Sealed-bid Auction Schemes using Threshold Cryptosystem

Wei-Chen Wu[1*], Horng-Twu Liaw[2] and Chih-Ta Yen[3]

[1]*Computer Center, Hsin Sheng College of Medical Care and Management, Taoyuan County, Taiwan, R.O.C.*
[2]*Department of Information Management, Shih Hsin University, Taipei, Taiwan, R.O.C.*
[3]*Department of Information Management, National Taiwan University of Science and Technology, Taipei, Taiwan, R.O.C.*
wwu@hsc.edu.tw, htliaw@cc.shu.edu.tw
**Corresponding Author*

Abstract

This paper proposes a secure sealed-bid auction schemes which adopt threshold cryptosystem without a third party. In the previous proposed sealed-bid auction schemes, an auctioneer is responsible for opening bids. However, malicious auctioneers can conspire with malicious bidders by revealing all bidding prices before the bid opening stage for bidding optimal bidding price to win the auction. To prevent against this, we decide to eliminate auctioneer from opening phase and involve plural clerks to choose secret keys, and then clerks distribute public keys to each other. On the bid opening phase, the clerks can cooperate with each other to open the bids without an auctioneer by using Pedersen's protocol and Lagrange interpolating polynomial. Hence, an auctioneer is only responsible for verifying user's identification and checking whether bids are valid or not. Furthermore, for enhancing security in our schemes, we utilize a hardware framework entitled "Untraceable Decryptor" to make all bids pass through it when the bids are transferred to clerks.

Key Words: *Security, Sealed-bid Auction, Untraceable Decryptor, Threshold Cryptosystems*

1. Introduction

Auction is one of the most important market mechanisms for a price negotiation. In an auction, a product price is determined through interactions among bidders in the market. With the importance of Internet is increasing continually, and it results in the electronic auction services growing. It results in a lot of research on auctions [1-8], and there is a large number of security issues need to be addressed on sealed-bid auctions. In sealed-bid auctions, each bidder seals his/her bid and submits it before a set time. After the set time, the winning bid will be opened, and the winner with the price is determined according to a pre-defined auction rule. In many auction applications, they are desired to keep the other bidders' private even at the end of the auction. This requirement is called bid privacy, and it is discussed in many papers. Bid privacy may have different definitions in different applications and may be implemented with different mechanisms under different assumptions. A sealed-bid auction protocol must satisfy the following requirements [1, 6-8, 12-14].

- (R1)Fairness: Auctioneers cannot see any bidding price before bid opening.
- (R2)Anonymity: All bidders must keep Anonymity.

- (R3)Verifiability: Everyone must be able to verify the correctness of each auction.
- (R4)Non-repudiation: Bidders cannot deny their bidding price
- (R5)Unforgeability: Auctioneers and bidders cannot forgery bids in each auction.
- (R6)Untraceability: Auctioneers cannot know the personal information of bidders.
- (R7)Privacy: A third party cannot get the detail payment information about a bidder.
- (R8)Confidentiality: Each bid must keep integrity and confidentiality until a bid opening.
- (R9)Traceability: The bidder can be identified when he/she wins the auction.
- (R10)Without a trusted third party.
- (R11)One-time Registration: A bidder can register once and bid auctions for auctioneers.

Sealed-bid auction [1-8] is an auction method, in which each bid submitted can be opened only after the closing time of an auction. After a bid opening phase, the auctioneer in this auction only announces the winner with his/her winning price. In our proposed auction schemes, an auctioneer is responsible for opening bids. However, malicious auctioneers can conspire with malicious bidders by revealing all bidding prices before the bid opening stage for bidding optimal bidding price to win the auction. To prevent this, we decide to eliminate the auctioneer from opening phase and involve plural clerks to choose the secret key, and then clerks distribute public keys to each other. Furthermore, to enhance security in our scheme, we utilize a hardware framework entitled "Untraceable Decryptor" to make all bids pass through it when the bids are transferred to clerks. Moreover, we propose two sealed-bid auction schemes for different security and efficiency considerations.

The remainder of this paper is organized as follows. In Section 2, we shall briefly the related theories and schemes which are used in this paper. Then we propose an untraceable and secure sealed-bid auction schemes based on Pedersen's protocol and Lagrange interpolating polynomial in Section 3 and we discuss the security and efficiency in Section 4. Finally, we conclude this paper in Section 5.

2. An Untraceable Decryptor

Untraceable Decryptor [10] is an important supplementary tool in Sealed bid Auction. It serves the following functions:

1. Having the ability to select a public key infrastructure parameter.
2. Once a public key infrastructure parameter is selected, it cannot be altered.
3. Having the ability to make encryption and decryption operation in public key infrastructure.
4. The order of data output is not related to the order of data input.

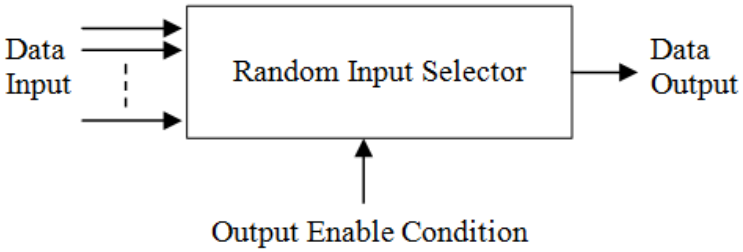

Figure 1. The Random Input Selector

The Untraceable Decryptor described above is composed of two parts. First is the Random Input Selector (RIS) with the purpose of completing the fourth requirement as described above. Second part is the public key decryptor with the purpose of completing the first three demands described above.

In the RIS is showed in Figure 1, it has the ability to store information; the input data can be stored temporarily in the buffer area, and then the output data is randomly selected from this area. Thus, the order of data output is not at all related to the order of data input. In the "Output Enable Condition" part, specific conditions can be determined to initiate the process of data output. For example, it can be set up in such a way that data output can proceed only after N number of data is input or at a specific time. The RIS will not initiate any data output without meeting the predetermined conditions. In addition, once an "Output Enable Condition" is set up, it cannot be altered. When an "Enable Signal" appears in a Public Key Decryptor (PKD) is showed in Figure 2, the decryptor will automatically select and output an appropriate set of parameters from the public key infrastructure.

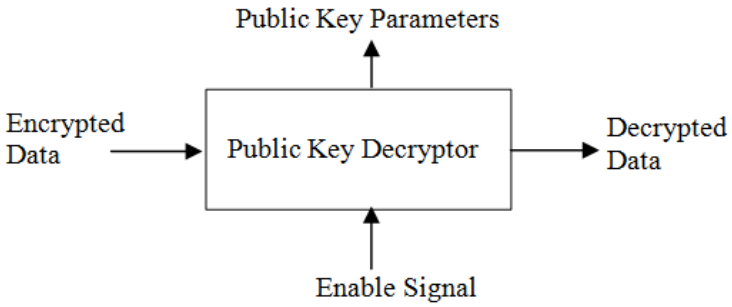

Figure 2. The Public Key Decryptor

The secret key is stored internally in PROM, and it is not able to be altered. When "Encrypted Data" are being input, the PKD will proceed with its internal decrypting. After that, the decrypted information will be hid partial data through Mask. RIS and PKD can be combined to form a complete Untraceable Decryptor is showed in Figure 3. All the input and output interfaces can be completely open and inspected by any member.

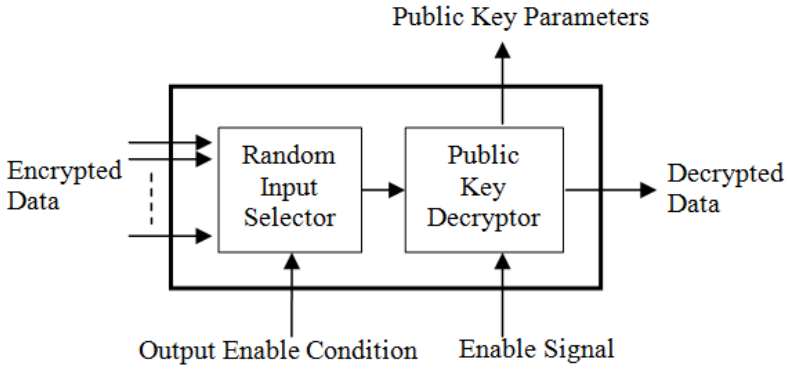

Figure 3. The Untraceable Decryptor

3. The Proposed Auction Scheme without a Register Center

In this section, we propose an untraceable and secure sealed-bid auction schemes which adopt threshold cryptosystem without a register center. In our schemes, we eliminate auctioneers from opening phase and involve plural clerks to choose the secret key, and then clerks distribute public keys to each other. The roles of these schemes involve bidders, clerks and an auctioneer, and these schemes consist of six phases: the initialization phase, the registration phase, the obtaining bids phase, the bidding phase, the announcement phase and the opening phase. Let A denotes an auctioneer, RM denotes a registration center, C_1,C_2, ..., C_n denote clerks, B_1,B_2, ..., B_m denote bidders, UD denotes an Untraceable Decryptor, ID denotes an identity of each bidder and "$X \rightarrow Y$: Z" denotes that a sender X sends a message Z to a receiver Y. Based on Pedersen's protocol and Lagrange interpolating polynomial, clerks cooperate to open the bids without an auctioneer. Hence, an auctioneer is only responsible for verifying user identification and checking whether bids are valid or not. Furthermore, to enhance security in our scheme, we use a new hardware framework said "Untraceable Decryptor" to make all bids pass through it when they transfer to clerks. We propose another scheme which removes the register center from the above scheme in this session, and its architecture presents as Figure 4.

3.1. The Initialization Phase

Auctioneer A chooses two system parameters p and g, where p is a large prime and g is a generator of order p in Z^*_p. To publish p and g and relevant information like the product's information and the specific number of this auction No. Then each clerk C_j chooses a secret key x_i at random and calculates $h_j = g^{xj} \bmod p$, where $1 \leq j \leq n$.

1. $A \rightarrow UD$: Output Enable Condition.

Auctioneer A start up the auction and set auction period time. Then UD generates a key pair K_u and K_u-1, publishes K_u and stores K_u-1. The concept is shown in Figure 3.

2. $C_j \rightarrow A$: h.

The public key h is computed by Auctioneer A as follows:

$h = \prod_{j=1}^{n} h_j$, where $1 \leq j \leq n$

3.2. The Registration Phase

First, bidders B_i would register with Auctioneer A. Then, Auctioneer A chooses each bidder B_i's secret key d_i and calculates the public key $e_i = g^{di} \bmod (p\text{-}1)$, where $1 \leq i \leq m$. The security comes from the difficulty of solving the discrete logarithm problem in a finite field, which is similar to the ElGamal scheme [11]. The steps are as follows.

1. $B_i \rightarrow A$: ID_i and No.

Each bidder B_i chooses his/her own ID and No, and then sends to Auctioneer A.

2. $A \rightarrow B_i$: (r_i, s_i) and h.

Auctioneer A obtains s_i and the signature of ID and No with bidder B_i is the pair (r_i , s_i) by using the extended Euclidean algorithm in the following equation:

$$H(ID_i \oplus No) = (d_i \times r_i + k_i \times s_i) \bmod (p\text{-}1), \text{ where } 1 \leq i \leq m$$

Continuously, Auctioneer A sends the pair (r_i, s_i) and a public key h back to the bidders.

3.3. The Obtaining Bids Phase

Bidders B_i would use the pair (r_i, s_i) to get the bidding bill from the auctioneer, where $1 \leq i \leq m$. The steps are as follows:

1. $B_i \rightarrow A$: (r_i, s_i), $ID \oplus No$.

Auctioneer A checks whether the validity of ID and No for each bidder B_i in the following equation: $e_i^{ri} \times r_i^{si} = g^{H(IDi \oplus No)} \bmod p$, where $1 \leq i \leq m$

If the above equation does not hold, auctioneer A rejects the bidder B_i to obtain a bid.

2. $A \rightarrow B_i$: Bid_{emptyi}.

If the above equation holds, auctioneer A chooses a random number X_A and calculates the bid as follows: The bid includes identity of each bidder and this auction No except his bidding price. Auctioneer A sends $Bid_{emptyi} = (ID_i \oplus No)^{X_A} \bmod p$, where $1 \leq i \leq m$, back to bidders B_i.

3. $A \rightarrow C_j$: X_A , Bid_{emptyi}, $ID_i \oplus No$

At the same time, Auctioneer A sends X_A , Bid_{empty} and $ID_i \oplus No$ back to clerks C_j, where $1 \leq j \leq n$.

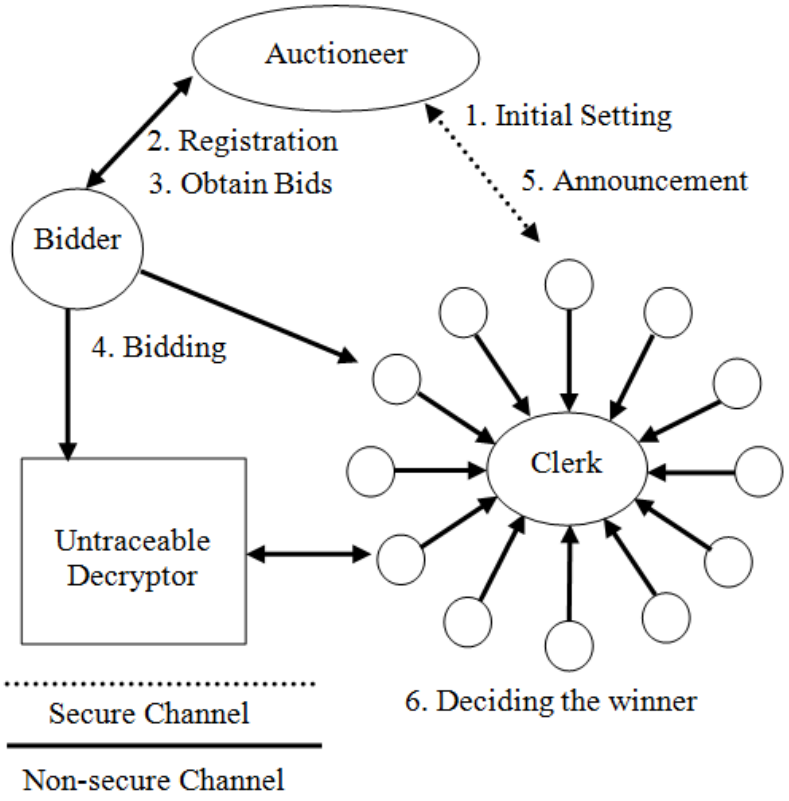

Figure 4. The Proposed Infrastructure without a Third Party

3.4. The Bidding Phase

To enhance security in our scheme, we use a new hardware framework said "Untraceable Decryptor" to make all Bid_i pass through it when they transfer to clerks in this phase.

1. $B_i \rightarrow UD : Bid_i$.

Each bidders B_i receives the empty bid (Bid_{emptyi}) and chooses his bidding price to compute $Bid_i = K_u(E_h(Bid_{emptyi} \oplus Price))$, where $1 \leq i \leq m$.

2. $B_i \rightarrow C_j : P_i, Z_i$.

Bidders B_i choose a random number r_i to compute $P_i=(ID_i \oplus No)^{ri}$ and $Z_i=(ID_i \oplus No)^{Bidi}$ $Bid_{emptyi}{}^{ri}$, where $1 \leq i \leq m$, to clerks C_j, where $1 \leq j \leq n$.

3. $UD \rightarrow C_j : E_h(Bid_{emptyi} \oplus Price)$.

After each bidders B_i delivers the Bid_i to the UD, it decrypted the Bid_i to derive $E_h(Bid_{emptyi} \oplus Price)$, where $1 \leq i \leq m$ and forwards to clerks C_j, where $1 \leq j \leq n$.

3.5. The Announcement Phase

When clerks C_j would publish P_i and Z_i in the auction web site, bidders B_i could check whether the result on the web. If not, he could appeal to the clerk within a fixed time and deliver his Bid_i again.

Clerks $C_1, C_2, \ldots, C_n$ cooperate to open the bids and n members share the secret key of an organization such that k Clerks ($1 \leq k \leq n$) must cooperate in order to open the bids without Auctioneer A base on Pedersen scheme [9].

1. C_i chooses at random a polynomial $f_i(x)$ of degree at most k-1 such that $f_i(0) = x_i$ Let $f_i(x) = a_{i,0} + a_{i,1} \cdot x + \ldots + a_{i,k-1} \cdot x^{t-1} \bmod p$, where $a_{i,0} = x_i$.
2. Except $F_{i,0} = h_i$ is known in initialization phase, C_i computes $F_{ij} = g^{ai,j}$ for $j=0, \ldots, k-1$. And then every C_i sends $s_{i,j} = f_i(j)$ secretly to C_j for $j=0, \ldots, n$.
3. C_i verifies that the share received from, C_j (s_{ji}) is consistent with the previously published values by verifying that $g^{s_{j,i}} = \prod_{l=0}^{k-1} F_{j,l}^{i^l}$

Because of

$$
\begin{aligned}
& g^{s_{ji}} = \prod_{l=0}^{k-1} F_{j,l}^{i^l} \\
& \Rightarrow g^{f_j(i)} = F_{j,0}^{i^0} \cdot F_{j,1}^{i^1} \cdot F_{j,2}^{i^2} \cdot \ldots \cdot F_{j,k-1}^{i^{k-1}} \\
& \Rightarrow g^{f_j(i)} = (g^{a_{j,0}})^1 \cdot (g^{a_{j,1}})^i \cdot (g^{a_{j,2}})^{i^2} \cdot \ldots \cdot (g^{a_{j,k-1}})^{i^{k-1}} \\
& \Rightarrow f_j(i) = a_{j,0} + a_{j,1} \cdot i + a_{j,2} \cdot i^2 + \ldots + a_{j,k-1} \cdot i^{k-1}
\end{aligned}
$$

4. C_i computes his share of x as the sum of all shares received as $s_i = \sum_{j=1}^{n} s_{j,i}$. Consequently, clerks $C_1, C_2, \ldots, C_n$ generate secret keys $s_1, s_2, \ldots, s_n$ respectively. If C_i has received correct shares, then each C_j ($i \neq j$) can compute σ_i as $\sigma_i = g^{s_i} = \prod_{j=0}^{n} g^{s_{j,i}}$.

Let f be the following polynomial: $f(x) = f_1(x) + f_2(x) + \ldots + f_n(x)$. By construction $s_i = f(i)$ for every $i=1, \ldots, n$, and thus s_i is a share of $f(0)=x$.

$$
\begin{aligned}
& f(x) = \sum_{j=1}^{t} f_j(x) \\
& \Rightarrow f(x) = f_1(x) + f_2(x) + f_3(x) + \ldots + f_t(x) \\
& \Rightarrow f(x) = \sum_{j=1}^{n} a_{j,0} + \sum_{j=1}^{n} a_{j,1} \cdot x + \sum_{j=1}^{n} a_{j,2} \cdot x^2 + \ldots + \sum_{j=1}^{n} a_{j,t-1} \cdot x^{t-1}
\end{aligned}
$$

Now, any t of the n or more members can recover the $\sum_{j=1}^{n} a_{j,0}$ by Lagrange interpolating polynomial as following: $f(x) = \sum_{i=1}^{t} s_i \prod_{1 \leq j \leq t, j \neq i} \frac{x-j}{i-j} \bmod p$

And then compute $h = g^{\sum_{j-1}^{n} a_{j,0}}$.

To find out the winning price, clerk C_i perform the following operations:

1. Verify identity of bidders to check whether $Z_i (P_i^{-1})^{XA} = ID_i^{Bidi}$.

2. Decrypt *the* $E_h(Bid_{emptyi} \oplus Price)$ with key h and makes an exclusive operation to derive Price.

Reveal each sealed price and find the bidder who bid the highest price. The bidder who bid the highest price wins and he can buy the item at his bid price.

4. Analysis

In this section, we present our schemes how to satisfy the requirements of a sealed bid auction and make the comparison with previous papers.

Table 1. A Requirement Comparison Table

Schemes	R1	R2	R3	R4	R5	R6	R7	R8	R9	R10	R11
Hwang[3]	✓	✓	✓	✓	×	×	×	✓	✓	×	×
Juang *et al*.[4]	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Liaw *et al*.[6]	×	✓	✓	×	✓	✓	×	✓	✓	×	×
Ha *et al*.[2]	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	×
Wu *et al*.[7]	✓	✓	✓	✓	✓	✓	✓	✓	✓	×	×
Lee *et al*.[5]	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Chen *et al*.[1]	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	×
Proposed Scheme	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

4.1. Requirements Analysis

We analysis the proposed schemes whether the schemes satisfy the requirements of a sealed bid auction, and table 1 presents the comparison with previous papers.

- (R1)Fairness: due to use the Untraceable Decryptor to protect the secrecy of bidding price as $Bidi=Ku(E_h(Bid_{emptyi} \oplus Price))$, the Bid_i guarantee no one can derive Price. Moreover, the bidding information is encrypted with key *h* that be only cooperated to calculate by *t* clerks. Although every bidder has the key *h* value, the Bid_i first pass through Untraceable Decryptor before using key *h* to decrypt. Otherwise, the Bid_i use key *h* to encrypt and then output value is invalid.
- (R2)Anonymity: because all the bidders bid auctions with the auction key $Y_{i,\ No}$, they compute the P_i and Z_i and sends to the supervisory group *Clerks*. Thus, the identity of the bidder B_i is difficult to be known in first scheme; because all bidders submit their

$P_i=(ID_i \oplus No)^{r_i}$ and $Z_i=ID_i^{Bid_i} Bid_{empty_i}{}^{r_i}$ to the clerks in the obtaining bids phase, take P_i and Z_i as their pseudonym to participate for anonymous in second scheme.

- (R3)Verifiability: in the obtaining bids phase, all bidders submit their P_i and Z_i to the clerks to verify. After it is identified, the P_i and Z_i will be published in the auction web site for anyone verifying the correctness. If his P_i and Z_i cannot be published, the bidder B_i can argue with the auctioneer A.
- (R4)Non-repudiation: the blank bidding bill Bid_{empty} used by the bidder B_i contains the information about the auction key, and only the bidder B_i's secret key could decrypt the encrypted message to bid.
- (R5)Unforgeability: all the parameters delivered between these roles are based on the public key cryptosystem. If someone wants to decrypt the encrypted message, he/she has to face the discrete logarithm problem of ellipse curve.
- (R6)Untraceability: the whole bidding process have been handled and controlled by the Untraceable Decryptor.
- (R7)Privacy: all the bidding would be processed by the auction key $Y_{i, No}$, the auctioneer A could not know the personal information about the bidder B_i in first scheme. In the second scheme, we use h to encrypt each bid price, and the bid price can be known until the opening phase.
- (R8)Confidentiality: all the messages delivered between these roles are based on the public key cryptosystem, and the public key cryptosystem could ensure the integrity and security. All the bidding information would be processed by the Untraceable Decryptor UD, therefore, the security could be ensured.
- (R9)Traceability: if there are controversies in the auction process or the winner B_i doesn't pay the money, the auctioneer A could investigate who is the real identity of the winner B_i though the registration center RM in first scheme. In second scheme, the auctioneer A could investigate who is the real identity of the winner B_i himself/herself.
- (R10)Without a trusted third party: without a trusted third party can reduce the system building cost.
- (R11)One-time Registration: in the first scheme, the bidder B_i who is interested in the product of the auction could register to the registration center RM only one time and obtain the registration key RK_i in first scheme. Subsequently, the bidder B_i wants to attend to the bidding of the auctioneer A only need to generate the auction key $Y_{i, No}$ by the registration key RK_i.

4.2. Efficiency Analysis

Table 2. A Computational Comparison Table

Schemes	Phase 1	Phase 2	Phase 3	Phase 4	Phase 5	Phase 6
Hwang[3]	$3nT$(exp)	0	$10nT$(exp)+$4nT$(⊕)		0	
Juang, *et al*., [4]	nT(exp)	$8nT$(exp) +8nT(ME) +$8nT$(⊕)	$8nT$(exp)+$6nT$(ME) +$17nT$(⊕)+$2nT$(h)		nT(exp)	
Liaw, *et al*., [6]	nT(exp)	$2nT$(exp) +$5nT$(h)	$5nT$(exp)		0	
Ha, *et al*., [2]	nT(exp)	$10nT$(exp) +nT(exp) +$3nT$(h)	n^2T(exp)		nT(exp)	
Wu, *et al*., [7]	nT(exp) +nT(h)	$2nT$(exp) +nT(h) +$2T$(S)	nT(ME) +$4nT$(exp)		nT(exp) +nT(ME) +$2nT$(S)	
Lee, *et al*., [5]	$2nT$(exp) +$2nT$(ME)	$3nT$(exp) $3nT$(ME)	$4nT$(ME) +$9nT$(exp) +nT(h)		$4nT$(ME) +$7nT$(exp) +$3nT$(h)	
Chen, *et al*., [1]	T(exp) +T(ME)	$2nT$(exp) +$4nT$(ME) +2nT(h)	$6nT$(exp)+$7nT$(ME) +$2nT$(h)		$2nT$(ME)+$2nT$(exp)	
Proposed scheme	nT(exp) +nT(ME) +nT(h)	nT(ME) +nT(⊕)	nT(ME) +$2nT$(exp) +nT(⊕)	$3nT$(exp) +$2nT$(⊕) +$4nT$(S)	0	$4nT$(exp) +nT(ME) +T(S)

■T(h): computation cost of one-way function

■T(⊕): computation cost of Exclusive-OR operation

■T(S): computation cost of symmetric encryption

■T(ME): computation cost of modular exponentiation

■T(exp): computation cost of exponentiation operation

Table 2 presents the computational comparison with previous papers and shows that our schemes do not have the lowest computational time. However, our schemes can eliminate the auctioneer from the opening phase for protecting bidding privacy and do not have a trust third party for driving down system building cost. Although some schemes [8-9] also achieve all the requirements, they have the higher computational time than our schemes.

5. Conclusion

We have proposed a secure sealed-bid auction schemes which adopt threshold cryptosystem without a register center. In our schemes, we eliminate auctioneers from opening phase and involve plural clerks to choose the secret key and distribute it themselves. Subsequently, based on Pedersen's protocol and Lagrange interpolating polynomial, clerks can cooperate to open the bids without an auctioneer. Hence, an auctioneer is only responsible for authenticating users and checking whether bids are valid or not. Furthermore, to enhance security in our schemes, we utilize a new hardware framework said "Untraceable Decryptor" to make all bids pass through it when they transfer to clerks. Moreover, our schemes achieve all the secure requirements and efficiency.

References

[1] Y. F. Chung, Y. T. Chen, T. L. Chen and T. S. Chem, "An agent-based English auction protocol using Elliptic Curve Cryptosystem for mobile commerce", Expert Systems with Applications, vol. 38, no. 4, **(2011)**, pp. 9900.
[2] J. H. Ha, J. Zhou and S. J. Moon, "A Secure Double Auction Protocol against False Bids", Decision Support Systems, vol. 44, no. 1, **(2007)**, pp. 147.
[3] M. Hwang, J. Lu and I. Lin, "Adding Timestamps to the Secure Electronic Auction Protocol", Data & Knowledge Engineering, vol. 40, **(2002)**, pp. 155.
[4] W. S. Juang, H. T. Liaw, P. C. Lin and C. K. Lin, "The Design of a Secure and Fair Sealed-bid Auction Service", Mathematical and Computer Modelling, vol. 41, no. 8-9, **(2005)**, pp. 973.
[5] C. C. Lee, P. F. Ho and M. H. Hwang, "A Secure E-Auction Scheme based on Group Signatures", Information System Frontiers, vol. 11, no. 3, **(2009)**, pp. 335.
[6] H. T. Liaw, W. S. Juang and C. K. Lin, "An Electronic Online Bidding Auction Protocol with Both Security and Efficiency", Applied Mathematics and Computation, vol. 174, no. 2, **(2006)**, pp. 1487.
[7] C. C. Wu, C. C. Chang and I. C. Lin, "New Sealed-Bid Electronic Auction with Fairness, Security and Efficiency", Journal of Computer Science and Technology, vol. 23, no. 2, **(2008)**, pp. 253.
[8] F. Zhang, Q. Li and Y. Wang, "A new secure electronic auction scheme", Proceeding of the EUROCOMM, vol. 54, **(2000)**.
[9] T. P. Pedersen, "A Threshold Cryptosystem without a Trusted Party", Lecture Notes in Computer Science, vol. 522, **(1991)**.
[10] H. T. Liaw, "A Secure Electronic Voting Protocol for General Elections", Computers & Security, vol. 23, no. 2, **(2004)**, pp. 107.
[11] T. A. ElGamal, "Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms", IEEE Transactions on Information Theory, vol. 31, no. 4, **(1985)**, pp. 469.
[12] I. V. Koskosas and N. Asimopoulos, "Information System Security Goals", International Journal of Advanced Science and Technology, vol. 27, **(2011)**, pp. 15.
[13] F. Y. Sattarova, T. H. Kim, "IT Security Review: Privacy, Protection, Access Control, Assurance and System Security", International Journal of Multimedia and Ubiquitous Engineering, vol. 2, no. 2, SERSC, **(2007)**, pp. 17.
[14] T. H. Kim and K. Sakurai, "A study on Security Level Management Model Description", International Journal of Multimedia and Ubiquitous Engineering, vol. 3, no. 1, SERSC, **(2008)**, pp. 87.