A New Auction with Convertible Cryptosystem and Mutual Authentication

Henry Ker-Chang Chang[1,*], An-Ta Liu[2], and Guo-Lun Luo[3]

[1,3] Graduate Institute of Information Management, Chang Gung University

[2] Ph. D student, Graduate Institute of Business Administration, Chang Gung University

ABSTRACT

Electronic auction is popular due to rapid development of Internet technology. However, the identity and privacy of bidders are facing an insecure environment. Hence, a secure trade-off environment which can protect the privacy of bidders is necessary for auction. However, it never emerges as a reasonable and complete solution for the auction center to control the bidder's privacy from contemporary research. The proposed protocol focuses on the English auction method that can reach mutual authentication between the bidders and auction center by Diffie-Hellman key exchange and can protect the security of message by applying convertible authentication cryptosystem during the transmission.

Keywords: English auction, cryptosystem, mutual authentication, auction center (AC).

一個具匿名與使用可轉換鑑別加密和相互認證之電子競標

張克章[1,*]　劉安達[2]　羅國綸[3]

[1,3] 長庚大學資訊管理研究所

[2] 博士生。長庚大學企業管理研究所

摘　要

隨著網際網路的進步，電子拍賣市場也跟著蓬勃發展。但投標人身分與隱私隨時面臨不安全等現象。因此，提供一個安全的交易環境並保障投標人隱私相應為網路電子拍賣的基本要求。而當代學者研究中並未提合理一個管制拍賣中心交易信息的完全解決方案。故本研究從英國式拍賣協定著手，所提架構除以 Diffie-Hellman 金鑰交換達成投標人與拍賣中心間互相認證外，亦達成通訊間密碼轉換確認以保障信息傳遞安全。

關鍵詞： 英國式拍賣，加解密系統，互相確認，拍賣中心

文稿收件日期 100.7.26;文稿修正後接受日期 101.3.28; *通訊作者
Manuscript received July 26, 2011; revised March 28, 2012; * Corresponding author

I. INTRODUCTION

Internet is developing rapidly in decades, and auction is also getting popular in the web. Auction allows the consumer and auctioneer can complete various commercial behaviors through transactions of electronic bidding. It saves not only a lot of time but also eliminates some unnecessary procedure. Yahoo, Amazon and eBay are the most popular auction platforms. Any kinds of merchandise can be trade-off on these auction platforms. There have some drawbacks in auction such as the auctioneer can modify the winning bidder and bidding price easily, that is the electronic data can easily be forged. Besides, it could also be a situation that the auctioneer makes the clear snow labor, gets the money but refuses to react the contract. Therefore, the robustness and reliability of the electronic auction protocol must consider the following: maintaining the correctness of the auction process, fairness and non-repudiation, protecting the bidder's privacy appropriately, convenience of electronic auction mechanism and promoting the bidding efficiency.

In manual-based auction, the bidders have to show up on the bid center personally if they want to participate in the auction. It takes time and money at that time. On the other hand, as results of Internet technology becomes increasingly mature and booming, the auction overcomes some drawbacks of manual-based auction. Now, the auction provider can give a more convenient and efficient bidding mechanism, and many internet users around the globe join the auction. Thus, bidders can bid anytime and anyplace on the Internet. Liaw *et al.* [1] described several auction types in the current auction market shown in Figure 1. Ireland government reported [2] that the electronic auction offers some different operation models. The special point is the joiners who can play this auction. Oz [3] expressed the B2B marketplace in auction model is like a virtual market; some businesses can increase profits from the virtual markets in Internet. Other applications like virtual auctions in Whiteley [4] are the profits that anyone can get from them. Thereafter, we can understand that the potential profit can be acquired from the electronic auction markets.

Recently, the electronic markets are also suffering attacks from malicious personage following the insecurity of Internet. In order to guarantee the user using e-auction system securely and maintain operation of the mechanism fairly, this work investigates related security issues and targets on English auction protocol.

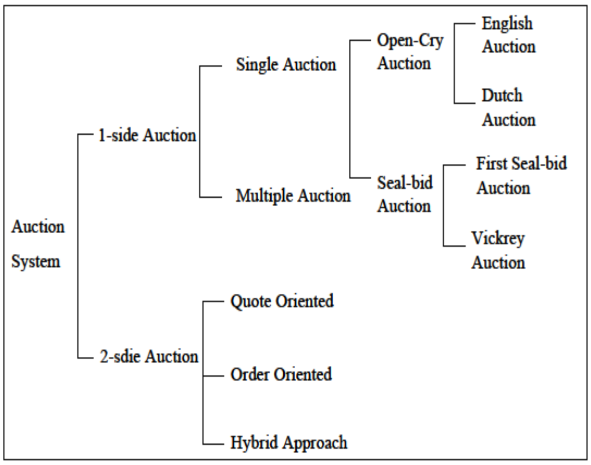

Fig. 1. Auction system classifications.

In the 21th century, most scholars started to combine the economic theory and mathematical theory in order to construct a secure and practical auction model. In 2002, Brandt [5] proposed a secure auction without auctioneer, which is designed only for Vickrey auction [6] with full privacy. All bidders are responsible for sharing each bid and they must jointly compute the winning price. Nonetheless Brandt's scheme put much attention on Vickrey auction which is different from our proposed protocol as shown in Fig.1. In addition, Brandt [5] gives emphasis on weakness on vulnerabilities of bidder collusion. The vulnerability of collusive bidding is that second-price auction is highly susceptible to collusion. Then auctioneers are obsolete in these "bidder-resolved" auction protocols. This is other weakness which we have to notice.

In public-auction related works, many researchers proposed various types of auction protocols. Chang and Chang [7] presented an efficient anonymous auction protocols to ensure that the bidders can bid arbitrarily and anonymously. They utilized the method of deniable authentication to completely achieve the anonymity and others such as verifiability and non-repudiation. Nonetheless, privacy inevitably is the main requirements in the event of a lost sealed-bid. And then Jiang *et al.* [8]

proposed an improvement on Chang and Chang [7] efficient anonymous auction protocols to overcome the security weakness in initiation phase. Chen [9] proposed an English auction scheme in the transaction environment, this study developed methods in response to security requirements of the English auction. Lastly, Chung *et al*. [10] proposed a bidder-anonymous English auction scheme with privacy and public verifiability, this scheme reduced not only the loading of registration procedure, but also the burden of the auction-manager through a key acquired from the end server. It also eliminates the need of bidders to download auction keys and auction certificates. While using Deffie-Hellman key exchange scheme [13], Su *et al*. [11] described an idea to include three identity-based cryptography schemes. Most existing cryptosystem designs incorporate just one cryptographic scheme; but, it is possible for an efficient algorithms proposed in the future to break one or more of these assumptions. The security of the proposed scheme follows from the difficulties in simultaneously solving the factoring (FAC) and discrete logarithms (DL) problems with arithmetic modulo of almost the same size. Each user in the system uses common arithmetic modulo and only requires one public key and one private key. Su *et al*. [11] scheme supports user identification, digital signature, encryption scheme does not achieve integrity and authenticity. Chen [22] improved the scheme by mending the weakness. After that, Zhang *et al*. [23] pointed out that authenticated encryption scheme by Tseng *et al*. [17] does not provide non-repudiation and forward secrecy properties. Finally, they present a new authenticated encryption scheme with message linkages that need to be resolved and key distribution. From this paper, we believe that the channel between three identity-based cryptography schemes can allow applying in our research. Su and Tsai [12] explained that a one-round and self-certified protocol has been proposed in order to enhance key exchange scheme. This scheme creates a more secure channel in which connection is able to exchange session keys between two participants at a time. We can recognize their ability for session-key exchange mode.

In view of these potential problems in the electronic auction, we present a new auction model that can be used in any auction types and satisfies all security requirements. In general, bidders must not only have the right to bid in secret, but also they are under obligation to admit their bids. Consequently, we emphasize an anonymous auction model with undeniable bid in this paper. We use the Diffie-Hellman key exchange [13] to setup the “mutual authentication” property among bidders and auction center (AC). When bidders send or get any message from AC, they can use this protocol to check identity of AC. Different from other auction schemes, we use only one auctioneer for the prevention of auctioneer’s collusion. Although auctioneer knows who the bidders are, it cannot prove their validity to others. Finally, we use convertible undeniable signature scheme to make arrangement for the “non-repudiation” property.

II. RELATED WORK

There are various schemes discussing bidding system. In order to establish our proposed a new auction system, we have referenced various cryptographic techniques. Those schemes are discussed in this paragraph.

2.1 Convertible Authenticated Encryption

A digital signature can achieve the functions of authentication, non-repudiation and integrity for a signed message. However, in certain situation, a signature requires maintaining privacy of messages which can only be verified by some specific receiver.

Using improved message recovery signature by Nyberg and Rueppel [14], Horster et al. [15] firstly proposed an authenticated encryption scheme with the above property. However, it is difficult to believe that a receiver signing the message is the actual receiver. Therefore when the signer repudiates his signature later, the receiver cannot prove the dishonesty of the signer to any third parties without disclosing confidential information. To overcome this weakness, Araki et al. [16] proposed a convertible limited verifier scheme enabling the receiver to convert the signature. But this method has an obviously drawback which needs the signer’s cooperation.

Following development of public

infrastructure, the communication fee is reduced that makes the message recovery of large amount also to save a lot of cost. Tseng et al. [17] proposed an authenticated encryption schemes with message linkage for message flows. The authenticated encryption scheme only allows a specified receiver to verify and recover the message. In this scheme, only the reduced usage of a random number and the communication costs can improve the time complexity by outperforming previous proposed schemes [18, 19, 20, 21]. However, this authenticated encryption scheme does not achieve integrity and authenticity. Chen [22] improved the scheme by mending the weakness. After that, Zhang *et al.* [23] pointed out that authenticated encryption scheme by Tseng *et al.* [17] does not provide non-repudiation and forward secrecy properties. Finally, they present a new authenticated encryption scheme with message linkages that need to be resolved.

2.2 Tzeng *et al*. proposed a different protocol

In the recent years, Tzeng *et al.* [24] proposed a new convertible authentication encryption scheme with message linkages. To protect the receiver's benefit, the receiver can easily convert the signature into an ordinary one that can be verified by anyone. The signature needs only be recovered and verified by the recipient in the normal procedure. In case of controversial situation, the receiver can demonstrate the converted signature to the verifier. The converted signature is embedded in the authenticated encryption signature, in which no signer is required to cooperate voluntarily.

Although Tzeng *et al.* [24] provided some new authenticated encryption scheme with message linkages; the operation status emphasized, this argument has not been supported publically. In addition, fairness is required when the auction affairs are running.

Since Taniar [25] also described the unfairness of e-auction, Taniar believes that the recovery of this fraud needs to be overcome. We then consider that the mutual authentication is used to avoid this attack. So the paper issued by Tzeng *et al.* [24] is much different from the proposed scheme.

2.3 Review of Chung et al. Auction Scheme

Different approach supported to auction scheme. This is another reason we have to discuss. Chung *et al.* [10] studies the English auction protocol, which comprises three interactive parties—the registration manager, the auction manager and the bidder. The registration manager confirms and authenticates the identities of bidders; the auction manager issues the bidding rights and maintains order in holding the auction. The scheme developed herein can effectively reduce the load on the registration and auction managers by requiring the end server to derive the key. It also eliminates the need for bidders to download the auction key and the auction certificate. Hence, the time complexity of processing data is clearly reduced and the best interests of the bidders can be achieved. Accordingly, the scheme is consistent with the actual practice of transactions. Although this method works efficiently, it still needs to rely on the third party to finish the authentication process.

III. THE PROPOSED SCHEME

There are three participants who are AC, bidder and auctioneer. The system contains six phases; they are registration phase, mutual authentication phase, bidding phase, declare winner phase and convertible signature phase as shown in Fig.2.

The system parameters used in our proposed scheme are:

p : A large prime

q : A large prime factor of $p-1$

g : A generator with order q in $GF(p)$

$h()$: A one-way hash function

Z_q^* : The integers modulo q denoted Z_q; the multiplicative group of Z_q are $Z_q^* = \{a \mid 1 \le a \le q-1\}$.

In addition, AC publishes p, q, g and $h()$.

3.1 Registration Phase

When a user $User_i$, bidder or auctioneer intends to join the system, he/she chooses a secret key x_i in Z_q^* and computes public key y_i using Eq. (1)

$$y_i = g^{x_i} \bmod p . \qquad (1)$$

For AC, it also should choose its secret key $x \in Z_q^*$, and computes the corresponding public key $y = g^x \bmod p$

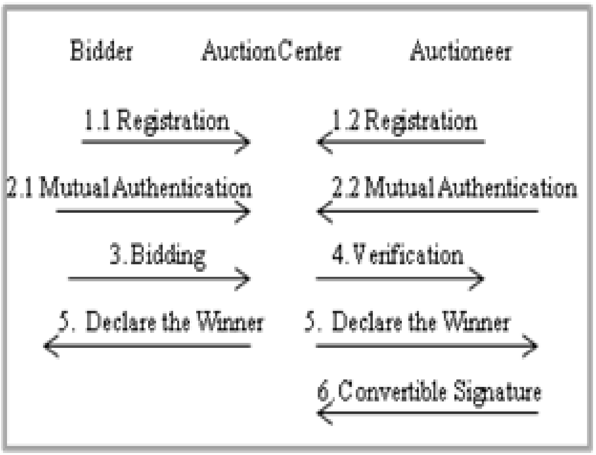

Fig. 2. A procedure of our scheme

3.2 Mutual Authentication Phase

In order to protect user rights and avoid users from encountering malicious attack likes hijack bids, validity needs to be confirmed before a user connects with AC. In the beginning, $User_i$ will do as follows:

Step 1: Selects a random integer $r_1 \in Z_q$ and a timestamp t_1

Step 2: Computes

$$A = y^{x_i} \bmod p \qquad (2)$$

$$Y_i = y_i^{r_1} \bmod p \qquad (3)$$

$$V_i = A^{r_1} \bmod p \qquad (4)$$

$$U = E_{V_i}(y_i) \qquad (5)$$

$$MAC_i = h(A \| V_i \| t_1) . \qquad (6)$$

Step 3: $User_i$ transfers (Y_i, MAC_i, t_1) to AC.

Step 4: After receiving the message (Y_i, MAC_i, U, t_1), AC verifies t_1 which is valid.

If it is required, then it computes:

$$V_i' = Y_i^x \bmod p \qquad (7)$$

$$y_i = D_{V_i'}(U) \qquad (8)$$

$$A' = y_i^x \bmod p . \qquad (9)$$

Step 5: Then AC checks the following equation:

$$h(A' \| V_i' \| t_1) \overset{?}{=} MAC_i \qquad (10)$$

If Eq. (10) holds, AC is identified as a valid message from $User_i$. If Eq. (10) is not true, such a request is rejected.

Step 6: If $User_i$ is valid, AC chooses a timestamp t_2 and a random integer $r_2 \in Z_q$

Step 7: Computes

$$V_j = (A')^{r_2} \bmod p \qquad (11)$$

$$K_{ij} = (V_i')^{r_2} \bmod p \qquad (12)$$

$$MAC_j = h(K_{ij} \| V_i' \| t_2) \qquad (13)$$

Step 8: AC sends the message (V_j, MAC_j, t_2) to $User_i$.

Step 9: After receiving the message, $User_i$ checks t_2 is valid and computes:

$$K_{ij} = V_j^{r_1} \bmod p \qquad (14)$$

Step10: Checks the equation by $User_i$ using

$$h(K_{ij} \| V_i \| t_2) \overset{?}{=} MAC_j . \qquad (15)$$

If the equation holds, $User_i$ understands that the AC is valid and the mutual authentication is completed. If it does not hold true, such a request is rejected. The mutual authentication with $User_i$ and AC is listed in Fig.3.

3.3 Bidding Phase

When bidder B_i decides to bid, B_i will undergo steps described as follows. Since $Y_i = y_i^{r_1} \bmod p = g^{x_i r_1} \bmod p$ is auction key, according to Eq. (1), $y_i = g^{x_i} \bmod p$, so $x_i r_1$ is the bidder's private key, Y_i is the corresponding public key in this auction. The proposed scheme is described as follows:

Step1: Selects a random integer $\theta \in Z_q^*$ to sign (R, S) where M_i represents the bidding price:

$$r = M_i \cdot y_j^{\theta} \bmod p \qquad (16)$$

$$R = h(M_i, \theta, g^{\theta}) \bmod p \qquad (17)$$

$$S = \theta - Rx_i r_1 \bmod p \qquad (18)$$

Step 2: Sends (R, S, r) to auctioneer.

$$C = E_{K_{ij}}(m) \qquad (21)$$

Sends message C to the bidder.

Step 2: After receiver C, the winner uses the shared key K_{ij} to decrypt it:

$$m = D_{K_{ij}}(C) \qquad (22)$$

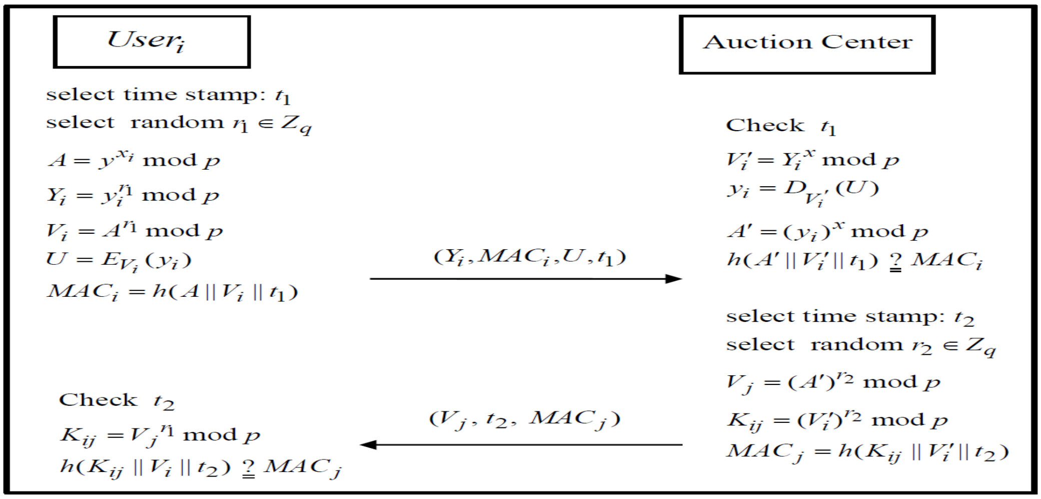
$User_i$
Auction Center
select time stamp: t_1
select random $r_1 \in Z_q$
$A = y^{x_i} \bmod p$
$Y_i = y_i^{r_1} \bmod p$
$V_i = A^{r_1} \bmod p$
$U = E_{V_i}(y_i)$
$MAC_i = h(A \| V_i \| t_1)$
(Y_i, MAC_i, U, t_1)
Check t_1
$V_i' = Y_i^{x} \bmod p$
$y_i = D_{V_i'}(U)$
$A' = (y_i)^{x} \bmod p$
$h(A' \| V_i' \| t_1) \overset{?}{=} MAC_i$
select time stamp: t_2
select random $r_2 \in Z_q$
$V_j = (A')^{r_2} \bmod p$
$K_{ij} = (V_i')^{r_2} \bmod p$
$MAC_j = h(K_{ij} \| V_i' \| t_2)$
(V_j, t_2, MAC_j)
Check t_2
$K_{ij} = V_j^{r_1} \bmod p$
$h(K_{ij} \| V_i \| t_2) \overset{?}{=} MAC_j$

Fig. 3. Mutual authentication with $User_i$ and AC

3.4 Verification Phase

After receiving message from bidder, auctioneer A_j can recover the M_i by following steps:

Step 1: Recover M_i

$$M_i = r \cdot ((g^S Y_i^R)^{x_j})^{-1} \bmod p \qquad (19)$$

Step 2: Verify the signature with following equality:

$$R \overset{?}{=} h(M_i, \theta, g^S Y_i^R) \bmod p . \qquad (20)$$

If the equality does, the signature is valid.

3. 5 Declare the Winner Phase

When the bidder with the highest bid in submission, he/she is the winner, and AC declares the news to the winner. The winner must do the following to verify his/her identification:

Step 1: AC uses the shared key which is generated in mutual authentication phase with bidder to encrypt the declaration message:

After checking the message physically coming from AC, and then the winner sends r_1 to AC to prove he/she has truly made a bid. But AC checks the following equation:

$$Y_i = y_i^{r_1} \bmod p \qquad (23)$$

If it holds, AC can be sure who is a real winner. Otherwise, AC rejects the deal.

3.6 Convertible Signature Phase

If bidder repudiates the signature, auctioneer can confirm the dishonesty of the signer by revealing the converted signature (R, S, r) for M_i to AC. With this converted signature, AC can confirm its validity using following equation.

In this conversion phase, the converted signature can be verified by Eq. (20).

Proof:

According to Eq. (20), we have

$$h(M_i, \theta, g^S Y_i^R) \bmod p$$
$$= h(M_i, \theta, g^{\theta - Rx_i r_1} Y_i^R) \bmod p$$
$$= h(M_i, \theta, g^{\theta} Y_i^{-R} Y_i^R) \bmod p$$

$$= h(M_i, \theta, g^{\theta}) \bmod p$$
$$= R \bmod q \, .$$

IV. SECURITY ANALYSES

In this section, comparisons of two auctions are displayed. The first one intends to illustrate the security of the proposed scheme. The second one aims at distinguishing the disadvantages from the approach issued from Tzeng *et al*. [24]. The security requirements of an English auction scheme are explained as follows:

(1) Anonymity: Anonymity refers to a message that does not carry any information about its sender and its intended recipient to make hackers have no way to get any information about the sender and recipient. Via the mutual authentication phase, AC endorses Y_i in B_i. Therefore we can use the key pair $x_i k$ and Y_i to bid in the bidding phase. No one knows who owns Y_i and obtain any information about B_i from Y_i.

(2) Integrity: Integrity refers to the wholeness the sender sends is the wholeness the recipient gets. It can approve that the contents have not been falsified during the transmission. In the mutual authentication phase, AC checks Y_i which is valid, Then AC generates the share key k_{ij} in MAC_j. In this case, no one can play of malicious AC to cheat $User_i$. In the bidding phase, $User_i$ uses the secret $x_i k$ to sign the biding price M_i and sends the bidding messages (R, S, r), if someone wants to alter the message of M_i. The auctioneer uses $R \overset{?}{=} h(M, r, g^S Y_i^R) \bmod p$ to check validity of the bidding message.

(3) Non-forgeability: Non-forgeability refers to the protection capability to keep the data from being forged. In the mutual authentication phase, anyone cannot generate a valid message (Y_i, MAC_i, t_1) to pass through AC's check. Because MAC_i includes A and V_i. If anyone wants to compute A, it computes V_i firstly. But there is a secret value *x*, which is a private key of AC in the computation of V_i. Therefore anyone has capability to figure out that V_i can use it to decrypt U. Hence, y_i is anonymous such that no one can compute A.

(4) Traceability: Traceability refers to the ability to trace the message routing to prove the validity of the messages. In the winner declaration phase, the winner releases the confidential value r_1 to prove his/her validity.

(5) Non-repudiation: Non-repudiation refers to the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they have originated. The winner cannot deny his/her winning bid after the winner declaration phase. If bidder repudiates the signature, Auctioneer can confirm the dishonesty of the signer by disclosing the converted signature (R, S, r) for M_i to AC.

(6) Public verifiability: Public verifiability refers to all participants that can verify the legitimacy of winner's bid. When auctioneer post up (R, S, r) for M_i, anyone can use Eq. (20) to test and verify the legitimacy.

(7) Fairness: Fairness refers to a legal principle allowing for the use of discretion and fairness when applying justice. There shall be a fairness principle for auction. The bidding price M_i transmits using authenticated encryption to protect it. Only the auctioneer can restore M_i using receiving message (R, S, r) and auctioneer's private key x_j. No one has capability to modify the bidding price.

(8) Authentication: Authentication refers to the act of confirming the truth of an attribute of a datum or entity. In the mutual authentication phase, before user communicates with AC, they use MAC_i and MAC_j to verify the identity of each other. User and AC use Diffie-Hellman key exchange to generate share key K_{ij}. Moreover, they can then use this key to continue the secure communications.

Furthermore, Trevathan and Read [27] explained that the security of a secure English auction has 13 conditions. But the proposed protocol is similar to the scopes of Trevathan and Read [27] and Fig.4 lists some comparisons. Security's eight requirements are in [27] too.

Discussing the disadvantages from the Tzeng *et al*. [24], we find that the style of auction is different model now. We hereby propose a scheme with AC, bidder and auctioneer under the control of the AC. Some examples can be seen through Certificate Authorization in Ministry of Interior (MOICA) issuing a certificate to each application for many usages. This certificate can apply to one of the 22 applications such as taxation portal for Ministry of Finance. The operation model can be special practice to the real auction market. But the operation model issued by Tzeng *et al*. [24] has less available to real EC. Since shopping malls or supermarkets are supported by their perspective companies, this is not successful as compared to the characters from the MOICA. Therefore the approach generated by Tzeng *et al*. [24] could not work in this scenario.

V. PERFORMANCE EVALUATION

Time complexity is used for comparison to estimate the cost of operation execution. The symbols are defined as shown in Table 1:

Then we show the performance evaluation in each phase as follows. In the registration phase, the generation of public key for each user requires computation complexity for one T_{exp} for Eq. (1). In the mutual authentication, to auction setup and generate auction key, the computation complexity requires $8T_{EXP} + 4T_H + 1T_E + 1T_D$ for Eq. (2) to Eq. (15). In the convertible authenticated encryption scheme, the signature is (R, S, r).

Therefore, the bidder requires $2T_{exp} + 3T_{MUL} + 1T_H$ to make the message, while verifying the message requires $5T_{EXP} + 2T_{MUL} + 1T_H + 1T_{INT}$ for the winner declaration, it requires $1T_E + 1T_D + 1T_{EXP}$ for Eq. (21) to Eq. (23). Operation of the proposed scheme is low and it is completely reasonable security even the mutual authentication is required. The comparison is listed in Table 2.

The computation of the proposed scheme has one more step of encryption and decryption in declare the winner phase for declaration as compared to that of Tzeng et al. [24]. Since this proposed scheme has the trust CA to issue, some new cryptosystem is required as the declaration should be done. This is the new concept, which this scheme suggests if the real electronic auction is required. As Patel [26] explained that the ecliptic curve cryptosystem (ECC) has small length of keys relative to RSA, ECC can be applied now.

VI. CONCLUSIONS AND FUTURE RESEARCH DIRECTION

6.1 Conclusions

In this work, we proposed a new auction model that satisfies the security requirements of the English auction scheme. It allows the bidder to make bids confidentially without having disclosure of any confidential information to third parties. In mutual authentication phase, the bidder and AC can verify identity of each other. Therefore, no one can find the way to forge it. Our scheme is based on Tzeng *et al*. [24] convertible authentication encryption scheme.

The bidder not only has capability to trace the bidden message but also has non-repudiation to the bidden message. In addition to conversion operator, the cooperation of the bidder is not required. Therefore, our auction model actually solves the obviously conflicting situation.

6.2 Future Research Direction

In order to continue this research work, some research topics can be followed: (1) the new auction model such as e-vote; (2) the value-added digital money can be used in this protocol.

Item No.	**Trevathan and Read [27]**	**The proposed definitions**	**similarity**
1	Unforgeability	Non-forgeability	The same meaning for both schemes
2	Verifiability	Public verifiability	The same meaning for both schemes
3	Exculpability	Convertible signature in Section 3.6	Since the exculpability means that no bidder can provides two different bids in the auction, but convertible signature can confirm the dishonesty signer as exculpability model.
4	Coalition-resistance	Integrity	This mutual authentication is applied as for both protocols, but the same function is used by distinguish words separately.
5	Robustness	Authentication	The same meaning between bidder and auctioneer, no illegal bid can affect the bid process.
6	Anonymity	Anonymity	The same meaning for both schemes
7	One-time registration	Fairness	Bidder can ask for signature to convince before justice decision, just like the one-time registration, bidder can join any bid in the future when auctioneer holds a bid session. Our concept is the similar to the Trevathan and Read [27].
8	Unlinkability	Robustness and reliability in Introduction at Section 1	In Section 1, we describe the meaning of robustness and reliability together, that also implies the meaning of unlinkability since no bidder can trace any bid price other bidders gave before.
9	Traceability	Traceability	The same meaning for both schemes
10	Revocation	Non-repudiation	Our idea is the a fixed right to cancel the bid directly
11	Unskewability	Similar reason	Auctioneer cannot change the timing, it surely exists
12	Unblockability	Similar reason	Auctioneer can selectively block bids on amount or bidder's identity
13	Conditional bid cancellation	Similar reason	When the bid continues, some bidders cannot stay at that time, so the auction policy can make the strictly bid condition.

Fig. 4. Meaning comparisons of English auction security.

Table 1. Definition of computation symbols

Symbol	**Definition**
T_{MUL}	Time complexity for modular multiplication computation
T_{exp}	Time complexity for modular exponentiation computation
T_{INV}	Time complexity for modular inverse computation
T_H	Time complexity for modular hash function computation
T_E	Time complexity for symmetry encryption computation
T_D	Time complexity for symmetry decryption computation

Table 2. Computation comparison is between two approaches.

	The proposed scheme	Tzeng *et al.* [24] scheme
Public key		$1\ T_{EXP}$
Registration phase	$1\ T_{EXP}$	$8T_{EXP}+4T_H+1T_E+1T_D$
Mutual authentication and auction key generation	$8T_{EXP}+4T_H+1T_E+1T_D$	$nT_{EXP}+nT_H\ (2n+1)T_{\mathrm{exp}}$
Auction setup		$(2n+1)T_{EXP}+nT_{MUL}$
Bidding	$2T_{\mathrm{exp}}+3T_{\mathrm{MUL}}+1T_{\mathrm{H}}$	$3T_{EXP}+6T_{MUL}+1T_H$
Verification	$5T_{EXP}+2T_{MUL}+1T_H+1T_{INV}$	$2T_{EXP}+1T_{MUL}+1T_H$
Winner declaration	$1T_E+1T_D+1T_{EXP}$	$T_{EXP}+T_{MUL}+T_H$
Total computation	$17T_{EXP}+6T_H+5T_{MUL}+2T_E+2T_D$ $+1T_{\mathrm{INV}}$	$(3n+16)T_{EXP}+(n+7)T_H+(n+8)T_{MUL}+T_E+T_D$

REFERENCES

[1] Liaw H. T., Juang W. H., and Lin C. K., "An electronic online bidding auction protocol with both security and efficiency," Applied Mathematics and Computation, Vol. 174, Issue 2, pp. 1487-1497, 2006.

[2] Ireland government, "The Quick Guide to Using Electronic Auctions," www.eprocnet.gov.ie/policy-guidance-documents/quick-20guide-20to-20e-auctions.pdf/, 2006.

[3] Oz, E., in Foundations of E-Commerce, Prentice Hall, Pearson Education Inc., NY, 2002.

[4] Whiteley, D., e-Commerce: Strategy, Technologies and Applications, McGraw-Hill International (UK) Limited, NY, 2000.

[5] Brandt, F., "Secure and Private Auctions without Auctioneers," Technical Report FKI-245-02, Department for Computer Science, Technical University of Munich, 2002.

[6] Vickrey, W., "Counterspeculation, Auctions, and Competitive Sealed Tenders," Journal of Finance, Vol. 16, Issue 1, pp. 8-37, 1961.

[7] Chang, C. C. and Chang, Y. F., "Efficient Anonymous Auction Protocols with Freewheeling Bids," Computers and Security, Vol. 22, No. 8, pp. 728-734, 2003.

[8] Jiang, R., Pan, L., and Li, J. H., "An Improvement on Efficient Anonymous Auction Protocols," Computer and Security, Vol. 24, No. 2, pp. 169-174, 2005.

[9] Chen, T. S., "An English Auction Scheme in the Online Transaction Environment," Computers and Security, Vol. 23, No. 5, pp. 389-399, 2004.

[10] Chung, Y. F., Huang, K. H., Lee, H. H., Lai, F. P., and Chen, T. S., "Bidder-Anonymous English Auction Scheme with Privacy an Public Verifiability," The Journal of Systems and Software, Vol. 81, No. 1, pp. 113-119, 2008.

[11] Su P. C., Lu E. H., and Henry Chang K. C., "Cryptographic Identification of Users Based on Inter-mixed Approach," J. Chung Cheng Institute of Technology, Vol. 33, No. 1, Nov., 2004.

[12] Su, P. C. and Tsai, C. H., "Self-Certified Key Exchange Scheme Based on Hybrid Mode Problems," J. Chung Cheng Institute of Technology, Vol. 39, No. 1, May, 2010.

[13] Diffie, W. and Hellman, M., "New Directions in Cryptography," IEEE Trans. Information Theory, Vol. IT-22. No. 6, pp. 644-654, 1976.

[14] Nyberg, K. and Rueppel, R. A., "Message Recover for Signature Schemes based on the Discrete Logarithm Problem," in

Advances in Cryptology – EUROCRYPT, pp. 182-193, 1995.

[15] Horster, P., Michels, M., and Petersen, H., “Authenticated Encryption Schemes with Low Communication Costs,” IEE Electronic Letters, Vol. 30, No. 15, pp. 1212-1213, 1994.

[16] Araki, S., Uehara, S., and Imamura, K., “The limited Verifier Signature and its Application,” IEICE Trans. Fundamentals, Vol. E82-A, No. 1, pp. 63-68, 1999.

[17] Tseng, Y. M., Jan, J. K., and Chien, H. Y., “Authenticated Encryption Schemes with Message Linkages for Message Flows,” Computers and Electrical Engineering, Vol. 29, No. 1, pp. 101-109, 2003.

[18] Hwang, S. J., Chang, C. C., and Yang, W, P., “Authenticated Encryption Schemes with Message Linkages,” Information Processing Letters, Vol. 58, No. 4, pp. 189-194, 1996.

[19] Lee, B., Kim K., and Ma, J., “Efficient Public Auction with One-Time Registration and Public Verifiability,” in Progress in Cryptology — INDOCRYPT, 2247, pp. 162-174, 2001.

[20] Lee, W. B. and Chang, C. C., “Authenticated Encryption Scheme without Using One Way Hash Function,” Electronics Letters, Vol. 31, Issue 19, pp. 1656-1657, 1995.

[21] Lee, W. B. and Chang, C. C., “Authenticated Encryption Scheme with Linkage Between Message Blocks,” Information Processing Letters, Vol. 63, No. 5, pp. 247-250, 1997.

[22] Chen, B. H., “Improvement of Authenticated Encryption Schemes with Linkages for Message Flows,” Computers and Electrical Engineering, Vol. 30, No. 7, pp. 465-469, 2004.

[23] Zhang, Z., Araki, S., and Xiao, G., “Improvement of Tseng et al.’s Authenticated Encryption Scheme with Message Linkages,” Applied Mathematics and Computation, Vol. 162, No. 3, pp. 1475-1483, 2005.

[24] Tzeng, S. F., Tang Y. L., and Hwang, M. S., “A New Convertible Authenticated Encryption Scheme with Message Linkages,” Computers and Electrical Engineering, Vol. 33, No. 2, pp. 133-138, 2007.

[25] Taniar, D., “Mobile Computing: Concepts, Methodologies, Tools, and Applications,” http://books.google.com.tw/books?id=2bJhcy7AlfUC&pg=PA1640&lpg=PA1640&dq=e-auction+%2B+unfairness&source=bl&ots=gp8S4Ps5zh&sig=v6ZXII6FVo3ojnKwPnTBGhPRmDM&hl=zh-TW&ei=lHHAS9ieKJDi7APGlYzDCQ&sa=X&oi=book_result&ct=result&resnum=7&ved=0CC4Q6AEwBg#v=onepage&q=e-auction%20%2B%20unfairness&f=false, 2009.

[26] Patel, V., “Key Sizes Selection in Cryptography and Selection comparison between ECC and RSA”, http://teal.gmu.edu/courses/ECE543/project/reports_2000/patel_report.pdf.

[27] Trevathan, J. and Read, W., “Secure Online English Auctions”, Third Int. Conf. E-Business and Telecommunication Networks, ICETE 2006, Setubal, Portugal, August 7-10, 2006.