/she openly broadcast his/her $\alpha_i$ and $\rho_i$ and commitment to defend integrity.
- If he/she does not follow this step must be disqualified.

### *Closing of Bids and Winner Declaration*

After completion of bidding phase reconstruction process of ***auction bid service manager*** (i.e. ***time keeper***) collect all shares from all auction servers (1, 2..n) and reconstruct them and calculate the winner.

Sum of all incoming shares of bids,

$$V' = \sum_{i=1}^{N} V_i' = (V_{3-1} + V_{0-2}) + (V_{0-1} + V_{1-2}) + (V_{1-1} + V_{2-2}) + (V_{2-1} + V_{3-2})$$

= (H(215) + H(135) + H(168) + H(225),
10 + H(167) + H(217) + H(180),
15 + H(165) + H(195) + H(250),
40 + H(162) + H(267),
50 + H(202) + H(246),
60 + H(160) + H(182),
105 + H(215),
160)

Determining the index of highest price bid,

Evaluates the ***Vector*** **W = $V^{prime}$ – 4 X V** and determines the ***index*** of the first non-zero value, as read from the right. This ***index*** is ***7***, so the ***highest price bid*** was ***35***.

Determining win bid value:

Calculate,

*Bid* = W7 – 3 X 35 = H(215)

### *Announcing Phase*

1) ***Auction bid service manager*** pass an ***auction list*** to the bidder when he/she ask for it. In ***auction list*** winner is declared.
2) Then Auction server asks for ***secret gammas*** to the claimed bidder as to proof he/she is the winner.
3) Auction server validates ***secret gammas*** and congratulates winner.

For full privacy the seller publish a seller signed version of ***winner's commitment***, $\mathbf{Sig_s(H(215))}$. Every participant *checks* if this equals the one they committed. $\mathbf{ID_2}$ would find they won. Others know nothing about the winning.

## 4. CONCLUSION

In this paper, a robust method has been proposed for ensuring security and privacy of online sealed bid auction. It has been observed that the algorithm is capable enough of finding the solution of security question with greater scope.

## 5. REFERENCES

[1] Doyle, Robert A.; Baska, Steve (November 2002), "History of Auctions: From ancient Rome to todays high-tech auctions"

[2] Pekec, Aleksandar; Rothkopf, Michael H. (November 2003), "Combinatorial auction design.", *Management Science* (INFORMS) 49 (11): 1485–1503,

[3] Krishna, Vijay (2002), *Auction Theory*, San Diego, USA: Academic Press, ISBN 0-12-426297-X

[4] Milgrom, Paul (2004), *Putting Auction Theory to Work*, Cambridge, United Kingdom: Cambridge University Press, ISBN 0-521-55184-6

[5] Shubik, Martin (March 2004), *The Theory of Money and Financial Institutions: Volume 1*, Cambridge , Mass., USA: MIT Press, pp. 213–219, ISBN 0-262-69311-9

[6] Klemperer, Paul (2004), *Auctions: Theory and Practice*, Princeton, N.J.: Princeton University Press, ISBN 0-691-11925-2

[7] Smith, Charles W. (1990), *Auctions: Social Construction of Value*, University of California Press, ISBN 0-520-07201-4

[8] Milgrom, P.; Weber, R. (1982). "A theory of auctions and competitive bidding". *Econometrica* 50 (5): 1089–1122.

[9] Rivest RL, Shamir A and Adleman L; (1978); A method of obtaining digital signatures and public key cryptosystems; Comm. ACM; 21(2); pp. 120-126.

[10] Daemen J and Rijmen V; (2002); the Design of Rijndael; Advanced Encryption Standard; Springer-Verlag, Berlin; pp. 103-111.