Expert Systems with Applications 38 (2011) 9900–9907

Contents lists available at ScienceDirect

Expert Systems with Applications

journal homepage: www.elsevier.com/locate/eswa

An agent-based English auction protocol using Elliptic Curve Cryptosystem for mobile commerce

Yu-Fang Chung [a,*], Yu -Ting Chen [b], Tzer-Long Chen [c], Tzer-Shyong Chen [d]

[a] Department of Electrical Engineering, Tunghai University, Taiwan
[b] Department of Computer Science, Chiao Tung University, Taiwan
[c] Department of Information Management, Taiwan University, Taiwan
[d] Department of Information Management, Tunghai University, Taiwan

ARTICLE INFO

Keywords:
Mobile agent
Elliptic Curve Cryptosystem
English auction
Anonymity
Public verification

ABSTRACT

Rapid development of the Internet and the extensive use of mobile phones have increased demand for mobile devices in Internet auctions. This trend is acting as an incentive to develop an auction model for mobile-based environment. Recently, Kuo-Hsuan Huang proposed a mobile auction agent model (MoAAM), which allows the bidders to participate in online auctions through a mobile agent. He used modular exponentiation operations in his method. As a result, the processing time for key generation, bidding, and verification were long. Thus, we propose to add the concept of Elliptic Curve Cryptosystem (ECC) onto MoAAM, because ECC has low computation amount and small key size, both of which will aid to increase the speed in generating keys, bidding, and verification. In terms of reduction of computation load on mobile devices and auction-manager server, the proposed method will make online auction system more efficient as well as more convenient to use. This paper mainly uses the English auction protocol as the key auction protocol. The protocol consists of four entities: Registration Manager (RM), Agent House (AH), Auction House (AUH), and Bidders (B). The Registration Manager registers and verifies Bidder identity. The Agent House manages the agents and assigns public transaction keys to Bidders. The Auction House provides a place for auction and maintains all necessary operations for a smooth online auction. Bidders are buyers who are interested in purchasing items at the auction. Our proposed method conforms to the requirements of an online auction protocol in terms of anonymity, traceability, no framing, unforgetability, non-repudiation, fairness, public verifiability, unlinkability among various auction rounds, linkability within a single auction round, efficiency of bidding, one-time registration, and easy revocation.

1. Introduction

Technical advancement of the Internet in recent years has managed to successfully replace offline auction with online auction, which is more far reaching, more convenient, more powerful, and more capable than the conventional way of holding an auction sale. Today, online auction protocols are applied in auctions that are held over the Internet. These auctions include open auction and sealed-bid auction. Open auction can be subdivided into two types: English auction and Dutch auction (Huang, 2003). In an English auction, all bidders place their bids on the basis of the reserve price that is preliminarily set by a host. When everything is in place, the host starts the bidding process. As bidding progresses, the bid prices go increasingly higher. When the auction time ends, the person with the highest bid wins. In a Dutch auction, bidders place their bids for lower prices. The auction closes when there is a bidder who is willing to pay the final price (Lee, Chen, & Hung, 2000). The bidding process in English auction is more transparent, bidders can observe the bids made by their competitors during the entire auction process and make immediate adjustments to his/her bid. Therefore, bidding is generally highly competitive under this kind of protocol, as the protocol would force the bid price to increase if the goods are desirable. Thus, we can say that the English auction protocol is more efficient as a good protocol helps auction goods get a higher price (Peng, Chang, & Chen, 2008). As a result, the expected return on the goods auctioned off using English auction protocol is generally higher than that of other protocols. So, most auction-based websites, such as eBay and Yahoo! Auctions, operate on English auction. Therefore, this paper will primarily focus on how to apply the English auction protocol in mobile commerce.

Omote and Miyaji (2001) proposed to use the bulletin board for verification in English auction protocol, declaring that it can satisfy

* Corresponding author. Tel.: +886 4 23590121.
E-mail address: yfchung@thu.edu.tw (Y.-F. Chung).

0957-4174/$ - see front matter © 2011 Elsevier Ltd. All rights reserved.
doi:10.1016/j.eswa.2011.02.039

the security requirements of English auction. Their method was based on a concept proposed by Wu, Chen, and Lin (2002) and Nguyen and Traore (2000), who utilized group signatures in English auction protocol to raise the security level for the bidders. However, for security reason, Omote and Miyaji's method does not publish any bidder information, because they understood it could cause a security breach to privacy. Above all, it would violate the purposes of anonymity, fairness, and unlinkability among various auction rounds, and other characteristics that are required in an English auction protocol. Later, Lee, Kim, and Ma (2001) made improvements on Omote and Miyaji's method. It allowed bidder's identities and information to be published, and at the same time, the relation among various rounds of auction for the same bidder was reinforced. Thus, the bidders need not worry about breach of privacy when their identity information is posted on the bulletin board. In 2003, Chang and Chang (2003) proposed a much simpler and more effective method for providing anonymity in English auction. However, Jiang, Pan, and Li (2005) pointed out that Chang et al.'s method was not secure enough to protect bidders' privacy because the bidder had no way of knowing whether the auctioneer was the same or not. Subsequently, Chang et al. utilized an alias to resolve the situation (Chang & Chang, 2006).

Rapid developments in mobile phones have caused an increase in the demand for mobile commerce. Recently, Kuo-Hsuan Huang proposed a mobile auction agent model (MoAAM) (Huang, 2008), which allows the bidders to participate in online auctions through mobile agents. Huang's method employs modular exponentiation operations, which unfortunately increases the processing time for key generation, bidding, and verification. Thus, we propose to add the concept of Elliptic Curve Cryptosystem (ECC) onto MoAAM since ECC has low computation amount and small key size. It will aid in speeding up key generations, bidding, and verification. In terms of reduction of computation load on mobile devices and connected servers, the proposed method will make online auction system more convenient for users. In order to maintain a fair and secure auction, certain security features must be included, as follows (Lee et al., 2001):

(1) Anonymity: During the course of an auction, no one shall be able to ascertain the identity of another bidder.
(2) Traceability: The winner's real identity can be disclosed at the end of the auction.
(3) No framing: The identities of all bidders remain independent. No person shall falsely claim to be any other bidder who participated in the auction.
(4) Non-forgeability: No one is able to forge another's bid price.
(5) Non-repudiation: The winning bidder shall not be able to deny his/her bid price after the winner is announced.
(6) Fairness: All bidding must be conducted in an open and fair manner.
(7) Public verifiability: Anyone can verify the identity and bid price of past bidders.
(8) Unlinkability among various auction rounds: No one shall be able to determine the same bidder's identity among different rounds of auction.
(9) Linkability within a single auction round: The bidders can repeatedly place new bid price within a single auction round and can be recognized by other bidders.
(10) Efficient bidding: In order to make the bidding efficient, processing time must be minimized.
(11) One-time registration: The bidder need only register once to participate in any number of auctions.
(12) Easy revocation: Registration Manager can easily revoke someone's right to bid.

The rest of this paper is organized as follows. Section 2 explains how mobile auction agent model actually work in practice and provide further explanation on Elliptic Curve Cryptosystem with examples. Section 3 shows our proposed method, which is about how to apply ECC onto MoAAM. Section 4 contains a security analysis performed to examine our proposed method. Conclusions are finally drawn in Section 5 and recommendations for further studies given.

2. The related research

2.1. Mobile auction agent model (MoAAM)

2.1.1. Communication in MoAAM

MoAAM (Huang, 2008) is designed to enable users to use their mobile devices to participate in online auctions. MoAAM consists of four agents: (1) a personal agent, (2) a customer agent, (3) an auctioneer agent and (4) a broker agent. How these agents work in MoAAM through a web server is shown in Fig. 2.1. Inside the mobile device, there is an interactive interface, called personal agent, which would connect with an agent house via the wireless network. In other words, a personal agent is a preset agent that operates on the mobile device and provides an interface to allow users to communicate with the Agent House server. The customer

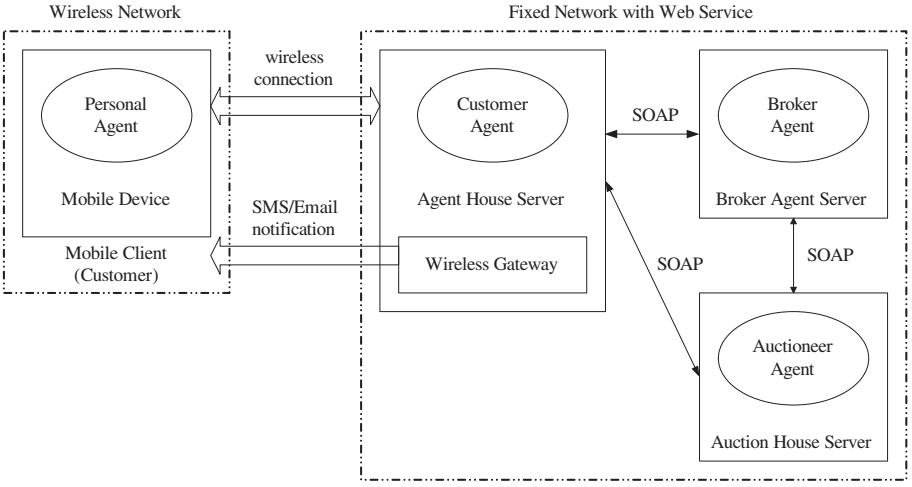

Fig. 2.1. Communication in MoAAM.

agent, auctioneer agent, and broker agent all stores and operates in the fixed network.

The personal agent connects to the customer agent when a mobile network user wants to buy a specific product. Then the personal agent sends the description of the desired products and price information to the customer agent. On the other hand, an auctioneer registers the information of products to broker agent. On receiving the user's request, the broker agent generates an auction list, that meets the user's needs, and send it back to the user. If the user decides to purchase any auction item on the received list, a bid agent will be created by the customer agent and dispatched to an auction house server to join in the bidding.

2.1.2. The structure of MoAAM

The structure of MoAAM (Huang, 2008) is shown in Fig. 2.2:

(1) Primary Participants in MoAAM
   (i) Broker agent: It is responsible for pairing up bidders and auctioneers. Moreover, it generates auction lists and provides bid price information for the users.
   (ii) Bid agent: An individual user would use it to participate in auctions and place the bids.
   (iii) Auctioneer agent: Auctioneers use it as their representative to manage the items they are selling.
   (iv) Auction house server: A platform where online auctions take place.

(2) How Customer Agent Operates
   The customer agent provides an interface with three different functions for the user:
   (i) Query the broker agent: To request broker agent for list of registered auction items and bid prices for the same.
   (ii) Specify the bid agent: A bidder sends his/her request and bidding information to the bid agent generator. The generator will create a bid agent from a template.
   (iii) Control the bid agent: This function allows the bidder to communicate with the bid agent and control the behavior of a bid agent.

(3) How Broker Agent Operates
   First, the auctioneer needs to register his/her agent with the broker agent, and then the broker agent will store the auctioneer's information in the database. When the customer agent sends a request for item information, the broker agent would reply with a list of recommended items to the customer agent.

(4) How Auction House Operates
   The auction house server offers a web interface to allow the auctioneers to execute the following functions:
   (i) Specify the auctioneer agent: An auctioneer sends his/her request and auction information to the auctioneer agent generator. The generator will create an auctioneer agent from a template. The newly created agent and auction information would be registered with the broker agent.
   (ii) Control the auctioneer agent: This interface allows the auctioneer to communicate with the auctioneer agent and control the auctioneer agent's behavior.

(5) Mobile agent platform
   The mobile agent platform is where bid agent and auctioneer agent would be sent to as the auction starts.

2.2. Elliptic Curve Cryptosystem

In 1985, Elliptic Curve Cryptography (ECC) was proposed by Koblitz (1987) and Miller (1986). The ECC was able to improve the

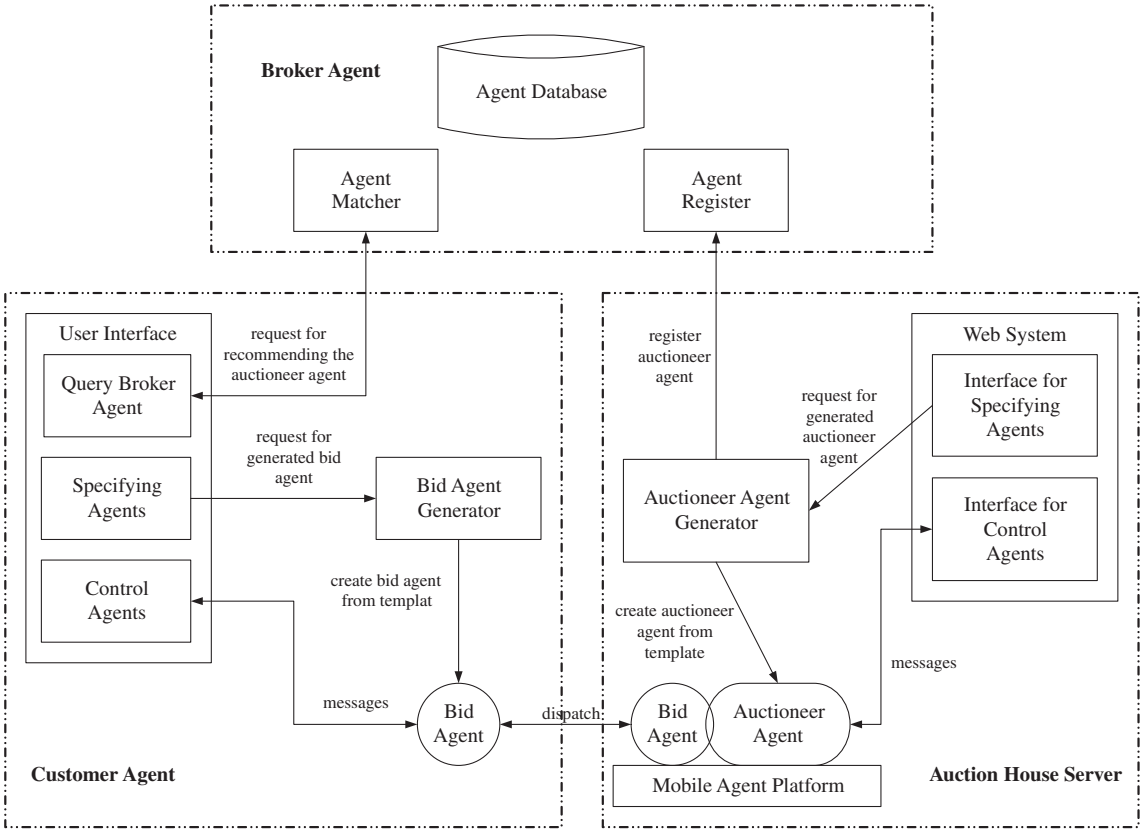

Fig. 2.2. Architecture of MoAAM.

existing cryptogram systems in terms of having smaller system parameter, smaller public-key certificates, lower bandwidth usage, faster implementations, lower power requirement, and smaller hardware processor requirement (Wu, 2005). Therefore, using the Elliptic Curve Cryptography to build a cryptosystem is commendable by the reasons of high security and efficiency (Chung, Lee, Lai, & Chen, 2008). The mathematic settings of Elliptic Curve Cryptosystem are as described below (Chung et al., 2008; Shieh, 2006).

First, elliptic curves can be divided into two families: prime curves and binary curves. Prime curves (Z_p) are good to use in software application, because it does not require extended bit-fiddling operation, which binary curves require. Binary curves ($GF(2^n)$) are best for hardware application as it require a few logic gates to build a powerful cryptosystems. Second, the variable and coefficients of the elliptic curves are limited to the elements of the finite field. Because of this limitation, it would increase the efficiency of ECC computing operation.

In the finite field Z_p, defined modulo a prime p, an elliptic curve is represented as $E_p(a,b)$: $y^2 = x^3 + ax + b(\mathrm{mod}\ p)$, where $(a,b) \in Z_p$ and $4a^3 + 27b^2 \bmod p \neq 0$. The condition, $4a^3 + 27b^2 \bmod p \neq 0$, is necessary to ensure that $y^2 = x^3 + ax + b(\mathrm{mod}\, p)$ has no repeated factors, which means that a finite abelian group can be defined based on the set $E_p(a,b)$ (Huang, Chung, Liu, Lai, & Chen, in press). Included in the definition of an elliptic curve, a point at infinity denoted as O is also called the zero point. The point at infinity O is the third point of intersection of any straight line with the curve, so that there are points including (x,y), $(x,-y)$, and O on the straight line.

For points on an elliptic curve, we define a certain addition, denoted "+". The addition rules are given below.

(1) $O + P = P$ and $P + O = P$, where O serves as the additive identity.
(2) $-O = O$.
(3) $P + (-P) = (-P) + P = O$, where $-P$ is the negative point of P.
(4) $(P + Q) + R = P + (Q + R)$.
(5) $P + Q = Q + P$.

For any two points $P = (x_p, y_p)$ and $Q = (x_q, y_q)$ over $E_p(a,b)$, the elliptic curve addition operation, which is denoted as $P + Q = R = (x_r, y_r)$, satisfies the following rules:

$$\begin{aligned} x_r &= (\lambda^2 - x_p - x_q) \bmod p \\ y_r &= (\lambda(x_p - x_r) - y_p) \bmod p \end{aligned}, \quad \text{where } \lambda = \begin{cases} \left(\frac{y_q - y_p}{x_q - x_p}\right) \bmod p, \text{if } P \neq Q \\ \left(\frac{3x_p^2 + a}{2y_p}\right) \bmod p, \text{if } P = Q \end{cases}$$

Given an equation of the form denoted as $E_{23}(1,4)$: $y^2 = x^3 + 1x + 4 \bmod 23$, $a = 1$, $b = 4 \in Z_p$, and $4a^3 + 27b^2 = 22 \bmod 23 \neq 0$, points over the elliptic curve $E_{23}(1,4)$ are shown in Table 1 (Johnson, Menezes, & Vanstone, 2001).

Example 2.1. Let $P = (7,3)$ and $Q = (8,15)$ in $E_{23}(1,4)$. When $P \neq Q$, we must derive λ before calculating $P + Q$, as follows:

$$\lambda = \left(\frac{15 - 3}{8 - 7}\right) \bmod 23 \equiv 12 \bmod 23 \equiv 12.$$

So, when $\lambda = 12$, x_r and y_r can be derived as shown below:

$$x_r = (12^2 - 7 - 8) \bmod 23 \equiv 129 \bmod 23 \equiv 14,$$
$$y_r = (12(7 - 14) - 3) \bmod 23 \equiv -87 \bmod 23 \equiv 5.$$

Thus, $P + Q = R = (14,5)$.

To calculate $2P$, $P = (7,3)$, we must first derive λ as follows:

$$\lambda = \left(\frac{3 \times 7^2 + 1}{2 \times 3}\right) \bmod 23 \equiv \left(\frac{148}{6}\right) \bmod 23 \equiv 17$$

So, when $\lambda = 17$, x_r and y_r can be derived as shown below:

$$x_r = (17^2 - 7 - 7) \bmod 23 \equiv 257 \bmod 23 \equiv 22$$
$$y_r = (17(7 - 22) - 3) \bmod 23 \equiv -258 \bmod 23 \equiv 18$$

Thus, $P + P = 2P = (22,18)$.

Although we can see point multiplication on the elliptic curve, we do not actually multiply one point with another. In fact, we have to use the equation, $Q = k \times P$, in order to obtain a point on the curve. By assuming k is a natural number and Q and P are points which are on E, Q can be defined as $P + P + \cdots + P$ in k times. The security of ECC in the finite field is based on double-and-add algorithm, $Q = k \times P$. Therefore, it is difficult to compute the result of k, even if the numbers of Q and P are given. This is the conundrum of Elliptic Curve Cryptography and is also known as Elliptic Curve Discrete Logarithm Problem (ECDLP) (Guan & Jen, 2005).

3. Research method

The proposed method includes six phases: (1) Initialization, (2) Registration, (3) Transaction Public Key Generation, (4) Signature, (5) Auction Bidding, and (6) Winner Announcement. The whole process flow is shown in Fig. 3.1. In the process, there are four main participants, which are Registration Manager (RM), Agent House (AH), Auction house (AUH), and Bidder (B).

3.1. The participants

(1) Registration Manager (RM)
  (i) It is a unit for bidders to apply for registration. All bidders need to register only once. After that, they can participate in any number of auctions without needing to register again.
  (ii) It is also responsible for storing the bidders' identity information and corresponding secret parameters.
  (iii) It manages and maintains the bulletin board, which is called BB_{RM}. On the bulletin board, two types of information are to be posted. One is registration key and identity information of a bidder. Another is the pseudonym that a bidder uses in a single auction round. Anyone can avail the posted information for identification verification. However, only the RM has authority to write and update the board.
(2) Agent House (AH)
  (i) It is responsible for communicating with broker agent and creating bid agents.
  (ii) It manages and maintains a bulletin board, which is called BB_{AH}. The bidder's transaction public key is posted on the board for verification purpose. However, only the AH has authority to write and update the board.

Table 1
Points over the elliptic curve $E_{23}(1,4)$.

(0,2)	(0,21)	(1,11)	(1,12)	(4,7)	(4,16)	(7,3)	(7,20)	(8,8)	(8,15)
(9,11)	(9,12)	(10,5)	(10,18)	(11,9)	(11,14)	(13,11)	(13,12)	(14,5)	(14,18)
(15,6)	(15,17)	(17,9)	(17,14)	(18,9)	(18,14)	(22,5)	(22,18)		

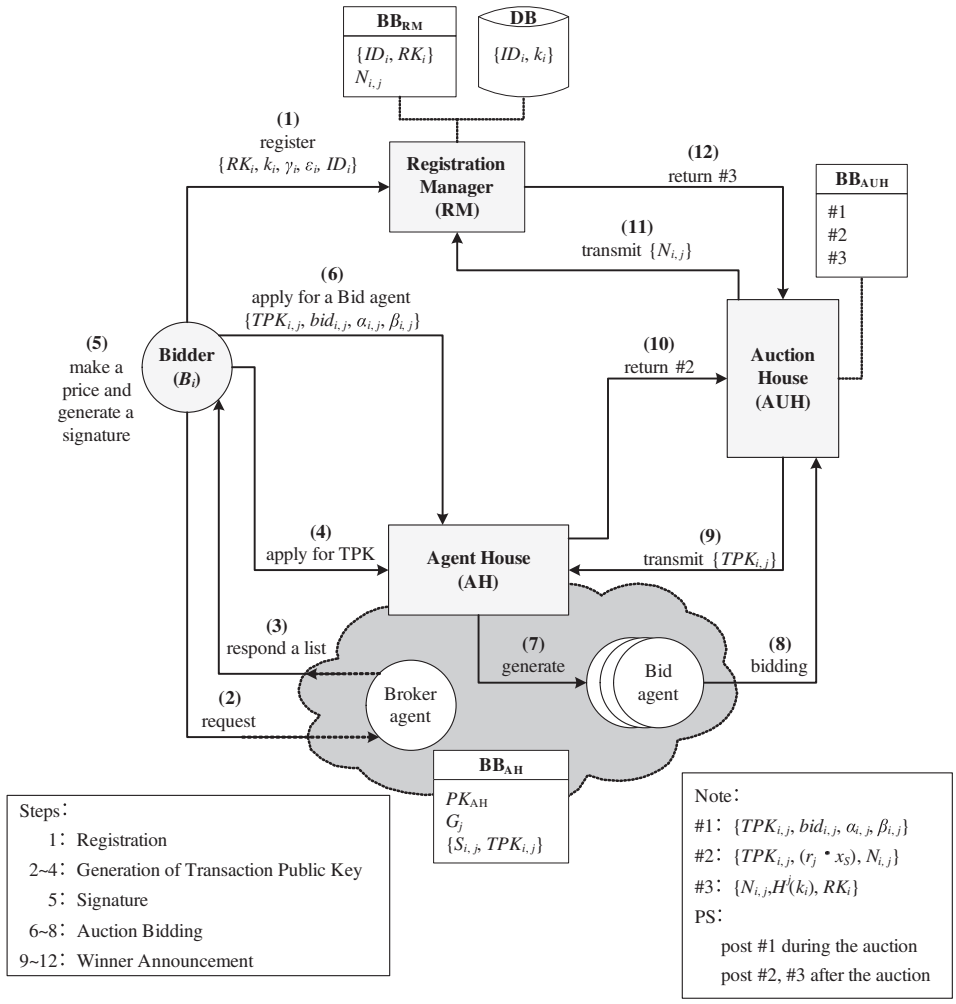

Fig. 3.1. Flow chart of MoAAM.

(3) Auction House (AUH)
   (i) It provides the auction place, maintains the operations, and hosts the auctions.
   (ii) It manages and maintains a bulletin board, which is called BB_{AUH}. The bidding information of bidders and the winning bidder's information will be posted on this bulletin board that. The information posted on the board can be used to verify a bidder's identity. However, only the AUH has authority to write and update the board.
(4) Bidder (B)
   (i) One who participates and place bids in the auction.

3.2. System parameters

The system parameters are shown in Table 2.

Table 2
System parameters.

p	A big prime number
q	A big prime number; q is the order of a generative point on an elliptic curve and its value is within $p+1\pm2\sqrt{p}$;
E	Elliptic curve equation $y^2 = x^3 + ax + b(\mathrm{mod}\, p)$, where a, b are real numbers and satisfy $4a^3 + 27b^2 \mathrm{mod}\, p \neq 0$;
G	A generative point on an elliptic curve with order as q;
F	A point on an elliptic curve;
x_F	The value of the x-coordinate of point F on the elliptic curve;
y_F	The value of the y-coordinate of point F on the elliptic curve;
$H(x)$	A one-way hash function, satisfying $H^j(x) = H(x, H^{j-1}(x))$ and $H^0(x) = x$;
SK_{AH}	AH's private key;
PK_{AH}	AH's public key;
B_i	The ith bidder;
$bid_{i,j}$	A bid price that is placed by B_i in the jth round of auction;
Sk_i	B_i's private key;
RK_i	B_i's registration key;
k_i, $t_{1,i}$, $t_{2,i}$	Three secret parameters that are chosen by B_i;
$N_{i,j}$	A pseudonym that RM creates for B_i in the jth round of auction;
r_j	A random number chosen by AH in the jth round of auction;
G_j	The public information published by AH in the jth round of auction;
$TPK_{i,j}$	A transaction public key that AH generates for B_i in the jth round of auction;

3.3. Proposed method

3.3.1. Initialization

RM and AH establish system parameters and the steps are as follows:

(1) RM

Step 1: Set up a read-only bulletin board (BB_{RM}) and post two kinds of information. One is registration key and identity information of all bidders, the other is pseudonyms used by the bidders in the jth round of auction. RM is the only one that can write and update the bulletin board.

Step 2: Select a big prime number for p.
Step 3: Declare an elliptic curve equation, $E_p(a,b)$: $y^2 = x^3 + ax + b \pmod p$, that satisfies $(a,b) \in Z_p$ and $4a^3 + 27b^2 \neq 0 \pmod p$.
Step 4: Select and declare a generative point G with an order as q, which is a big prime number and its value should be within $p + 1 \pm 2\sqrt{p}$.

(2) AH
Step 1: Set up a read-only bulletin board (BB_{AH}) and post the transaction public key and related information of all bidders on the board. AH is the only one authorized to write and update the bulletin board.
Step 2: Randomly select an integer $SK_{AH} \in [1, q-1]$ as the private key and use it to calculate the corresponding public key PK_{AH}. The equation is as follows:

$$PK_{AH} = SK_{AH}G. \tag{1}$$

Step 3: Post PK_{AH} on BB_{AH}.

3.3.2. Registration

Before a new bidder (B_i) can join in an auction, he/she must first apply for registration with RM. On completing registration, RM will generate a pseudonym for B_i; the pseudonym can only be used in the jth round of auction.

B_i should first calculate all relevant parameters before registering with RM. The registration process is as shown below:

Step 1: B_i randomly selects an integer $SK_i \in [1, q-1]$ as the private key and computes a corresponding registration key RK_i. The equation is as follows:

$$RK_i = SK_iG. \tag{2}$$

Step 2: B_i randomly selects an integer $k_i \in [1, q-1]$ as a secret parameter.
Step 3: B_i randomly selects an integer $t_{1,i} \in [1, q-1]$ and computes the verification information $(\gamma_i, \varepsilon_i)$. The computation steps are as follows:

$$F_{1,i} = t_{1,i}G = (x_{F_{1,i}}, y_{F_{1,i}}), \tag{3}$$

$$\gamma_i = H(x_{F_{1,i}} \| y_{F_{1,i}}), \tag{4}$$

$$\varepsilon_i = (t_{1,i} + \gamma_i \cdot SK_i) \bmod q. \tag{5}$$

Step 4: B_i sends the information $\{RK_i, k_i, \gamma_i, \varepsilon_i\}$ and identity information (ID_i) through a secure channel to RM. On receiving the information, RM processes the registration.
Step 5: RM authenticates the validity of $\{RK_i, k_i, \gamma_i, \varepsilon_i\}$ by the following equations:

$$F'_{1,i} = \varepsilon_i G - \gamma_i RK_i = \left(x_{F'_{1,i}}, y_{F'_{1,i}}\right), \tag{6}$$

$$\gamma'_i = H\left(x_{F_{1,i'}} \| y_{F'_{1,i}}\right), \tag{7}$$

$$\gamma'_i \stackrel{?}{=} \gamma_i. \tag{8}$$

If Eq. (8) holds, $\{RK_i, k_i, \gamma_i, \varepsilon_i\}$ is valid. This proves SK_i and RK_i correspond to each other. In contrast, RM would refuse to accept the registration application from B_i if the received information is forged.
Step 6: RM stores B_i's identity information ID_i and the corresponding secret parameter k_i in its own database.
Step 7: RM would post B_i's identity information ID_i and registration key RK_i on BB_{RM}.
Step 8: Before the jth round of auction starts, RM would generate a pseudonym ($N_{i,j}$) for each bidder B_i. The order of all pseudonyms would be randomly arranged and posted on BB_{RM}. The equation is as shown below:

$$N_{i,j} = H^j(k_i)RK_i. \tag{9}$$

Step 9: B_i can use Eq. (9) to compute his/her own pseudonym and verify that his/her pseudonym matches with the one that is posted on BB_{RM}. If B_i does not find his/her pseudonym on BB_{RM}, he/she can appeal to RM.

3.3.3. Transaction public key generation

In the jth round of auction, B_i can obtain auction information through AH who retrieves information about currently open auctions from the broker agent. The broker agent would prepare an auction list that matches the needs of B_i and send the list back to the AH for B_i to review. After B_i decides which auction he/she wants to participate in, B_i has to apply for a transaction public key ($TPK_{i,j}$), which is managed by AH. AH would generate $TPK_{i,j}$ with B_i's pseudonym on BB_{RM} for the bidder. The steps are as follows:

Step 1: AH randomly selects an integer $r_j \in [1, q-1]$ and computes public information G_j. Then, AH posts G_j on BB_{AH}. The equation is as shown below:

$$G_j = r_jG \tag{10}$$

Step 2: AH uses $N_{i,j}$ and its own private key SK_{AH} to generate a parameter $S_{i,j}$ and $TPK_{i,j}$ for each B_i, and post the generated information on BB_{AH}. The equation is shown as below:

$$S_{i,j} = SK_{AH}N_{i,j} = (x_{S_{i,j}}, y_{S_{i,j}}) \tag{11}$$

$$TPK_{i,j} = \left(r_j \cdot x_{S_{i,j}}\right)N_{i,j} \tag{12}$$

3.3.4. Signature

Before B_i starts to participate in the auction, B_i must verify the $TPK_{i,j}$ given by the AH on BB_{AH}. If the key is valid, B_i would calculate the corresponding signature with his/her bid price along with the related information. Subsequently, B_i can start participating in the bidding. The steps are as follows:

Step 1: B_i uses AH's public key PK_{AH} to compute a parameter $S'_{i,j}$, as follows:

$$S'_{i,j} = (H^j(k_i) \cdot SK_i)PK_{AH} = \left(x_{S'_{i,j}}, y_{S'_{i,j}}\right) \tag{13}$$

Step 2: B_i combines his/her private key SK_i and parameter $S'_{i,j}$ to generate $TPK'_{i,j}$, as follows:

$$TPK'_{i,j} = (H^j(k_i) \cdot x_{S'_{i,j}} \cdot SK_i)G_j \tag{14}$$

B_i must check that $S'_{i,j}$ and $TPK'_{i,j}$ matches with the information posted on the BB_{AH}; if not, B_i can appeal to AH.
Step 3: B_i randomly selects an integer $t_{2,i} \in [1, q-1]$ and decides on a bid price $bid_{i,j}$. Afterwards, a corresponding signature $\{\alpha_{i,j}, \beta_{i,j}\}$ is created, as shown below:

$$F_{2,i} = t_{2,i}G_j = (x_{F_{2,i}}, y_{F_{2,i}}) \tag{15}$$

$$\alpha_{i,j} = H(x_{F_{2,i}} \| y_{F_{2,i}} \| bid_{i,j}) \tag{16}$$

$$\beta_{i,j} = (t_{2,i} + \alpha_{i,j} \cdot H^j(k_i) \cdot x_{S_{i,j}} \cdot SK_i) \bmod q \tag{17}$$

3.3.5. Auction bidding

Before the start of the auction, B_i needs to obtain a bid agent from the AH. After a bid agent is acquired, B_i, then, is allowed to bid. The bidding process is as follows:

Step 1: $B_i$should first send out the bidding information $\{TPK_{i,j}, bid_{i,j}, \alpha_{i,j}, \beta_{i,j}\}$ to AH and apply for a bid agent.
Step 2: After the AH receives the bidding information from B_i, $\{TPK_{i,j}, bid_{i,j}, \alpha_{i,j}, \beta_{i,j}\}$ has to be verified. The equations for verification are as shown below:

$$F'_{2,i} = \beta_{i,j}G_j - \alpha_{i,j}TPK_{i,j} = \left(x_{F'_{2,i}}, y_{F'_{2,i}}\right) \quad (18)$$

$$\alpha'_{i,j} = H\left(x_{F'_{2,i}} \| y_{F'_{2,i}}\right) \quad (19)$$

$$\alpha'_{i,j} \stackrel{?}{=} \alpha_{i,j} \quad (20)$$

If Eq. (20) holds, this proves that $\{TPK_{i,j}, bid_{i,j}, \alpha_{i,j}, \beta_{i,j}\}$ is valid, and vice versa. AH can reject the bidding request from B_i if the received information is false.

Step 3: AH uses the bidding information to create a new bid agent for B_i. The new agent is then sent to the selected AUH to represent B_i in the auction.
Steps 1, 2, and 3 can be skipped if the bid is placed more than once. Only the bidding information would be verified.

Step 4: When the bid agent arrives at the AUH, the $TPK_{i,j}$ is checked to see that it matches that posted on BB_{AH}. If not, AUH can reject B_i's application.

Step 5: AUH verifies the bidding information $\{TPK_{i,j}, bid_{i,j}, \alpha_{i,j}, \beta_{i,j}\}$ like in Step 2. If Eq. (20) holds, it means that $\{TPK_{i,j}, bid_{i,j}, \alpha_{i,j}, \beta_{i,j}\}$ is valid.

Step 6: AUH posts the bidding information $\{TPK_{i,j}, bid_{i,j}, \alpha_{i,j}, \beta_{i,j}\}$ on BB_{AUH}. Anyone can use the equation listed in Step 2 to verify the bidding information of B_i.

3.3.6. Winner announcement

When the jth round of auction ends, the one who places the highest bid price would be announced as the winner. Then AUH would take the winner's $TPK_{i,j}$ to reconfirm the winner's information, $N_{i,j}$ and RK_i, with AH and RM. Afterwards, the result would be posted on BB_{AUH} and can be used by anyone for verification purpose. The steps are as follows:

Step 1: AUH takes the winner's $TPK_{i,j}$ to AH and ask for the pseudonym $N_{i,j}$ used by the winner.

Step 2: AH returns the information $\{TPK_{i,j}, (r_j \cdot x_{S_{i,j}}), N_{i,j}\}$ to the AUH.

Step 3: AUH can use Eq. (12) to confirm the relationship between $TPK_{i,j}$ and $N_{i,j}$.

Step 4: AUH takes the winner's $N_{i,j}$ to RM and ask for the winner's RK_i.

Step 5: RM returns the information $\{N_{i,j}, H^j(k_i), RK_i\}$ to the AUH.

Step 6: AUH can use Eq. (9) to confirm the relationship between $N_{i,j}$ and RK_i.

Step 7: The AUH will post the winner's information, $\{TPK_{i,j}, (r_j \cdot x_{S_{i,j}}), N_{i,j}\}$ and $\{N_{i,j}, H^j(k_i), RK_i\}$, on BB_{AUH}. The winner's information on BB_{AUH} can be obtained by anyone to verify again by using Eqs. (9) and (12).

4. Security analysis

Security requirement for the online auction protocol (Lee et al., 2001) are examined as follows:

(1) Anonymity
Unless RM and AH work together to reveal the identity during the auction, nobody else can determine the identity of a bidder. We analyze the anonymity of bidders from the perspectives of RM, AH, and AUH.
(i) AUH is only authorized to obtain the bidding information $\{TPK_{i,j}, bid_{i,j}, \alpha_{i,j}, \beta_{i,j}\}$. $\{\alpha_{i,j}, \beta_{i,j}\}$ is the signature for $bid_{i,j}$ and $TPK_{i,j}$ is a key for verification. Thus, AUH can only use $TPK_{i,j}$ to verify the signature and compare $TPK_{i,j}$ to the one that is posted on BB_{AH}. AUH cannot determine the identity of a bidder.
(ii) AH merely knows the relationship between $N_{i,j}$ and $TPK_{i,j}$; thus, it does not have enough information to be able to recognize the bidder.
(iii) Although RM has all the bidder's identity information, it is still unable to derive the corresponding $N_{i,j}$ from $TPK_{i,j}$.

(2) Traceability
Anyone can get $\{TPK_{i,j}, (r_j \cdot x_{S_{i,j}}), N_{i,j}\}$ and $\{N_{i,j}, H^j(k_i), RK_i\}$ from the BB_{AUH} and use Eqs. (9) and (12) to verify the winning bidder's identity.

(3) No framing
Unless attackers get the B_i's SK_i, B_i's signature cannot be forged. Even if attackers get the RK_i and intend to derive the SK_i from the RK_i, it will be difficult for him/her to obtain SK_i because of the Elliptic Curve Discrete Logarithm Problem (ECDLP).

(4) Unforgeability
Attackers will be unable to calculate the transaction public key by using the equation $TPK_{i,j} = (H^j(k_i) \cdot x_{S'_{i,j}} \cdot SK_i)G_j$ or forge any valid bidding information $\{TPK_{i,j}, bid_{i,j}, \alpha_{i,j}, \beta_{i,j}\}$. The reason can be explained in three aspects.
(i) Attackers cannot obtain Bi's SK_i, K_i and $S_{i,j}$.
(ii) Attackers have to spend a great deal of time trying to solve ECDLP, even if they manage to obtain $(H^j(k_i) \cdot x_{S'_{i,j}} \cdot SK_i)$.
(iii) Because $H^j(k_i)$ is different in each around of auction, the bidder's pseudonym $N_{i,j}$ and transaction public key $TPK_{i,j}$ would also be different in each around of auction.

(5) Non-repudiation
Signature is hidden inside the bidding information and it has the characteristics of no framing. Therefore, the winning bidder of the auction shall not be able to deny his/her signature.

(6) Fairness
All bidders use pseudonyms to join in the auction. AUH will post the valid bidding information on the BB_{AUH}. If B_i does not find his/her bidding information, he/she can appeal to AUH. In this way, AUH can handle all bidders' information with fairness.

(7) Public verifiability
Anyone can confirm the validity of the bidder, the validity of a bid, and the winning bidder's real identity.

(8) Unlinkability among various auction rounds
The pseudonym generated by RM and the transaction public key generated by AH are different for each auction. Unless RM and AH share these keys with each other, no one else can know B_i's relationship with the various auction rounds.

(9) Linkability within a single auction round
Within a single round of the auction, B_i holds the same $TPK_{i,j}$ to place a bid in the auction. How many times a bidder places bids and who has placed a bid can be traced.

(10) Efficiency of Bidding
The Elliptic Curve Cryptosystem can reduce the computation loads that are generated by online bidding operations.

(11) One-time registration
Bidder uses a pseudonym $N_{i,j}$ to participate in the auction. Hence, B_i only needs to register once with RM.

(12) Easy revocation
It is easy for RM to delete the bidder's identification and secret parameters from the database. Once the information is removed from the database, the bidder loses the right to participate in auctions.

5. Conclusion

This paper puts forward an agent-based English auction protocol to allow bidders to obtain information and participate in auctions using an agent. Our security analysis shows that our

proposal clearly satisfies all of the security requirements of online auction protocol, such as anonymity, traceability, fairness, and so on. Since we recognize that, inherently, mobile devices have weaker computation capability, we employ Elliptic Curve Cryptosystem on the mobile agent to give it a lower computation amount and small key size, both of which helps in reducing the time consumed by verification and computation. This is a means to make online auction on mobile devices more efficient and convenient. As wireless networks continue to be used extensively, our proposed method uses only the least possible amount of wireless data exchange for the sake of better security. In the future, we plan to focus on enhancing data protection in relation to auctions.

Acknowledgements

The authors are very grateful to the anonymous reviewers for their constructive comments which improved the quality of this paper. This work was supported by National Science Council of Taiwan, ROC under Grant NSC 99-2221-E-029-023.

References

Chang, C.C., & Chang, Y.F. (2006). Enhanced anonymous auction protocols with freewheeling bids. In *20th international conference on advanced information networking and applications. Vol. 1* (pp. 353–358).

Chang, C. C., & Chang, Y. F. (2003). Efficient anonymous auction protocols with freewheeling bids. *Computers and Security, 22*(8), 728–734.

Chung, Y. F., Lee, H. H., Lai, F., & Chen, T. S. (2008). Access control in user hierarchy based on elliptic curve cryptosystem. *Information Sciences, 178*(1), 230–243.

Guan, D.J., & Jen, L.H. (2005). Study and implementation of elliptic curve cryptosystem, Master's Thesis, National Sun Yat-Sen University of Technology, Kaohsiung.

Huang, Z.X. (2003). Applying data mining to analyze online auction market, Master's Thesis, Chaoyang University of Technology, Taichung.

Huang, K.H. (2008). Mobile auction agent model using agent-based english auction protocol, Doctoral Dissertation, National Taiwan University, Taipei.

Huang, K. H., Chung, Y. F., Liu, C. H., Lai, F., & Chen, T. S. (2009). Efficient migration for mobile computing in distributed networks. *Computer Standards & Interfaces, 31*(1), 40–47.

Jiang, R., Pan, L., & Li, J. H. (2005). An improvement on efficient anonymous auction protocols. *Computers and Security, 24*(2), 169–174.

Johnson, D., Menezes, A., & Vanstone, S. (2001). The elliptic curve digital signature algorithm (ECDSA). *Information Security, 1*, 36–63.

Koblitz, N. (1987). Elliptic curve cryptosystems. *Mathematics of Computation, 48*(177), 203–209.

Lee, F. M., Chen, J. P., & Hung, J. W. (2000). Applying software agent on internet auction and bargaining system. *Institute of Information and Computing Machinery, 3*(2), 67–80.

Lee, B., Kim, K., & Ma, J. (2001). Efficient public auction with one-time registration and public verifiability. In *Second international conference on cryptology-DINDOCRYPT 2247*(pp. 162–174).

Miller, V.S. (1986). Use of elliptic curves in cryptography, advances in cryptology. In *Proceedings of Crypto '85. Vol. 218*(pp. 417–426).

Nguyen, K.Q., & Traore, J. (2000). An online public auction protocol protecting bidder privacy. In *5th Australasian conference on information security and privacy. Vol. 1841* (pp. 427–442).

Omote, K., & Miyaji, A. (2001). A practical english auction with one-time registration. In *6th Australasian conference on information security and privacy. Vol. 2119* (pp. 221–234).

Peng, F. C., Chang, C. O., & Chen, M. C. (2008). A study of influence of different auction mechanism to no-performing assets. *Sun Yat-Sen Management Review, 16*(3).

Shieh, C.W. (2006). An efficient design of elliptic curve cryptography processor, Master's Thesis, Tatung University, Taipei.

Wu, S.T. (2005). Authentication and group secure communications using elliptic curve cryptography, Doctoral Dissertation, National Taiwan University of Science and Technology, Taipei.

Wu, T. C., Chen, K. Y., & Lin, Z. Y. (2002). An english auction mechanism for internet environment. In *ISC 2002* (pp. 331–337).