An Anonymous Auction Protocol Based on GDH Assumption

Fuw-Yi Yang and Cai-Ming Liao
(Corresponding author: Fuw-Yi Yang)

Department of Computer Science and Information Engineering, Chaoyang University of Technology
Taichung County 41349, Taiwan, R.O.C. (Email: {yangfy, s9527645}@cyut.edu.tw)
(Received Nov. 23, 2009; revised and accepted Mar. 17, 2010)

Abstract

The popularization and conveniences of Internet have changed traditional auction transactions into electronic auction via Internet. In 2006, Chang and Chang proposed an anonymous auction that enabled bidders to bid in anonymous cases without any bonds. However, in the initiation phase, the bidder is unable to be anonymous as there is no mechanism to protect his (her) identity. Therefore, the lawless person might take this chance to do something illegal. Once the latter, who participates in the auction activity, knows the bidder's identity, he may threaten the honest bidder to become the bid winner. This situation may make bidders refuse to bid to avoid damages. To solve the above mentioned matter, in this paper, we propose an efficient anonymous auction protocol, to protect all bidders' identities in both initiation and auction phases with low levels of computation and communication: only 27% and 50% of Chang and Chang protocol, respectively. A problem in anonymous auction protocol is that bidder A impersonates bidder B to participate an auction. This may be harmful to bidder B. We prove the proposed auction protocol is secure against this attack as it is based on the Gap Diffie-Hellman (GDH) assumption.

Keywords: Anonymous auction, deniable authentication, electronic auction, gap Diffie-Hellman assumption, public-key cryptosystem

1 Introduction

In the past few years, the booming of Internet which provides a new transaction environment for all bidders, attracts more and more people to do electronic (e-commerce), therefore, electronic auction becomes one of the important items in e-commerce. Nowadays, auctions that are familiar to many people are: ascending-price auction (English auction), descending-price auction (Dutch auction), sealed-bid auction, and others. English auction is public bidding where bids are broadcast to all participants. After the auctioneer sets up a floor price and the limit of time and condition to win bids, each participant might choose his (her) bid from a bid list. This bid price must be higher than the current floor price. When a bidder reaches the auctioneer's limit of time and condition, the auctioneer will end the auction activity and announce who is the winner and the final price he bid. Dutch auction and English auction are almost similar; the only difference between them is in Dutch auction the price will be reduced from the highest until the first bidder makes a bid. Different from both said auctions, sealed-bid auction can execute in a single-round of communication between the bidders and the auctioneers. 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 end the auction activity and announce who are the winner and the final price he bid.

In 2003, Chang and Chang proposed a simple and efficient anonymous auction protocol [3], the bidder can negotiate via session key with the auctioneer, and makes a bid under anonymous status. However, in the protocol, the negotiation of session key and check of identity must be achieved by the initiation and authentication phases (number of communication is 4), therefore it is not very efficient. In order to improve communication cost, in 2006, Chang and Chang proposed an efficient anonymous auction protocol [4] 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 (number of communication is 3), so the efficiency enhances greatly. However, in the initiation phase of C-C protocol, there is no mechanism to protect the bidder's identity, obviously. After knowing the bidder's identity, a lawless person might threaten the honest bidder, because the lawless person will try by all means to win the bid at a lower price. In some countries, bidding without the bidder's name is required if the auctions are held by opposition party. In the cases stated above, any honest bidder is unable to bid in security and equity situation. It could make some bidders refuse the bid to avoid damages.

In this paper, we propose an anonymous auction protocol. In the initiation and auction phases of protocol, all

bidders can bid under anonymous status with security. In the initiation phase, with key distribution mechanism, the bidder will generate a session key to encrypt his identity, and the bidder will be provided a token (anonymous bidding name) by the auctioneer. In the auction phase, this token will be used in anonymous status; as a result all bidders will be unidentified during their business transactions. Also, the proposed protocol is more efficient than C-C protocol in computational cost and communication bandwidth; we'll discuss it in Section 4.1.

The "non-interactive deniable authentication" protocol [7] inspired the design of our initiation phase. Compared with the traditional authentication protocol, the "deniable authentication" protocol [5] has two characteristics different from the traditional authentication. First, only the intended receivers can identity the true source of a given message. Second, the receiver cannot prove the source of the message to the third party. According to the character 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 identity the true 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. Therefore, a "deniable authentication" could protect the privacy, rights and benefits of the bidder, reach a fair auction.

Electronic auction is always associated with money matters, the bidder only feels secure during business transaction if there is a guarantee of electronic auction of protocol's security. A malicious bidder A may impersonate bidder B to join an auction. This is called impersonation attack. Bidder B may suffer from this attack. Therefore, we discuss more details about security of electronic auction protocol in Section 4. Theorem 1 proves this protocol is secure against impersonation attack based on Gap Diffie-Hellman (GDH) assumption, i.e. the GDH problem has been solved efficiently. Namely, the security is based on mathematical difficult problem. More details are postponed to Section 4.2.

2 Review of C-C Protocol

2.1 C-C Protocol

In this protocol, there exist a certification authority (CA), a just auctioneer P and m bidders U_i $(1 \leq i \leq m)$. The public system parameters include n and g, where n is a large prime as in the Diffie-Hellman protocol and $g \in Z_n^*$ with large prime order. A just auctioneer P's secret-public key pair is denoted by (SK_P, PK_P). Similarly, bidder U_i holds secret-public key pair (SK_i, PK_i) and is with unique identity ID_i. Let $E2_{PK}(m)$ denote an asymmetric encryption algorithm, where PK (publicly published) is the encryption key and $m \in Z_n$ 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. In addition to asymmetric encryption/decryption algorithms, C-C protocol requires symmetric encryption/decryption algorithms, $E1_K(m)$ and $D1_K(m)$, where K is the secret session key. Let $H(\cdot)$ be collision-resistant hash function, and T be a timestamp. The symbol "$\|$" is the concatenate operator of strings. In a practical implementation, the quantities n, g, SK_P, PK_P, SK_i and PK_i are numbers with bit length 1024 or more. The asymmetric encryption/decryption algorithm could be RSA cryptosystem [2, 10] and symmetric encryption/decryption algorithms AES cryptosystem [1].

Auction activity consists of two phase: Initiation and auction phases as follows.

2.1.1 Initiation Phase

At first, U_i must discuss, verify its identity with P via session key K_i in the initiation phase. Then P attributes a token to U_i instead of identity; in the auction phase, U_i shall make anonymous auction under this token. The initiation phase is displayed in the following Figure 1:

1) U_i chooses a random number a_i, and computes $X = g^a \bmod n$ and $X' = S2_{sk}(X)$, then sends X, X', ID_i to P.

2) After P receives X, X', ID_i, verifies $X \stackrel{?}{=} E2_{PK}(X')$; if not equal, stop performing. On the contrary, P chooses a random number b, and computes $Y = g^b \bmod n$, $Y' = S2_{SK_p}(Y)$, $K_i = X^b = g^{a_i b} \bmod n$ and $W = El_{k_i}(AID_i \| H(ID_i \| X \| Y))$; where AID_i is the token attributed to U_i by the P. Sends Y, Y', W to U_i.

3) After U_i receives Y, Y', W, verifies $Y = E2_{PK_p}(Y')$; if not equal, stop performing; otherwise, U_i computes $K_i = Y^{a_i} = g^{a_i b} \bmod n$ and decrypts $AID_i \ \|H'(ID_i\| \ X\|Y) = Sl_{K_i}(W)$, Verifies $H'(ID_i \| X \| Y) = H(ID_i \| X \| Y)$; if not equal, stop performing; otherwise, continue to compute $Z = El_{k_i}(AID_i \| H(Y \| Y' \| W))$ and sends (ID_i, Z) to P.

4) After P receives (ID_i, Z), decrypts $AID_i \ \| \ H'(Y \| Y' \| W) = Sl_{K_i}(Z)$ and verifies $H'(Y \| Y' \| W) = H(Y \| Y' \| W)$; if not equal, stop performing.

5) At this time, U_i and P have the same session key U_i and P is the token of U_i.

2.2 Discussion

It is obvious that in the initiation phase, when the bidder U_i sends the auctioneer P his (her) identity under plaintext ID_i in their communication, there is no mechanism to protect bidder's identity. Once a lawless person who takes part in the auction activity, after knowing the bidder's identity, might threaten the honest bidder, because

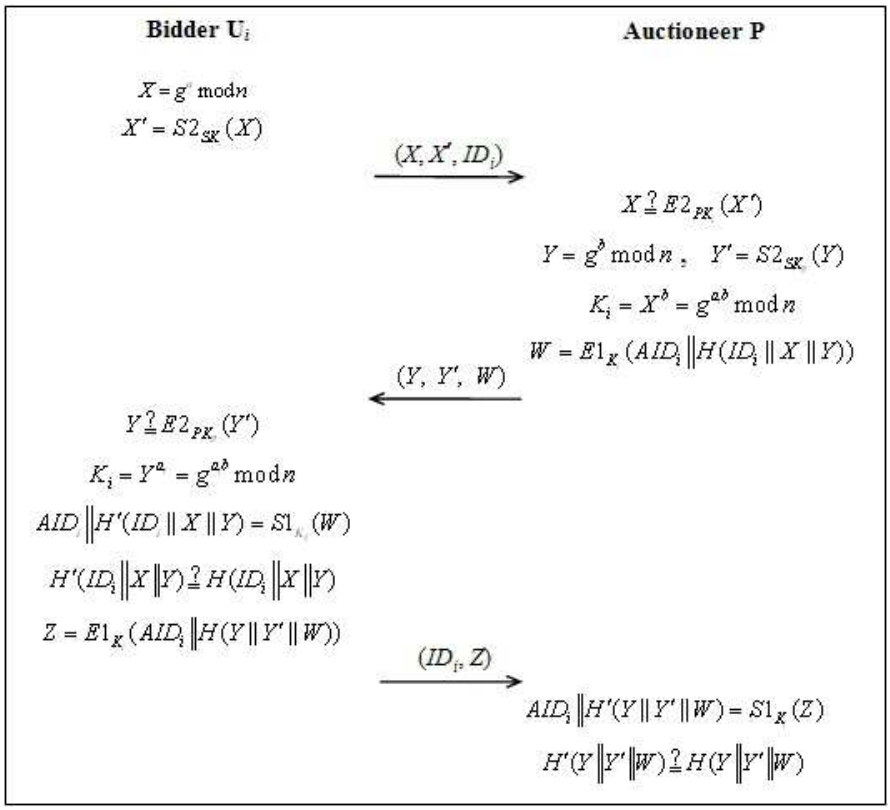

Figure 1: C-C protocol - Initiation phase

the lawless person will try his (her) best to win the bid at lower price. It could make some bidders to refuse the bid to avoid damages. In such cases, honest bidder will not dare to participate the auction activity under insecurity and non-equity situation.

In order to facilitate later comparison, English auction phase of C-C protocol is shown in Figure 2, whereas the process of sealed-bid auction is shown in Figure 3.

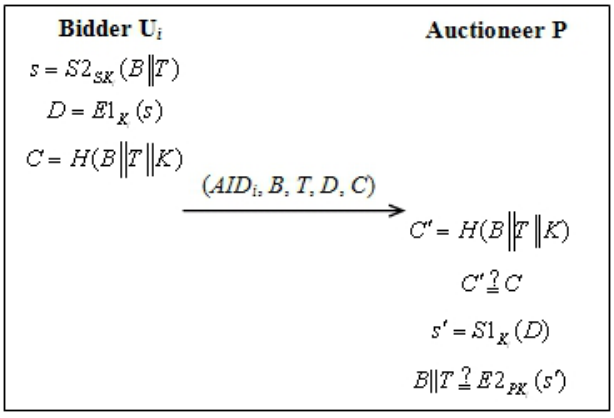

Figure 2: C-C protocol - English auction phase

3 Our Protocol

In order to sort out the problems induced by disclosure of bidder's identity mentioned at Section 2.2, we propose an anonymous auction protocol that may hides the bidder's identity during communication with the auctioneer. In the initiation phase, the bidder uses the session key K_i and agrees mutual authentication with auctioneer, and the latter computes a token P_i for the said bidder who could use it in the auction phase. When the bidder communicates with the auctioneer, identities of other bidders are protected and the matter of identity exposure is settled. Our protocol comprises two phase: initiation and auction phases, as follows.

3.1 Initiation Phase

Suppose the bidder U_i wants to join an auction. In the initiation phase, the U_i generates a session key K_i to encrypt its identity when communication with the auctioneer P and a token is computed by the P. In the auction phase, the U_i shall make anonymous auction under this token. Protocol system parameter establishment: Let p and q are two large prime such that $q|p-1$, $Z_p = \{0, 1, \ldots, p-1\}$ be a addition group of modulo p, be a multiplicative group of modulo p, Z_q be a addition group of modulo q; $g \in Z_p^*$ and the order is q, is a cycle group generated by g, $|G|$ stands for the set element

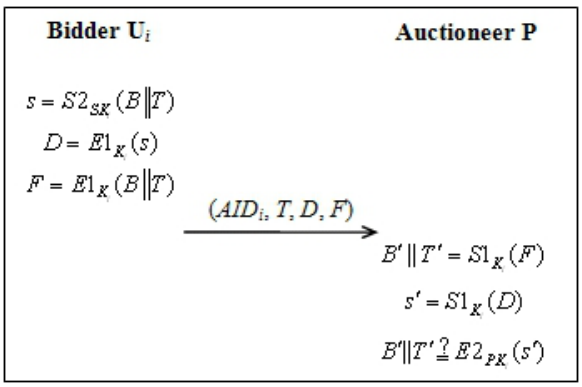

Figure 3: C-C protocol - Sealed-bid auction phase

number of G; let $H(\cdot)$ be collision-resistant hash function with output value corresponding to Z_q, $H_K(\cdot)$ be collision-resistant keyed hash function with output value corresponding to Z_q. The symbol "$\|$ " is the concatenate operator of strings; $E1(\cdot)$ and $D1(\cdot)$ are respectively symmetric encryption/decryption functions, $E2(\cdot)$ and $D2(\cdot)$ are public-key encryption/decryption functions, respectively. The $U_i(1 \leq i \leq m)$ chooses a secret key X_i from Z_q and the corresponding public key $X_i = g^x \bmod p$, is the U_i's identity; the P chooses a secret key y from Z_q and the corresponding public key $Y = g^y \bmod p$. The P has the additional public encryption key pub_b and decryption key sec_p. Public key X_i and Y are verified via certificate center (and electronic certification as well). The initiation phase process is illustrated in the following Figure 4:

1) At first, the U_i performs the following jobs:
   a. Choosing a random number $a \in Z_q$ and obtain a timestamp T, computing $t = H(T\|a)$, $K_i = Y^{x_i t} \bmod p$ and $C = E2_{pub_p}(T\|a\|a\|ID_i\|K_i)$;
   b. Sending C to P.
2) After P receives C, the P performs the following jobs:
   a. Decrypting $D2_{sec_p}(C) = (T\|a\|a\|ID_i\|K_i)$;
   b. Checking if T and ID_i are legal user and timestamp. If they are legal, continue to compute $t = H(T\|a)$ and verify $X_i^{yt} = K_i \bmod p$; if not equal, stop performing; otherwise, the value that P gets from is (T, a, ID_i, K_i) correct, continue performing;
   c. Computing $P_i = H(ID_i\|t)$ and $MAC = H_{K_i}(ID_i\|ID_p\|P_i)$, where P_i is the token of the bidder in replacement of its identity in the auction phase;
   d. Sending MAC to U_i and saving (ID_i, P_i, K_i) in the database.
3) After U_i receives MAC, the U_i performs the following jobs:
   a. Computing $P_i = H(ID_i\|t)$;
   b. Verifying $MAC = H_{K_i}(ID)i\|ID_p\|P_i)$; if not equal, stop performing; otherwise, the value that P gets from (K_i, ID_i, P_i) is correct, continue performing.
4) At this moment, U_i and P share the session key K_i and token P_i.

3.2 Anonymous English and Dutch Auction Phase

The auction mode of English and Dutch auction is almost similar. Let's take English auction as example. Each bidder uses the session key K_i and token P_i to bid. There are three steps performed in English auction and Figure 5 shows the process of anonymous English auction phase.

1) The U_i performs the following jobs:
   a. Choosing a bidding price B and timestamp T, computing $W = H_{K_i}(B\|T\|P_i)$;
   b. Sending (B, T, P_i, W) to P.
2) After P receives (B, T, P_i, W), the P performs the following jobs:
   Using P_i as index key value, searching for the record (ID_i, P_i, K_i) in the database, verifying $W = H_{K_i}(B\|T\|P_i)$; if not equal, regarding as nullity bid; otherwise, such bid and bidding price are legal.
3) When a bidder reaches the auctioneer's limit of time and condition, the auctioneer will end the auction activity and perform the following jobs:
   a. Announcing the bid-winning price;
   b. Announcing name of the bid winner as ID_i.

3.3 Anonymous Sealed-Bid Auction Phase

When sealed-bid auction begins, all bidders use the K_i and P_i to bid. There are three steps performed in a sealed-bid auction and Figure 6 shows the process of anonymous sealed-bid auction phase.

1) The U_i performs the following jobs:
   a. Choosing a bidding price B and timestamp T, computing $F = E1_{K_i}(B|\ T)$ and $W = H_{K_i}(B|\ T\|P_i)$;
   b. Sending (P_i, F, W) to P.
2) After receiving (P_i, $F4$, W), the P performs the following jobs:
   a. Using P_i as index key value, searching for the record (ID_i, P_i, K_i) in the database.
   b. Decrypting $B\|T = D1_{K_i}(F)$, verifying $W = H_{K_i}(B\|T\|P_i)$; if not equal, regarding as nullity bid; otherwise, such bid and bidding price are legal.

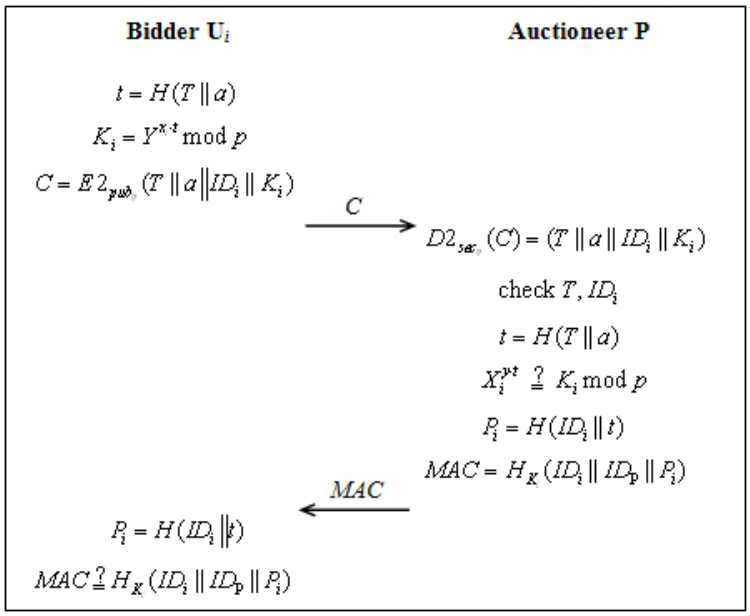

Figure 4: Initiation phase

3) When a bidder reaches the auctioneer's limit of time and condition, the auctioneer will end the auction activity and perform the following jobs:

   a. Announcing the bid-winning price;
   b. Announcing name of the bid winner as ID_i.

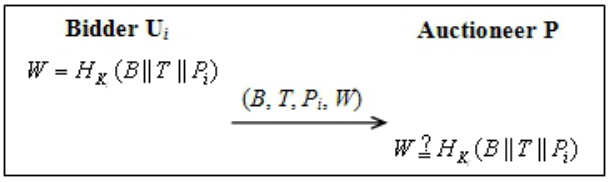

Figure 5: Anonymous English auction phase

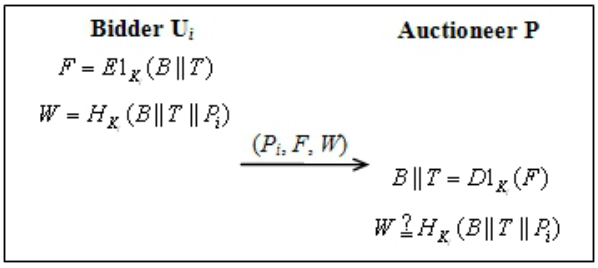

Figure 6: Anonymous sealed-bid auction phase

4 Protocol Analyzes

In this section, we will analyze the security and efficiency of our protocol.

4.1 Efficiency Analyzes

In the following Table 1, we will analyze our protocol and C-C protocol based on three factors: the number of communication, communication cost and exponential computation in the initiation phase and auction phase. Suppose in the public-key cryptosystems, the secret level that sets up the bit size of modulo n and p are 1024 bits ($|n| = 1024$, $|p| = 1024$), the bit size of modulo q is 160 bits ($|q| = 160$); the public-key encryption function $|E2_{pub_p}(\cdot)|$ is 1248 bits ($|E2_{pub_p}(\cdot)| = 1248$); —$ID_i$—, $|B|$ and $|T|$ are 32 bits; $|P_i|$ and $|AID_{U_i}|$ are 160 bits; the collision-free one way hash function $H(\cdot)$ and $H_K(\cdot)$ produces string of 160 bits ($|H(\cdot)| = |H_k(\cdot)| = 160$). As the computation cost of exponential operator is greater the computation cost of the hash function and symmetric cryptosystems, we will neglect the two items in our analysis.

From the Table 1, we know that in our protocol, the session key K_i is determined by the U_i and not generated by the mutual negotiation of U_i and P. Therefore, it reduces the number of communication and computation cost in the negotiation via session key. The bidder U_i only sends the ciphertext C to the auctioneer to complete session key verification and authentication, so the number of communication and the cost of computation we need are reduced. As the P stores (ID_i, P_i, K_i) in the database in the initiation phase, the U_i only needs to use an operator of hash function and symmetric cryptosystem in the auction phase, the P can verify the legality of bid list according to the information of its database.

4.2 Security Analysis

This section goes further steps to prove the security of our protocol based on Gap Diffie-Hellman (GDH) assump-

Table 1: Efficiency analyzes

Protocols		C-C Protocol	Our Protocol
		U — P	U — P
Initiation Phase	Communication Number	3	2
	Communication Cost (Bits)	4800	1480
	Exponential Computational	4 — 4	2 — 2
English and Dutch Auction Phase	Communication Cost (Bits)	1480	384
	Exponential Computational	1 — 1	0 — 0
Sealed-bid Auction Phase	Communication Cost (Bits)	1280	384
	Exponential Computational	1 — 1	0 — 0

tion, Computational Diffie-Hellman (CDH) assumption and Decision Diffie-Hellman (DDH) assumption. The following gives a brief description for CDH, GDH, and DDH together with examples, for further details, please refer [6, 8, 9, 11].

Suppose G is a multiplicative group, the order of which is a large prime q; $g \in G$ and g could generate the multiplicative group G. The CDH problem as follows: randomly chooses two large numbers X and Y from G, finds $Z = g^{xy} \in G$, where $x = \log_g^X$ and $y = \log_g^Y$. The CDH assumption implies that CDH problem is hard to solve. Namely, the probability of solving CDH problem is negligible. An example will help to describe it. Let $p = 227$, $q = 113$ and $g = 3$ be system parameters. Then $G = \{g^i \bmod p | i = 1, 2, \ldots, q\}$. Assume that $x = 23$ and $y = 31$. The quantities X and Y are: $X = g^x \bmod p = 3^{23} \bmod 227 = 7$, $Y = g^y \bmod p = 3^{31} \bmod 227 = 73$. The CDH assumption states that only given X, Y, and system parameters (g, p, q), it is hard to compute $Z = g^{xy} \bmod p$. In the example above $Z = g^{xy} \bmod p = 3^{23*31} \bmod 227 = 11$.

Other parameters of CDH and DDH problem are similar as follows: As G chooses randomly three large numbers X, Y and Z, we check whether z is equal to xy modulo $q(z \stackrel{?}{=} xy \bmod q)$, where $x = \log_g^x$, $y = \log_g^Y$ and $z = \log_g^Z$. Namely, given three random numbers $X = 7$, $Y = 73$ and $Z = 11$, together with system parameters (g, p, q); DDH assumption requires that it is hard to determine whether ($\log_3^7 \bmod 227$) ($\log_3^{73} \bmod 227$) is equal to ($\log_3^{11} \bmod 227$) mod 113. In the above, the tuple (X, Y, Z) is called a valid Diffie-Hellman tuple if $z = xy \bmod q$.

Parameters are similar to CDH and DDH problems. GDH problem states that: given the DDH oracle solve CDH problem, where DDH oracle is a deterministic algorithm answers whether a given tuple (X, Y, Z) is a valid Diffie-Hellman tuple. Again let an example illustrate GDH problem. Given a pair (X, Y), a DDH oracle and system parameters (g, p, q), we want to compute the quantity $Z = g^{xy} \bmod p$ (the quantities of x and y are unknown). While solving the quantity $Z = g^{xy} \bmod p$, a DDH is available to answer whether (X', Y', Z') is a valid Diffie-Hellman tuple. The GDH assumption implies that CDH problem (finding $Z = g^{xy} \bmod p$) is hard to solve, despite the assistance of DDH oracle. The assumption seems strange, because by asking DDH oracle at most $q - 2$ times we obtain the answer. However, in practical implementation q is as large as 2^{160}. Group G contains q elements make exhaustive search infeasible.

The information about bidder (name, account number, address, etc.) does not expose either in the initiation phase or auction phase. An adversary collects no information to identify any bidder. Thus the proposed auction protocol provides anonymous auction to bidders. However, another threat to bidders is possible. An adversary may impersonate another bidder to join the initiation phase. After successful experiment in initiation phase, the adversary then can impersonate the victim bidder to bid in any auction phase. The victim bidder may suffer from this result. Theorem 1 proves that the proposed protocol is secure against the attack of impersonation.

Theorem 1. *Suppose that the auctioneer P faithfully executes the registration protocol in Figure 4, and $E2(\cdot)$ and $D2(\cdot)$ are secure encryption/decryption function. If an adversary is able to impersonate bidder U_i with non-negligible probability, then CDH problem is also solved with non-negligible probability.*

Proof. Suppose g generate $G \subset Z_p^*$. We choose two random elements X_i and Y from the multiplicative group G. Given X_i and Y, our goal is to solve the GDH problem, that means we can find out $Z = g^{x_i y} \in G$. Suppose the bidder U_i's public key be X_i, the auctioneer P's public key be Y. Publish public keys of U_i and P, and the parameters of multiplicative group G, that are X_i, Y, g, q and p. Let the $Ans_{DDH}(\cdot)$ be DDH oracle. □

The auctioneer P definitely doesn't know the discrete logarithm value of public key Y, however, via the reply of $Ans_{DDH}(\cdot)$, the P still guesses if the initiation information is correct or not, the process is as follows:

1) Receiving C;

2) Decrypting $D2_{sec_p}(C) = (T \| a \| ID_i \| K_i)$;

3) Computing $t = H(T \| a)$;

4) Computing $Z = (K_i)^{1/t} \bmod p$;

5) $Ans_{DDH}(X_i, Y, Z)$.

If $Ans_{DDH}(\cdot)$ says Yes, that means $Z = g^{xy} \bmod p$, the auctioneer P accepts the initiation information. Saying No means the auctioneer P refuses the initiation information. If an adversary is able to impersonate bidder U_i with non-negligible probability, that means the adversary can compute $Z = g^{xy} \bmod p$ with non-negligible probability. The result contradicts to the GDH assumption, thus completes the proof, by this disproof, the security of the protocol is equal to GDH problem.

5 Conclusions

Our protocol can effectively achieve anonymous targets, since no information useful to identify bidder is exposed in either initiation or auction phases. Impersonation attack could be another threat to any anonymous auction protocol. Based on the GDH assumption, Theorem 1 in Section 4.2 proves that the proposed auction protocol can withstand the impersonation attack. Regarding efficiency we use lighter algorithm to reduce the communication and computation costs: 30% and 50% of C-C protocol, respectively. As a result, our protocol is applicable in real situations.

References

[1] *Advanced Encryption Standard*, Federal Information Processing Standard 197 (FIPS 197), 2001.

[2] M. Bellare and P. Rogaway, "Optimal asymmetric encryption - how to encrypt with RSA," *Advances in Cryptology Eurocrypt' 94*, LNCS 950, pp. 92-111, Springer-Verlag, 1996.

[3] C. C. Chang and Y. F. Chang, "Efficient anonymous auction protocols with freewheeling bids," *Computers & Security*, vol. 22, pp. 728-734, 2003.

[4] C. C. Chang and Y. F. Chang, "Enhanced anonymous auction protocols with freewheeling bids," *Proceedings of IEEE Advanced Information Networking and Applications*, vol. 1, pp. 353-358, 2006.

[5] X. Deng, C. H. Lee, and H. Zhu, "Deniable authentication protocols," *IEEE Proceedings Computers & Digital Techniques*, vol. 148, pp. 101-104, 2004.

[6] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644-654, 1976.

[7] W. B. Lee, C. C. Wu, and W. J. Tsaur, "A novel deniable authentication protocol using generalized ElGamal signature scheme," *Information Science*, vol. 177, pp. 1376-1381, 2007.

[8] T. Okamoto and D. Pointcheval, "The Gap-Problems: A new class of problems for the security of cryptographic schemes," Proceedings of the 4th International Workshop on Practice and Theory in Public Key Cryptography: Public Key Cryptography, LNCS 1992, pp. 104-118, Springer-Verlag, 2001.

[9] T. Okamoto and D. Pointcheval, "REACT: Rapid enhanced security asymmetric cryptosystem transform," *Proceedings of CT-RSA 2001*, LNCS 2020, pp. 159-174, Springer-Verlag, 2001.

[10] V. Shoup, "OAEP reconsidered," *Proceedings of Advances in Cryptology Crypto'01*, LNCS 2139, Springer-Verlag, 239-259, 2001.

[11] V. Shoup, *On Formal Models for Secure Key Exchange*, IBM Research Report RZ 3120 Version 4, 1999.

Fuw-Yi Yang received the BS and MS degree in the Department of Electronic Engineering from National Taiwan University of Science and Technology, Taipei, Taiwan, and the Ph.D. degree in the Department of Applied Mathematics, National Chung Hsing University, Taichung, Taiwan. He is currently an associate professor with the Department of Computer Science and Information Engineering, Chaoyang University of Technology, Taichung, Taiwan. He is a member of the Chinese Cryptology and Information Security Association (CCISA) and Taiwanese Association for Consumer Electronics (TACE). His research interests include computer cryptography, network security, and information security.

Cai-Ming Liao received the M.S. degree in Computer Science and Information Engineering from Chaoyang University of Technology (CYUT), Taichung, Taiwan, in 2009. His current research interests include applied cryptography and data security.