Efficient English Auction Scheme without a Secure Channel

Tzong-Chen Wu[1], Tzuoh-Yi Lin[1], Tzong-Sun Wu[2], and Han-Yu Lin[2]
[1]Department of Information Management, National Taiwan University of Science and Technology, Taiwan
[2]Department of Computer Science and Engineering, National Taiwan Ocean University, Taiwan

Abstract: *English auctions become tremendously popular on the Internet today. This paper presents a new English auction scheme that can be realized in the public network environments without any additional secure channel. Our scheme not only satisfies security requirements of anonymity, traceability, no framing, fairness, public verifiability, unlinkability among different rounds of auction and linkability in an auction round, but also provides one-time registration and easy revocation. Furthermore, as compared with the pervious works, the proposed scheme has a better performance in terms of the computation and the size of bidding information.*

Keywords: *English auction, bilinear pairings, bilinear Diffie-Hellman problem, hash function.*

Received August 6, 2012; accepted April 26, 2013; published online June 26, 2014

1. Introduction

Auctions have become tremendously popular over the Internet and many kinds of them are proposed continually in recent years. One of the most familiar types of auctions is English auction, in which every Bidder (Bi) incrementally raises the prices for the goods and all the bids are made public so that every Bi can easily obtain the current bid. Finally, the Bi who offers the highest price wins the goods. Nowadays, many English auction services are provided on the Internet, such as eBay, Christie's live and Gavel. Nguyen and Traore [18] proposed an English auction scheme using group signature scheme [4]. They utilized the property of group signature that one of the members in the group can sign anonymously on behalf of the group and the group manager can identify the signer later. However, the English auction based on group signature requires a complicated signature generation and verification procedure. Moreover, the revocation of a Bi is also inefficient in their scheme. To obviate this disadvantage of the Nguyen-Traore scheme, Omote and Miyaji [19] proposed an efficient model of English auction by using bulletin board as a public communication channel. Their scheme consists of three kinds of roles: Auction Manager (AM), Registration Manager (RM) and a set of Bi's and meantime achieves the following security and performance requirements of English auction:

- *Security Requirements*:
  1. Anonymity: Nobody can identify the Bi from his bid information.
  2. Traceability: A winner who has placed the Bid cannot deny it after the winner announcement.
  3. No framing: Nobody can impersonate a certain Bi.
  4. Unforgeability: Nobody can forge a bid with a valid signature.
  5. Fairness: All bids placed by the Bi's should be fairly dealt with during the auction.
  6. Public verifiability: Anybody can verify bidding information and confirm the validity of the bidding information.
  7. Unlink ability among different rounds of auction: Nobody can link the same Bi's bids among several auctions.
  8. Linkability in a Round of Auction: Anybody can link which and how many times of bids are placed by the same Bi in an auction.
- *Performance Requirements*:
  1. Efficiency of Bidding: The computation and communication cost in both bidding and verifying a bid are practical.
  2. One-time registration: Any Bi can participate in many rounds of auction anonymously with a one-time registration.
  3. Easy revocation: The system can easily revoke a Bi.

After that, many English auction protocols are proposed [5, 6, 7, 14, 15, 16, 17, 21, 23]. However, a secure channel and secret key databases are necessary in those schemes, which results in additional costs. Furthermore, once the secure channel or secret key databases are compromised, their schemes will be insecure.

In this paper, we intend to propose a new English auction scheme based on the bilinear pairings. The pairing was initially considered as a negative property on the design of elliptic curve cryptosystems, because it reduces the discrete logarithm problem on some elliptic curves (especially for super-singular curves) to the discrete logarithm problem in a finite field and such property diminishes the strength of super-singular curves in practice. However, after the subsequently successful designs of the tripartite key agreement protocol proposed by Joux [9] and the identity-based encryption scheme proposed by Boneh and Franklin [2], the pairing now becomes beneficial and favorable for the basis of modern cryptographic protocols or cryptosystems [3, 20, 22].

The proposed scheme can achieve all security and performance requirements of the English auction without any additional secure channel and secret key databases. Moreover, in the proposed scheme, the computation of bidding information is faster than previous works [6, 7, 14, 19] and the size of bidding information is only half of that produced by them. Hence, the proposed scheme is more applicable to be realized in the online auction environment.

The organization of this paper is as follows. In next section, we proposed an online English auction scheme. In section 3, we will make some security and performance analyses of the proposed scheme. Finally, the conclusions are given in section 4.

2. Proposed Scheme

Our English auction scheme consists of three kinds of roles: *AM*, *RM* and a set of Bi's. We assume that there are no secure channels among the participants. That is, all communication can be done in the public channels. The services provided by *RM* are:

1. System Initialization.
2. Bi's Registration.
3. Round Key Generation in each Round of Auction.
4. Winner Announcement.
5. Maintain a Public Bulletin Board (*RM_BB*) and a database (*RM_DB*).

AM is responsible for: Start a new auction; auction key generation in each round of auction; winner announcement and maintain a public bulletin board (*AM_BB*), a Bidding board (*BID_BB*), and a database (*AM_DB*).

It should be noticed that if *AM* and *RM* collude with each other, they can identify any Bi during the auctions. We assume that *AM* and *RM* work independently without conspiracy in this paper. In the following, we first summarize defined functions to facilitate the description of the proposed scheme.

- *Round Key* (Y_i, $x_{RM, j}$; $RK_{i,j}$): It is a round key generation function. On input a temporary secret key $x_{RM,j}$ of *RM* in the j^{th} auction and a Bi's public key Y_i, output the Bi's round key $RK_{i,j}$ in the j^{th} auction as:

$$RK_{i,j} = k_{RM,i,j} Y_i \tag{1}$$

Where, the session key $k_{RM,i,j}$ between *Bi* and *RM* is computed as:

$$k_{RM,i,j} = H_2(x_{RM,j} Y_i) \tag{2}$$

- *Auction Key* ($RK_{i,j}$, $x_{AM,j}$; $AK_{i,j}$): It is an auction key generation function. On input a temporary secret key $x_{AM,j}$ of *AM* in the j^{th} auction and Bi's round key $RK_{i,j}$ output an auction key as:

$$AK_{i,j} = k_{AM,i,j} RK_{i,j} \tag{3}$$

Where, the session key $k_{AM,i,j}$ between Bi and *AM* is computed as:

$$k_{AM,i,j} = H_2(x_{AM,j} RK_{i,j}) \tag{4}$$

- *Witness* (AID_j, $price_{i,j}$, $k_{RM,i,j}$, $k_{AM,i,j}$,x_i; $BW_{i,j}$): It is a bid witness generation function. On input an auction identity AID_j, the Bidding price $price_{i,j}$, two session keys $k_{RM,i,j}$ and $k_{AM,i,j}$ and a Bi's private key x_i, output the witness of $price_{i,j}$ for *Bi* in the j^{th} auction as:

$$BW_{i,j} = (k_{RM,i,j} k_{AM,i,j} x_i) H_1(AID_j \,||\, price_{i,j}) \tag{5}$$

- *BidVerify* ($BID_{i,j}$, $AK_{i,j}$, *Boolean*): It is a bid verification function. On input the Bidding information $BID_{i,j}$ and an auction key $AK_{i,j}$, output *True* if :

$$e(BW_{i,j}, Q) = e(z, AK_{i,j}) \tag{6}$$

Where,

$$z = H_1(AID_j \,\|\, price_{I,j}) \tag{7}$$

The proposed scheme consists of six stages: System initialization, key generation, Bi registration, auction setup, bidding and winner announcement. We illustrate the bidding procedure in Figure 1 and detail each stage as follows:

- *System Initialization Stage*: The system selects two groups (G_1, +) and (G_2, ×) of the same prime order q. Let Q be a generator of order q over G_1, e: $G_1 \times G_1 \rightarrow G_2$ be a bilinear pairing and H_1: $\{0, 1\}^* \rightarrow G_1$ and H_2: $G_1 \rightarrow Z_q^*$ be collision resistant hash functions [13].
  The system then publishes system parameters $\{G_1, G_2, q, e, Q, H_1, H_2\}$.
- *Key Generation Stage*: The Bi chooses a private key $x_i \in Z_q$ and computes the corresponding public key $Y_i = x_i Q$.
- *Bi Registration Stage*: The Bi runs the following protocol interactively with *RM* to earn a legal auction membership:

1. Bi computes the authenticator S_i as:

$$S_i = x_i H_1(ID_i) \tag{8}$$

Where, ID_i is Bi's identity. After that Bi sends $\{ID_i, S_i\}$ to *RM*.

2. RM checks whether:

$$e(Y_i, H_1(ID_i)) = e(S_i, Q) \tag{9}$$

If it holds, RM declares that Bi is a legal Bi. Otherwise, RM rejects the registration of Bi.

3. RM publishes $\{ID_i, Y_i\}$ on the RM_BB.

- *Auction Setup Stage*: Let $G_j = \{B_1, B_2, ..., B_n\}$ be the subset of Bi's invited to join the j^{th} auction associated with the identity AID_j. First of all, RM generates the round keys $RK_{i,j}$'s as follows:

1. Randomly determine a temporary key pair ($x_{RM,j}$, $Y_{RM,j}$), where $x_{RM,j} \in Z_q$ and.

$$Y_{RM,j} = x_{RM,j}Q \tag{10}$$

2. Compute the set of round keys, denoted by $RKSET_j=\{RK_{1,j}, RK_{2,j}, \dots, RK_{n,j}\}$, where $RK_{i,j}=$ RoundKey(Y_i, $x_{RM,j}$).
3. Compute an index key $s_{i,j}$ for each $RK_{i,j} \in RKSET_j$, where:

$$s_{i,j} = x_{RM,j}RK_{i,j} \tag{11}$$

4. Store all ($s_{i,j}$, Y_i)'s to RM_DB and shuffle the order of round keys in $RKSET_j$, then publish $RKSET_j$ on RM_BB.

After the round keys generation, AM randomly selects a temporary key pair ($x_{AM,j}$, $Y_{AM,j}$), where $x_{AM,j} \in Z_q$ and.

$$Y_{AM,j} = x_{AM,j}Q \tag{12}$$

Next, AM obtains $RKSET_j$ from RM_BB and computes the set of auction keys, denoted by $AKSET_j=\{AK_{1,j}, AK_{2,j}, \dots, AK_{n,j}\}$, where $AK_{i,j}=$AuctionKey($RK_{i,j}$, $x_{AM,j}$). Afterward, AM computes an index key $d_{i,j}$ for each $AK_{i,j} \in AKSET_j$, where.

$$d_{i,j} = x_{AM,j}AK_{i,j} \tag{13}$$

Finally, AM stores all ($d_{i,j}$, $RK_{i,j}$)'s to AM_DB, shuffles the order of auction keys in $AKSET_j$ and publishes $AKSET_j$ on AM_BB.

- *Bidding Stage*: To join the j^{th} auction, a Bi first obtains the session keys ($k_{RM,i,j}$, $k_{AM,i,j}$) by computing:

$$k_{RM,i,j} = H_2(x_iY_{RM,j}) \tag{14}$$

$$k_{AM,i,j} = H_2((k_{RM,i,j}x_i)Y_{AM,j}) \tag{15}$$

Then, Bi computes the round key and auction key pair ($RK_{i,j}$, $AK_{i,j}$) as:

$$RK_{i,j} = k_{RM,i,j}Y_i, \tag{16}$$

$$AK_{i,j} = k_{AM,i,j}RK_i, \tag{17}$$

Afterwards, Bi searches $AK_{i,j}$ from AM_BB. If $AK_{i,j}$ exists, Bi is a qualified Bi and he can get an index value of $AK_{i,j}$, denoted by $ind_{i,j}$. Otherwise, she/he has been excluded from the auction. If Bi is a qualified Bi, she/he can determine the bidding price $price_{i,j}$ and sends his Bidding information $BID_{i,j}$ = (AID_j, $price_{i,j}$, $BW_{i,j}$) along with $ind_{i,j}$ to BID_BB, where $BW_{i,j}$ is the witness of $price_{i,j}$ for Bi in the j^{th} auction and $BW_{i,j}$ = Witness (AID_j, $price_{i,j}$, $k_{RM,i,j}$, $k_{AM,i,j}$, x_i). It is should be noticed that everyone can verify the validity of $BID_{i,j}$ by checking Bid Verify ($BID_{i,j}$, $AK_{i,j}$). If it returns *True*, $BID_{i,j}$ is a valid bid.

- *Winner Announcement Stage*: Suppose that $BID_{i,j}$ is the authentic highest bid at the end of auction. AM and RM runs the following protocol to announce the auction winner:

1. AM first obtains $AK_{i,j}$ from AM_BB by using $ind_{i,j}$ and then searches $RK_{i,j}$ from AM_DB by using index key $d_{i,j}$, where:

$$d_{i,j} = x_{AM,j}AK_{i,j} \tag{18}$$

2. AM Computes:

$$k_{AM,i,j} = H_2(x_{AM,j}RK_{i,j}) \tag{19}$$

Sends $\{AK_{i,j}, k_{AM,i,j}\}$ to RM and announces $\{AK_{i,j}, k_{AM,i,j}\}$ on BID_BB.

3. RM Computes the Index Key:

$$s_{i,j} = x_{RM,j}RK_{i,j} \tag{20}$$

and searches Y_i from RM_DB by using index key $s_{i,j}$, where:

$$RK_{i,j} = k^{-1}_{AM,i,j}AK_{i,j} \tag{21}$$

If it is found, RM proceeds to next step. Otherwise, RM terminates the winner announcement.

4. RM Computes:

$$k_{RM,i,j} = H_2(x_{RM,j}Y_i) \tag{22}$$

and publishes $\{RK_{i,j}, k_{RM,i,j}\}$ on BID_BB. After the winner announcement, anyone can check whether $RK_{i,j} = k^{-1}_{AM,i,j}AK_{i,j}$. If the equality holds, the winner's public key can be computed as $Y_i = k^{-1}_{RM,i,j}RK_{i,j}$. After that, the winner's identity can be obtained by searching Y_i from RM_BB.

In the following, we show that the proposed scheme works correctly.

If S_i is a valid authenticator of Bi, it will satisfy Equation 9 from the left-hand side of Equation 9, we have:

$$\begin{aligned} e(Y_i, H_1(ID_i)) &= e(x_iQ, H_1(ID_i)) \\ &= e(Q, x_iH_1(ID_i)) \\ &= e(Q, S_i) \quad \text{(by Equation 8)} \\ &= e(S_i, Q) \end{aligned}$$

Which leads to the right-hand side of Equation 9.

If $BID_{i,j}$ is a valid bid generated by Bi, bid verify ($BID_{i,j}$, $AK_{i,j}$) will return *True*. From the left-hand side of Equation 6, we have:

$$\begin{aligned} e(BW_{i,j}, Q) &= e((k_{RM,i,j}k_{AM,i,j}x_i)H_1(AID_j \parallel price_{i,j}), Q) \quad \text{(by Equation 15)} \\ &= e(H_1(AID_j \parallel price_{i,j}), (k_{RM,i,j}k_{AM,i,j}x_i)Q) \\ &= e(H_1(AID_j \parallel price_{i,j}), (k_{RM,i,j}k_{AM,i,j})Y_i) \quad \text{(by Equation 16)} \\ &= e(H_1(AID_j \parallel price_{i,j}),(k_{AM,i,j}RK_{i,j})) \\ &= e(H_1(AID_j \parallel price_{i,j}), AK_{i,j}) \quad \text{(by Equation 17)} \\ &= e(z, AK_{i,j}) \end{aligned}$$

Which leads to the right-hand side of Equation 6.

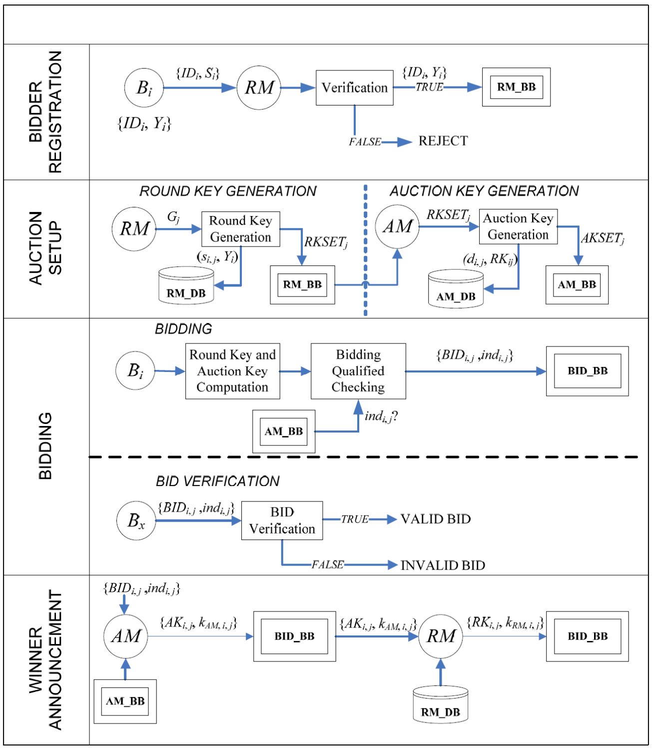

Figure 1. Illustration of the budding procedure.

3. Security and Performance

In this section, we will show that the proposed scheme is secure against malicious adversaries and has a better performance than previous works.

3.1. Security Analysis

The security of the proposed scheme is based on the Elliptic Curve Discrete Logarithm Problem (ECDLP), Bilinear Pairing Inversion Problem (BPIP) [22] and the One-Way Hash Function (OWHF) assumptions:

- *ECDLP*: Let E be an elliptic curve over $GF(p)$, $P \in E$ a base point of order q and Y a point in E, where p is a large prime. Given Y, it is computationally infeasible to determine the integer x, $0 \le x \le q-1$, such that $Y=xP$.
- *OWHF*: A secure OWHF h operates on an arbitrary length input x and outputs a fixed length $y=h(x)$ such that: Given x, it is easy to compute $y=h(x)$, Given y, it is computationally infeasible to derive x satisfying that $y=h(x)$ and It is computationally infeasible to find two distinct integers x and x' fulfilling that $h(x)=h(x')$.
- *BPIP* [24]: Let G_1 be a subgroup of points on an elliptic curve over a finite field and G_2 a subgroup of the multiplicative group of a related finite field. Given $Q \in G_1$ and $e(P, Q) \in G_2$ it is computationally infeasible to determine $P \in G_1$.

We demonstrate that the proposed scheme achieves all security requirements of online English auction scheme as follows:

- *Anonymity*: The adversary can identify the Bi if he is capable of deriving *Bi's* public key from the bidding information. One possible way is first to compute $RK_{i,j} = k_{AM,i,j}^{-1} AK_{i,j}$ and then obtain Bi's public key as $Y_i = k_{RM,i,j}^{-1} RK_{i,j}$. However, in our scheme, if Bi is not the final winner, *AM* and *RM* will not publish the values of $k_{AM,i,j}$ and $k_{RM,i,j}$ in the end of the auction. Thus, the adversary cannot reveal the identity of Bi successfully.
- *Traceability*: In the winner announcement stage, *AM* and *RM* publish $\{AK_{i,j}, k_{AM,i,j}\}$ and $\{RK_{i,j}, k_{RM,i,j}\}$, respectively. With $\{AK_{i,j}, k_{AM,i,j}, RK_{i,j}, k_{RM,i,j}\}$, everyone can derive the winner's public key as $Y_i = k_{RM,i,j}^{-1} k_{AM,i,j}^{-1} AK_{i,j}$ and then check its validity from *RM_BB*.
- *No Framing and Unforgeability*: If the adversary has the ability to generate a valid $BW_{i,j}^*$ for a new price $price_{i,j}^*$, he can impersonate or frame Bi during the auction. In order to generate a valid $BW_{i,j}^*$, the adversary has two approaches. One is that he collects the value of $\{k_{RM,i,j}, k_{AM,i,j}, x_i\}$ and then computes $BW_{i,j}^* = (k_{RM,i,j} k_{AM,i,j} x_i) H_1(AID_j \| price_{i,j}^*)$.
  However, he will face the intractability of ECDLP to derive x_i from Y_i, $k_{AM,i,j}$ from Equation 3 and $k_{RM,i,j}$ from Equation 16. The other is that the adversary attempts to find a $BW_{i,j}^*$ satisfying that $e(BW_{i,j}^*, Q) = e(\alpha, AK_{i,j})$ where $\alpha = H_1(AID_j \| price_{i,j}^*)$.
  Unfortunately, he will encounter the difficulty of BPIP and fail to make it.
- *Fairness*: Since, all bidding information is posted on *BID_BB* by the Bi himself, all bids can be dealt with in a fair way.
- *Public Verifiability*: Seeing that all information of Bidding and the winner announcement is posted on *BID_BB*, everyone can verify the correctness of winner announcement and the validity of bids with the bid verify function.
- *Unlinkability among Different Auctions*: In different auctions, *AM* and *RM* also chooses different temporary secret keys to generate round keys and auction keys, respectively. Therefore, nobody can link the same Bi's Bids among different auctions.
- *Linkability in an Auction*: For that the Bi uses the same auction key to place bids in an auction, everyone knows which bids are placed by the same Bi and how many times of bids are placed by the same Bi in an auction.

3.2. Performance Evaluation

In this subsection, we show that the proposed scheme achieves performance requirements of the online English auction scheme.

- One-time Registration**:** because our scheme fulfills the security requirements of anonymity and unlinkability among different auctions, all Bi's can participate in plural rounds of auction anonymously with one-time registration, even though the winner's identity will be published in the end of bidding.

- Easy Revocation: when *RM* wants to revoke a Bi, he can simply delete the Bi's public key and round key from *RM_BB*.
- Efficiency of Bidding: in a live English auction, the computation and the communicational costs for placing a bid are the most important issues. The Bi's repeatedly make bids against competing Bi's on the Internet in real time if someone has out bid him. Consequently, the efficiency evaluation will primarily focus on the comparisons of computation and communication costs. We first define some used notations. Let T_E be the time for computing modular exponentiation, T_M be the time for computing modular multiplication, T_{ECM} be the time for computing point multiplication in an elliptic curve and T_B be the time for computing the bilinear pairing. It should be noted that T_{ECM} can be expected to be about 8 times faster than T_E [10, 12], and the computation of T_B is getting more efficient nowadays [1, 8, 11]. We compare the proposed scheme with some previous works including the Omote and Miyaji (OM for short) [19], Lee *et al.* (LKM for short) [14], Chen's *et al.* (Ch for short) and (CHL for short) schemes [6, 7]. Detailed comparisons in terms of the computation and the communicational costs are listed in Table 1. The comparison of functionalities is made in Table 2. From these comparisons, we conclude that our scheme provides better efficiency and functionalities.

Table 1. Comparison of efficiency.

Schemes Item		OM	LKM	Ch	CHL	Ours
Computation Cost in Bidding Stage	Bidding	$2T_E$	$3T_E$	$3T_{ECM} + 6T_M$	$3T_E + 6T_M$	T_{ECM}
	Verification	$2T_E$	$2T_E$	$2T_{ECM}$	$2T_E + T_M$	$2T_B$
Communication Cost *1	Placing a Bid	520 Bits	520 Bits	520 Bits	2248 Bits	221 Bits *2

*1: Suppose that the sizes of p, q, $ind_{i,j}$, and $price_{i,j}$ are 1024, 160, 20 and 40 Bits, respectively. Also, a collision-resistant cryptographic hash function, e.g., SHA-1 is adopted.
*2: Use point compression technique [9].

Table 2. Comparison of functionalities.

Functionalities / Schemes	OM	LKM	Ch	CHL	Ours
All Requirements of English Auction	×	√	√	√	√
Without non-Repudiation Protocols	×	√	√	√	√
Without Secure Channels	√	×	×	×	√
Without Secure Databases	√	×	×	×	√

4. Conclusions

In this paper, we have proposed an efficient English auction scheme achieving all the performance requirements of English auction without additional secure channel. Moreover, as compared with previous works, the proposed scheme has better efficiency and functionalities. Hence, the proposed scheme is suitable for realization in online bidding environments. In the future research, we will try to combine our scheme with key-insulated system to mitigate the impact of key compromise and further provide provable security.

Acknowledgement

We would like to thank anonymous referees for their valuable suggestions. This work was supported in part by the National Taiwan Ocean University under the contract number 102B29001N.

References

[1] Barreto P., Kim Y., Lynn B., and Scott M., "Efficient Algorithms for Pairing-based Cryptosystems," *in Proceedings of the 22nd Annual International Cryptology Conference on Advances in Cryptology*, Berlin, London, pp. 354-368, 2002.

[2] Boneh D. and Franklin M., "Identity-Based Encryption from the Weil Pairing," *Appears in SIAM Journal of Computing*, vol. 32, no. 3, pp. 213-229, 2001.

[3] Boneh D., Lynn B., and Shacham H., "Short Signatures from the Weil Pairing," available at: https://www.iacr.org/archive/asiacrypt2001/22480516.pdf, last visited 2001.

[4] Camenisch J. and Stadler M., "Efficient Group Signature Schemes for Large Groups," *in Proceedings of the 17th Annual International Cryptology Conference on Advances in Cryptology*, Berlin, UK, pp. 410-424, 1997.

[5] Chang C., Cheng, F., and Chen Y., "A Novel Electronic English Auction System with a Secure On-shelf Mechanism," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 4, pp. 657-668, 2013.

[6] Chen S., "An English Auction Scheme in the Online Transaction Environment," *Computers and Security*, vol. 23, no. 5, pp. 389-399, 2004.

[7] Chung F., Huang H., Lee H., Lai F., and Chen S., "Bidder-anonymous English Auction Scheme with Privacy and Public Verifiability," *The Journal of Systems and Software*, vol. 81, no. 1, pp. 113-119, 2008.

[8] Galbraith D., Harsison K., and Soldera D., "Implementating the Tate Pairing," available at: http://www.hpl.hp.com/techreports/2002/HPL-2002-23.pdf, last visited 2002.

[9] Joux A., "A One-Round Protocol for Tripartite Diffie-Hellman," *in Proceedings of the 4th International Algorithmic Number Theory Symposium*, London, UK, pp. 385-394, 2000.

[10] Jurisic A. and Menezes J., "Elliptic Curves and Cryptography," *Dr. Dobb's Journal*, pp. 26-32,

1997.

[11] Kobayashi T., Kobayashi T., Aoki K., and Imai H., "Efficient Algorithms for Tate Pairing," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E89-A, no. 1, pp. 134-143, 2006.

[12] Koblitz N., Menezes J., and Vanstone S., "The State of Elliptic Curve Cryptography," *Design, Codes and Cryptography*, vol. 19, no. 2-3, pp. 173-193, 2000.

[13] Lakshmanan T. and Muthusamy M., "A Novel Secure Hash Algorithm for Public Key Digital Signature Schemes," *the International Arab Journal of Information Technology*, vol. 9, no. 3, pp. 262-267, 2012.

[14] Lee B., Kim K., and Ma J., "Efficient Public Auction with One-time Registration and Public Verifiability," *in Proceedings of the 2nd International Conference on Cryptology in India Chennai*, India, pp. 162-174, 2001.

[15] Lee C., Ho F., and Hwang S., "A Secure E-Auction Scheme Based on Group Signatures," *Information Systems Frontiers*, vol. 11, no. 3, pp. 335-343, 2009.

[16] Lee C., Hwang S., and Lin W., "A New English Auction Scheme using the Bulletin Board System," *Information Management and Computer Security*, vol. 17, no. 5, pp. 408-417, 2009.

[17] Li J., Juan J., and Tsai J., "Practical Electronic Auction Scheme with Strong Anonymity and Bidding Privacy," *Information Sciences*, vol. 181, no. 12, pp. 2576-2586, 2011.

[18] Nguyen K. and Traore J., "An Online Public Auction Protocol Protecting Bidder Privacy," *in Proceedings of the 5th Australasian Conference on Information Security and Privacy*, London, UK, pp. 427-442, 2000.

[19] Omote K. and Miyaji A., "A Practical English Auction with One-time Registration," *in Proceedings of the 6th Australasian Conference on Information Security and Privacy*, London, UK, pp. 221-234. 2001.

[20] Peterson G., "ID-Based Signature from Pairings on Elliptic Curves," *Electronics Letters*, vol. 38, no. 18, pp. 1025-1026, 2002.

[21] Shiha H., Yenb C., Cheng H., and Shih H., "A Secure Multi-Item E-Auction Mechanism with Bid Privacy," Computers and Security, vol. 30, no. 4, pp. 273-287, 2011.

[22] Smart P., "An Identity Based Authenticated Key Agreement Protocol Based on the Weil Pairing," *Electronic Letters*, vol. 38, no. 13, pp. 630-532, 2002.

[23] Sun H. and Feng Q., "Model and Optimal Bidding Strategies in Multi-attribute English Auction," *in Proceedings of International Conference on Information Technology, Computer Engineering and Management Sciences*, Nanjing, Jiangsu, pp. 11-15. 2011.

[24] YacoBi Y., "A Note on the Bi-Linear Diffie-Hellman Assumption," available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.19.1959 & rep=rep1 & type=pdf, last visited 2002.

Tzong-Chen Wu received BS degree in information engineering from National Taiwan University in 1983, MS degree in applied mathematics from National Chung Hsing University in 1989 and PhD degree in computer science and information engineering from National Chiao Tung University in 1992. He joined the Department of Information Management, National Taiwan University of Science and Technology (NTUST) in 1992. Since, February 1997 till now, he has been the professor in the Department of Information Management, NTUST. Professor Wu is the member of IEEE, ACM and the Chinese Cryptology and Information Security Association. His current research interests include data security, cryptography, network security, and data engineering.

Tzuoh-Yi Lin received his BS, MS, and PhD degrees in information management from National Taiwan University of Science and Technology in 1995, 1997 and 2008, respectively. He is now the General Manager of Li-Ming Machinery Industrial Co. Ltd. His current research interests include coffee logy, network security, cryptography and data engineering.

Tzong-Sun Wu received his BS degree in electrical engineering from National Taiwan University in 1990 and his PhD degree in information management from National Taiwan University of Science and Technology in 1998. From 1998 to 2001, he has been an Assistant Professor in Department of Information Management, Huafan University. From 2001 to 2007, he has been an Associate Professor in Department of Informatics, Fo Guang University. He is currently with Department of Computer Science and Engineering, National Taiwan Ocean University, Keelung, Taiwan. His research interests include information security, watermarking, digital right management, and e-commerce.

Han-Yu Lin received his BA degree in economics from Fu-Jen Catholic University of Taiwan in 2001, his MS degree in information management from Huafan University of Taiwan in 2003 and his PhD degree in computer science and engineering from National Chiao Tung University of Taiwan in 2010. He was an engineer in CyberTrust Technology Institute, Institute for Information Industry, Taiwan from 2012 to 2012. Since, 2012, he has been an Assistant Professor in the Department of Computer Science and Engineering, National Taiwan Ocean University, Taiwan. His research interests include cryptology, network security, digital forensics, RFID privacy and application, cloud computing security and e-commerce security.