# An efficient and anonymous auction protocol

**Fuw-Yi Yang  Cai-Ming Liao**
**Department of Information Engineering, Chaoyang University of Technology**
yangfy@cyut.edu.tw  s9527645@cyut.edu.tw

## Abstract

With the popularization of the network, more and more users make use of the convenience of the network to precede business transactions in the network. In 2006, the researcher proposed an anonymous auction protocol, enable bidders to bid in anonymous cases. The protocol contains initiation phase and anonymous auction phase. However, in the initiation phase, the bidder is unable to be anonymous; therefore, the lawless person will use this opportunity to do something illegal. Once a lawless person, who participates in the auction activity, knows the bidder's identity, he may threaten the honest bidders in order to win the item; this kind of situation make many bidders refuse to bid to avoid damage. In order to solve such the problem, in this paper, we propose an efficient and anonymous auction protocol.

**Keywords:** electronic auction, anonymous, token

## 摘要

隨著網路的普及，越來越多的使用者，想藉由網路環境所帶來的便利性，在網路上進行買賣。在2006年，研究學者提出一個匿名競標的協定，使得投標者能在匿名的情況下進行競標。此協定可細分為加入與競標兩個階段，然而在加入階段中，投標者卻無法匿名；因此，給予不法份子可乘之機，設若彼等也參加競標活動，在得知投標者的身分之後，為了得標，善良的投標者將遭受威脅，或是投標者因害怕受到傷害，而不敢投標。為了解決這樣的問題，在本論文中，我們提出一個有效率且具匿名性的競標協定，解決無法匿名的問題。

關鍵字：電子競標、匿名性、假名

## 1. Introduction

In recent years, the flourishing development and popularization of the network technology provide a new business environment to users, and more and more users do commercial transactions through the network. Electronic auctions become one of the main parts of the electronic commerce gradually. At present, the main auctions types are traditional English auction, Dutch auction, and sealed-bid auction. The mode of traditional English auction is public biding. An auctioneer may set up a floor price and the limit of time and condition to win. Each bidder chooses a price to bid from the bid list; this price must higher than the present floor price. When a bidder reaches the auctioneer's limit of time and condition, the auctioneer will finishes this auction activity and announce who is the winner and the final price he bid. The mode of Dutch auction is very similar to traditional English auction; the only difference is the price: in Dutch auction, the price will be reduced until the first bidder makes a bid. The mode of Sealed-bid auction is different from the traditional English auction and the Dutch auction. All bidders only can throw a sealed bid list in one time. When a bidder reaches the auctioneer's limit of time and condition, the auctioneer will finishes this auction activity and announce who is the winner and the final price he bid.

In 2003, the researcher proposed a simple anonymous auction protocol (Chang Y.F. and Chang C.C., 2003, [1]): the bidder can discuss session key with auctioneer and makes a bid in anonymous condition. In the protocol, the negotiation of session key must be achieved by the initiation and authentication phase; therefore, it is not very efficient.

In order to improve its efficiency, the researcher proposed a new anonymous auction protocol (Chang and Chang, 2006, [2]), which is called C-C Protocol now. According to C-C Protocol, the negotiation of session key and authentication are integrated in the initiation phase, so the efficiency enhance greatly. For the purpose of achieving anonymous auctions, the auctioneer designates a token to the bidders in the initiation phase and the bidders use the token to bid in the auction activity. However, in the initiation phase of C-C Protocol, there are no protect mechanism of bidder's identity, obviously. Once a lawless person participates in the auction activity, after knowing the bidder's identity, the honest bidders will be threatened, because the lawless person will try his best to win the bid at a lower price. It could make some bidder refuse to bid to avoid damage. In such cases, any honest bidder is unable to bid in the security and equity situation. In view of such crisis, we propose an efficient and anonymous auction protocol. In this initiation phase and auction phase of protocol, all bidders needn't expose the identity in the communication with auctioneer; thus, all bidders can bid in the anonymous situation.

Recently, the researcher proposed a "Deniable Authentication Protocol" (Deng X., Lee C.H. and Zhu H., 2001, [3]). Compare to traditional Authentication protocol, the "deniable authentication" protocol has two characteristics which is different from traditional authentication. First, only the intended receiver can identify the true source of a given message. Second, the receiver cannot prove the source of the message to a third party. According to the characteristic of this protocol, if we assume that the receiver is the auctioneer and the sender is the bidder in an auction, after the bidder throws out the bid list, the auctioneer can only identify the true source of the bid list and legitimacy of the price. But the auctioneer is unable to prove the bidder's true identity to other bidders; therefore, the characteristics of "deniable authentication" protocol can be applied to protect personal secrets of these bidders. In 2007, the researcher (Lee W.B., Wu C.C., Tsaur W.J., 2007, [4]) proposed "non-interactive deniable authentication" protocol; this protocol not only can achieve two requiring characteristics of "deniable authentication" protocol, but also reduced the number of communication and negotiation of session key. We incorporate with such technology in our anonymous auction protocol to improve the efficiency of communication and negotiation of session key

In this paper, we will introduce the notation used in this article. In section 3, we will explain and indicate the potentially crisis of exposing the identity of the bidder; in section 4, we will explain the anonymous auction protocol and analyze its efficiency and security.

## 2. Notation

The notations used in this paper are listed as follow:

$E2_{PK}(m)$: an asymmetric encryption algorithm, where PK (publicly published) is the encryption key and $m$ is the message to be encrypted

$S2_{SK}(m)$: an asymmetric decryption algorithm, where decryption key is SK (hold secretly) and $m$ is a ciphertext under decrypting. (Note that some technical literatures treat the result of $S2_{SK}(m)$ as a signature on the message $m$)

$E1_K(m)$: a symmetric encryption algorithm, where $K$ is the secret session key and $m$ is the message to be encrypted

$D1_K(m)$: a symmetric decryption algorithm

P: the just auctioneer

U: the bidder

$ID_U$: the unique identity of U

$(PK_P, SK_P)$: the auctioneer P's public-private key

$(PK_U, SK_U)$: the bidder U's public-private key

$n$, $g$: the public system parameters, where $g$ and $n$ are two large primes as in the Diffie-Hellman protocol

$H(\cdot)$: a collision-free one-way hash function

||: the concatenation symbol

## 3. Reviewed of C-C Protocol

In this section, we will review the C-C Protocol.

In this protocol, there exists a certificate authority (CA), a just auctioneer P and the bidders $U_i$ ($1 < i < m$). All bidders U and the auctioneer P respectively own private-public key ($SK_U$, $PK_U$), ($SK_P$, $PK_P$); where private key $SK_U$ and $SK_P$ is respective chosen by the U and P in secret, the public key $PK_U$ and $PK_P$ is issued to pass through CA identifies. The protocol contains initiation phase and anonymous auction phase.

We will show that the negotiate process of the session key in subsection 3.1 (initiation phase); in subsection 3.2, discuss the C-C Protocol unable to hide the identity of bidder, some crises will exist.

### 3.1 Initiation phase

The following five steps are performed to have P and U achieve the verification of identity and the negotiation of session key. Fig. 1 shows the process of initiation phase.

**1.** The U performs the following job:
- **1.1** chooses a random large number $a$, computes $X = g^a \bmod n$ and $X' = S2_{SK_U}(X)$.
- **1.2** sends $X$, $X'$ and $ID_U$ to P.

**2.** After receiving ($X$, $X'$, $ID_U$), the P performs the following job:
- **2.1** verifies $X \stackrel{?}{=} E2_{PK_U}(X')$; if not equal, stops to perform.
- **2.2** chooses a random large number $b$, computes $Y = g^b \bmod n$, $Y' = S2_{SK_P}(Y)$, $K = X^b \bmod n = g^{ab} \bmod n$, $H_1 = H(ID_U||X||Y)$ and $W = E1_K(AID_U||H_1)$, where $AID_U$ is a token selected by P.
- **2.3** sends $Y$, $Y'$ and $W$ to U.

**3.** After receiving ($Y$, $Y'$, $W$), the U performs the following job:
- **3.1** verifies $Y \stackrel{?}{=} E2_{PK_P}(Y')$; if not equal, stops to perform.
- **3.2** computes $K = Y^a \bmod n = g^{ab} \bmod n$ and decrypts, $AID_U||H_1 = D1_K(W)$.
- **3.3** verifies $H(ID_U||X||Y) \stackrel{?}{=} H_1$; if not equal, stops to perform.
- **3.4** computes $Z = E1_K(AID_U||H_2)$, where $H_2 = H(Y||Y'||W)$.
- **3.5** sends $ID_U$ and $Z$ to P.

**4.** After receiving ($ID_U$, $Z$), the P performs the following job:
- **4.1** decrypts, $AID_U||H_2 = D1_K(Z)$.
- **4.2** verifies $H(Y||Y'||W) \stackrel{?}{=} H_2$; if not equal, stops to perform.

**5.** Now, the U and P share a session key $K$ and token $AID_U$.

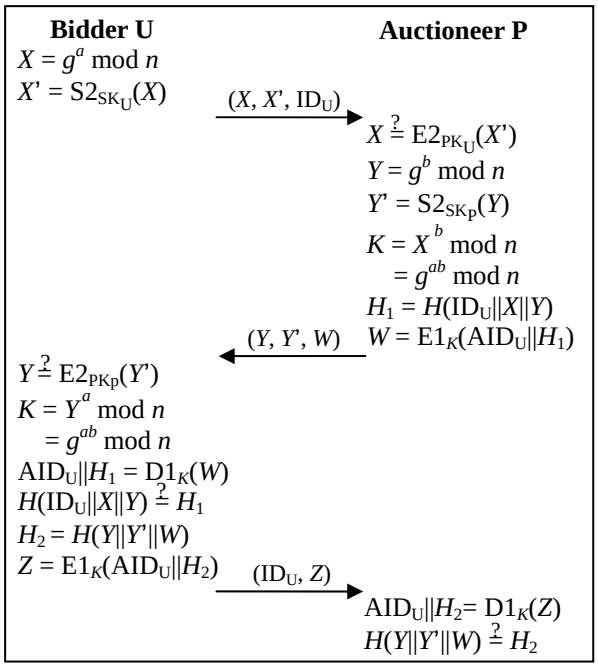


**Fig. 1 C-C Protocol initiation phase**

### 3.2 Discuss

Obviously, in the initiation phase, the identity of bidder U use as plaintext send with P on the communication, and there is no mechanism of any protection. In a situation that such the identity of U is exposed, suppose a lawless persons participate in the auction activity, after learning the bidder's identity, in order to win the item or want to win the bid thing at lower price, therefore threaten or injury to the honest bidders; Under so insecure a situation, all honest bidders will not dare to bid only because of subject to threaten, or not dare to participate the auction activity only because of subject to injury.

In order to facilitate follow-up comparison, the anonymous English auction phase of C-C Protocol is shown in the Fig. 2; the Fig. 3 shows the process of anonymous Sealed-bid auction phase.

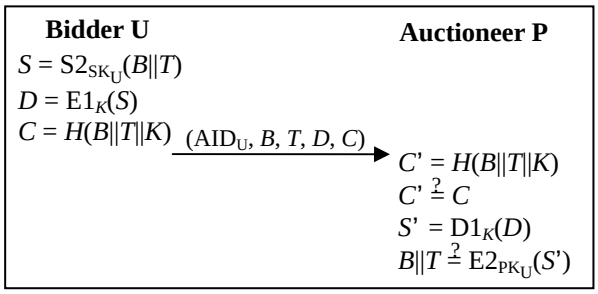


**Fig. 2 C-C Protocol English auction phase**

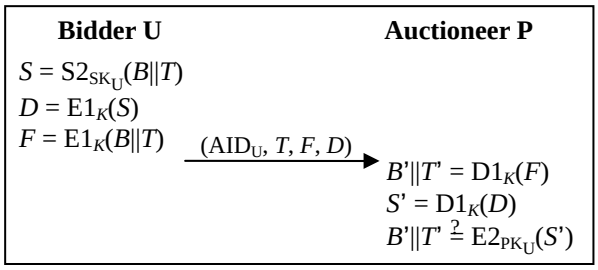


**Fig. 3 C-C Protocol Sealed-bid auction phase**

## 4. Our protocol

Because above-mentioned problems, we will propose an efficient and hide the identity of bidder auction protocol, solves such problem. In our protocol, the identity of all bidders protected with the auctioneer on the communication. The bidder anonymously agrees the session key and mutual authentication with the auctioneer in the initiation phase and the auctioneer chooses a token to the bidder. The bidder uses the token to bid in the auction phase, therefore achieve the anonymous goal.

In subsection 4.1, we will show that the U and P in the anonymous cases, how to agree session key and mutual authentication; in subsection 4.2 and 4.3, shows that improved the auction process of the English auction, Dutch auction and Sealed-bid.

### 4.1 Initiation phase

In the initiation phase, The U and P respectively own private-public key ($X_U$, $Y_U = g^{X_U} \bmod n$), ($X_P$, $Y_P = g^{X_P} \bmod n$), where private key $X_U$ and $X_P$ are respective chosen by the U and P in secret, the public key $Y_U$ and $Y_P$ is issued by CA identifies. The U agrees a share session key with P in the initiation, and chooses a token $P_U$ to U by P. There are four steps performed in initiation phase as follow. Fig. 4 shows the process of initiation phase.

**1.** The U performs the following job:

**1.1** chooses a random large number $a$, computes $r = Y_U^{\,a} \bmod n$, $K = (Y_P)^{X_U \cdot a} \bmod n$, $G = E1_K(ID_U)$ and $MAC = H(K||ID_U)$.

**1.2** sends ($r$, $G$, $MAC$) to P.

**2.** After receiving ($r$, $G$, $MAC$), the P performs the following job:

**2.1** computes $K = r^{X_P} \bmod n$ and decrypts, $ID_U = D1_K(G)$.

**2.2** verifies $H(K||ID_U) \stackrel{?}{=} MAC$; if not equal, stops to perform.

**2.3** $P_U$ is a token chosen by P for U, and computes $Z = E1_K(P_U||ID_U)$; where $P_U = E1_K(ID_U||t)$, $t$ is a random number chosen by P, start the initiation phase to reselect in each time, the byte length of $t$ varies with security level, such as $|t| = 80$.

**2.4** sends $Z$ to U, and stores the ($P_U$, $ID_U$, $t$, $K$) to database.

**3.** After receiving $Z$, the P performs the following job:

**3.1** decrypts, $P_U||ID_U = D1_K(Z)$.

**3.2** checks $ID_U$; if is invalid, stops to perform.

**4.** Now, U and P share a session key $K$ and token $P_U$.

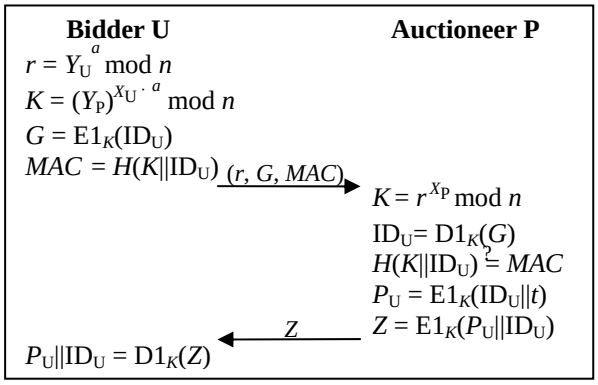


**Fig. 4 Initiation phase**

### 4.2 Anonymous English and Dutch auction phase

The auction mode of the English and Dutch auction is almost similar. Take English auction as the example, each bidder uses the session key $K$ and token $P_U$ to bid. There are three steps performed in English auction phase as follow. Fig. 5 shows the process of anonymous English auction phase.

**1.** The U performs the following job:

**1.1** chooses a bidding price $B$, and computes $W = H(B||P_U||K)$.

**1.2** sends $B$, $P_U$ and $W$ to P.

**2.** After receiving ($B$, $P_U$, $W$), the P performs the following job:

**2.1** Using $P_U$ as indexing key value, finds out the record ($P_U$, $ID_U$, $t$, $K$) from the database, and verifies $ID_U||t \stackrel{?}{=} D1_K(P_U)$; if not equal, regards as nullity bid.

**2.2** verifies $H(B||P_U||K) \stackrel{?}{=} W$; if not equal, regards as nullity bid.

**3.** When a bidder reaches the auctioneer's limit of time and condition, the auctioneer will finishes this auction activity, and performs the following job:

**3.1** Publish bid-winning price.

**3.2** Publish name of winning bidder as $ID_U$.

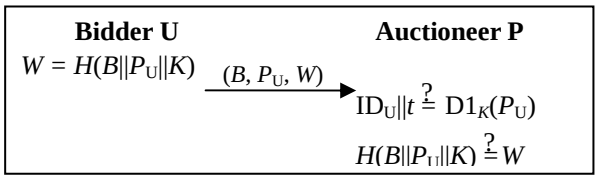


**Fig. 5 Anonymous English auction phase**

### 4.3 Anonymous Sealed-bid auction phase

When anonymous sealed-bid auctions beginning, all bidders used the $K$ and $P_U$ to bid. There are three steps performed in Sealed-bid auction phase as follow. Fig. 5 shows the process of anonymous Sealed-bid auction phase.

**1.** The U performs the following job:

**1.1** chooses a bidding price $B$, and computes $F = E1_K(B||P_U)$ and $W = H(B||K)$.

**1.2** sends $P_U$, $F$ and $W$ to P.

**2.** After receiving ($P_U$, $F$, $W$), the P performs the following job:

**2.1** Using $P_U$ as indexing key value, find out the record ($P_U$, $ID_U$, $t$, $K$) from the database, and verify $ID_U||t \stackrel{?}{=} D1_K(P_U)$; if not equal, regards as nullity bid

**2.2** decrypts, $P_U||B = D1_K(F)$, and verifies $H(B||K) \stackrel{?}{=} W$; if not equal, regards as nullity bid.

**3.** When a bidder reaches the auctioneer's limit of time and condition, the auctioneer will finishes this auction activity, and performs the following job:

**3.1** Publish bid-winning price.

**3.2** Publish name of winning bidder as $ID_U$.

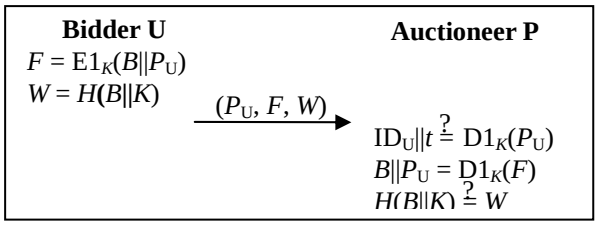


**Fig. 6 Anonymous Sealed-bid auction phase**

## 5. Protocol Analyses

Our protocol is anonymous in the initiation and auction phases. All bidder tender a bid under the security and equity situation, and only uses lighter algorithm and communication cost in the auction activity, enhances the efficiency of auction activity greatly. Under the two subsections, we will be aimed at the security and efficiency of our protocol to analyze.

### 5.1 Security Analyses

Property 1: *Man-in-the-middle Attacks*

In our protocol, sets up the mechanism of mutual authentication, if an attacker wants to falsify ($r$, $G$, $MAC$) among parameters, the P will unable to compute the correct $K$ value and decrypt to get the $ID_U$ of valid, and successfully verify the $MAC$; if an attacker wants to falsify $Z$' and sends to the U, due to unable to obtain or compute the $K$ value; where $K = r^{X_P} \bmod n = (Y_P)^{X_U \cdot a} \bmod n = g^{X_P \cdot X_U \cdot a} \bmod n$, the $X_P$ and ($X_U$, $a$) are secret parameter of the P and U, respectively, any person unable to obtain or know; consequently, an attacker unable to send a $Z$' of valid, enable to successfully verify $P_U||ID_U \stackrel{?}{=} D1_K(Z')$. We proposed protocol can safeguard against the Man-in-the-middle Attacks.

Property 2: *Replay Attacks*

In our protocol, the P and U choose disparity $a$ and $b$ in each auction activity, respectively. All communication parameters ($r$, $G$, $MAC$, $Z$, $P_U$, $B$, $F$, $W$) are all different in each auction activity. In initiation

phase and auction phase, all communication parameters are all different. An attacker can not use the parameters of initiation and use at the auction. Therefore, we proposed protocol can safeguard against the replay attacks.

Property 3: *Impersonation Attacks*

In initiation, only the designate P can correctly compute $K = r^{X_P} \bmod n$ and $ID_U = D1_K(G)$ to verify *MAC* by uses own private key $X_P$. In anonymous auction phase, only the designate P can verify the $P_U$ and obtain the correctly $K$ value from database. Therefore, an attacker can not to verify and open the bid by impersonate the auctioneer. Our protocol can safeguard against the impersonation attacks.

### 5.2 Efficiency Analyses

In following Table 1, we aimed at our protocol and C-C Protocol, analyses the efficiency of the communication number, communication cost and exponential Computation in the initiation phase and anonymous auction phase. Suppose in the public key cryptosystems, the secret level sets up the bit size of $n$ is 1024 bits ($|n| = 1024$), $|ID_U|$, $|P_U|$, $|AID_U|$, $|B|$ and $|T|$ are 160 bits, the $H(\cdot)$ is 128 bits in the MD5 ($|H(\cdot)| = 128$), the symmetric cryptosystems if uses the AES for 128 bits. Due to the computation cost of exponential operation is great than the computation cost of the hash function and symmetric cryptosystems. Therefore in the analyses of computation cost, we will neglect the two items.

**Table 1 Efficiency analyses**

| | Protocol | C-C Protocol | | Our protocol | |
|---|---|---|---|---|---|
| | | U | P | U | P |
| Initiation phase | Communication number | 3 | | 2 | |
| | Communication cost(bits) | 4672 | | 1408 | |
| | Exponential Computation | 4 | 4 | 2 | 1 |
| English and Dutch auction | Communication cost(bits) | 736 | | 416 | |
| | Exponential Computation | 1 | 1 | 0 | 0 |
| Sealed-bid auction | Communication cost(bits) | 576 | | 384 | |
| | Exponential Computation | 1 | 1 | 0 | 0 |

From the table 1, we can know that in our protocol, the session key is determined by the U; it's not generated by the mutual negotiates of U and P. Therefore, it reduced the number of the communication and computation cost in the negotiation. The parameter we used is generated by a hash function or a symmetric cryptosystem, so the number of communication and the cost of computation we need are reduced. Because the P stores up the ($ID_U$, $t$, $P_U$, $K$) to the database in the initiation phase, the U only needs to use a operation of hash function or symmetric cryptosystem in the auction phase, then, the P can verify the bid list.

## 6. Conclusions

Our protocol can effectively achieve perfect anonymous. Solve the Bidder's identify has not protected in the initiation phase, therefore, will be threatened and injured. In efficiency, we use lighter algorithm to reduce the communication cost and computation cost. In future, we will continue studying the lighter communication cost and computation cost.

## 7. References

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

[2] Chang, C.C. and Chang, Y.F., "Enhanced Anonymous Auction Protocols with Freewheeling Bids," IEEE Advanced Information Networking and Applications, Vol. 1, April 2006.

[3] Deng, X., Lee, C.H. and Zhu, H., "Deniable Authentication Protocols," IEE Proceedings of Computers and Digital Techniques, Vol. 148, March 2001, pp. 101-104. [4] Lee W.B., Wu C.C., Tsaur W.J., "A novel deniable authentication protocol using generalized ElGamal signature scheme," Information Science, Vol. 177, Issue 6, March 2007, pp. 1376-1381.