SECURE SCHEMES FOR AN ON-LINE AUCTION SERVICE

Woei-Jiunn Tsaur and *Kao-Hsin Hu*

Department of Information Management
Da Yeh University, Changhwa, Taiwan, R.O.C.
Email: wjtsaur@mail.dyu.edu.tw

ABSTRACT

In this paper we construct secure on-line auction schemes suitable for English auction. This paper uses a self-certified public key cryptosystem so that the system authority cannot impersonate any legal bidder. Moreover, the auction chairman cannot know who joins the auction since bidders join it with pseudonym for anonymity. For the considerations of efficiency, the schemes are developed by using elliptic curve cryptosystems instead of modular exponentiation, because it possesses faster computation and fewer bits achieving the same security degree as other public key cryptosystems. In this paper, we design several security schemes in an on-line auction environment using the self-certified public key cryptosystem based on elliptic curve cryptosystems. The proposed schemes make the on-line auction securely workable.

Keywords: Electronic commerce, Information security, Self-certified public key cryptosystems, Auction, Elliptic curve cryptosystems

1. INTRODUCTION

Communication security is one of important topics in the Internet, especially in electronic commerce. In this paper, we discuss several security issues of an on-line auction, develop efficient self-certified public key cryptosystems rather than current digital certificate scheme, and apply them to the on-line auction.

Most of auction web sites are off-line auction activities. It means when someone joins an auction, he/she will get the result after a period (maybe 3 days). But, in our real life we are used to English auction (all bidders bid at the same place and time and get the result at the moment). In other words, there are a variety of differences between our real life and current web sites auction. In addition, most of the electronic commerce web sites use the SSL (Secure Socket Layer) [19] or SET (Secure Electronic Transaction) [19] scheme as their security protection. The two schemes are to use the digital certificate scheme signed by the trusted third party to achieve the identity authentication. When using the digital certificate scheme, it is assumed that the certification authority (CA) must be fully trusted and cannot be intruded. Therefore, we have developed efficient self-certified schemes instead of using digital certificate. The proposed schemes can prevent CA from intervening in the transactions between web sites and customers, and they can authenticate their identities each other without the help of CA. Although many self-certified public key cryptosystems, e.g., [3], [7], [13], and [16], are presented, but they all used inefficient modular exponentiation operation, which has a high computation time complexity. In this paper, we propose efficient self-certified public key cryptosystems based on elliptic curve cryptosystems (ECC) to improve the inconvenient digital certificate scheme.

The rest of this paper is organized as follows. In Section 2, we review all kinds of auction, elliptic curve cryptosystems, and other public key cryptosystems. In Section 3, we develop ECC-based self-certified cryptosystems and apply them to the on-line English auction. In Section 4, we analyze the security of our proposed schemes and the on-line English auction. In Section, we analyze the performance of our proposed on-line English auction. Finally, some concluding remarks are given in Section 6.

2. PRELIMINARY

2.1 The Kinds of Auction

The auction is a market economy with clear rules, and bidders win the resources by the bided-price. There are two kinds of auction rules according to the price whether is public or not [1, 8, 13].

2.1.1 Open Outcry

The rule is that all bidders bid at the same place and time. According to the public price type, there are the following two kinds of auction:

(1) English auction: there is a chairman in charge of the auction. The bidders must go to the auction place to join the auction. The bidders bid from the floor price freely until there is no bidder to bid higher price. Finally, the last bidder wins the resource with the last price. All the bid prices are opened at the auction conference.

(2) Dutch auction: it is the same as English auction expect that there is a difference at the price decision. In Dutch auction, the chairman bids a very high price at first. If none promises the price, then the chairman will reduce the price. Until there is some bidder agrees to the price, the auction is over. The first outcry bidder is the winner with that price.

2.1.2 Sealed Bid

Each buyer submits only one bid in a sealed envelope. When the deadline is due, the chairman opens the sealed envelopes and claims the winner by the auction rules. By the price decision, there are two kinds of sealed bid auction as follows:

1. First-price sealed bid auction: the winner's price is the price he wrote down.

2. Second-price sealed bid auction: the winner's price is the next highest one.

This paper will focus on the English auction because we are used to it. As for the sealed bid auction, Franklin and Reiter [6] have proposed a secure auction scheme.

2.2 Elliptic Curve Cryptosystems (ECC)

The solution of an elliptic curve E: $y^2 = x^3 + ax + b$ ($4a^3+27b^2 \neq 0$) will be a group. Let P and Q be the points of E. If the order n of E is large enough (n * P = O, O is the infinite point), then it is hardly to find x to satisfy Q = x * P. This is well-known ECDLP [20] (Elliptic curve discrete logarithm problem). Koblitz [11] and Miller [12] implement this characteristic to elliptic curve cryptosystems. We need 1024 bits of key when using modular exponentiation schemes, like RSA or ElGamal cryptosystems, but we can get the same security level only using 160 bits in ECC [9].

2.3 Public Key Cryptosystems

There are two important keys in public key cryptosystems. One is secret key (SK) for decryption and signature, the other is public key (PK) for encryption and de-signature. There are three kinds of public key cryptosystems as follows: certificate-based public key cryptosystems, identity-based public key cryptosystems, and self-certified public key cryptosystems. We describe the three kinds of cryptosystems as below.

2.3.1 Certificate-Based Public Key Cryptosystems

Because the public keys are as public as possible, they are particularly vulnerable to active attacks in the system. Hence, we need another parameter G to guarantee the public key. In this system, we must add 2 important parameters, ID for one's identity and G for guaranteeing the ID and PK. However, certificate-based public key cryptosystems have the following two drawbacks [7]:

Table 1: The comparisons of four kinds of self-certified public key cryptosystems

	Girault [7]	Saeednia [16, 23]	Chang, Wu and Huang [3]	Petersen and Horster [13]
Generating secret key	Created by users	Created by users	1.Created by users 2.With the help of users' PK	1.Created by users 2.With the help of CA' s signature
Generating public key	Created by CA	Created by users according to their SK	1.Create by CA 2.With the help of the random number selected by users	Created from the public information
Verifying public key	1.Verifying by users themselves 2.With the help of CA' s PK	1.Verifying by users themselves 2.Verifying according to the identities of users themselves	1.Verifying by users themselves 2.Verifying by users' SK and CA' s PK	1.Verifying by users themselves 2.Verifying by users' SK and public information
Generation order of keys and verification formula	1.SK 2.PK 3.Verification formula	1.SK 2.PK 3.Verification formula	1.PK 2.SK 3.Verification formula	1.Verification formula 2.SK 3.PK
Security basis	RSA [14]	RSA [14]	ElGamal [5]	Schnorr [17]
Trust level	Level 3	Level 3	Level 3	Level 4

2.3.1 Certificate-Based Public Key Cryptosystems

Because the public keys are as public as possible, they are particularly vulnerable to active attacks in the system. Hence, we need another parameter G to guarantee the public key. In this system, we must add 2 important parameters, ID for one's identity and G for guaranteeing the ID and PK. However, certificate-based public key cryptosystems have the following two drawbacks [7]:

1. Because G is a guarantee generated by CA, CA can arbitrarily forge a legal user. If CA is dishonesty or attacked, then CA can create a fake user and other legal users cannot detect the situation.

2.For the correctness of users' PK, CA must store extra parameter (G).

2.3.2 Identity-Based Public Key Cryptosystems

Shamir [18] proposed this scheme at 1984. The characteristic of this systems is that the PK = ID and SK = G, so CA needs fewer storage space. But identity-based public key cryptosystems also have two drawbacks [13]. One is that dishonest CA may impersonate any user, since all secret keys of users are known to CA. The other is that it can hardly create a secret channel in the Internet for SA to transmit the secret key to users.

2.3.3 Self-Certified Public Key Cryptosystems

The self-certified public key can implicitly verify itself without accompanying with additional certificate. The four trust levels proposed by Girault [7] and Pertson-Hoster [13] are described as follows:

Level 1: the authority knows (or can easily compute) uses' secret keys and, therefore, can impersonate any user at any time without being detected.

Level 2: the authority does not know (or cannot easily compute) users' secret key. Nevertheless, the authority can still impersonate a user by generating false guarantees (e.g. false certificates).

Level 3: the frauds of the authority are detectable. More precisely, a public-key scheme will be said of level 3 if the authority cannot compute users' secret keys, and if it can be proven that it generates false guarantees of users if it does so.

Level 4: the authority issues a self-certified public key to a user with pseudonym PS, such that the real identity of the user is hidden to the authority. Nevertheless, all operations using the same pseudonym are linkable for any person.

In fact, self-certified public key cryptosystems can reach trust level 3 at least. But identity-based public key cryptosystems reach only level 1 and certification-based public key cryptosystems also reach only level 2. We compare four proposed self-certified public key cryptosystems in Table 1. All methods in Table 1 depend on RSA [14], ElGamal [5], and Schnorr [17] schemes. They are to use modular exponentiation needing large computing resource. However, the ECC scheme possesses faster computation and fewer bits achieving the same security degree as other public key cryptosystems. Although the certificate-based public key cryptosystem is a well-known and well-used method, by comparing it with the self-certified cryptosystem in Table 3 [13], we find it is more inefficient. Therefore, we develop efficient self-certified public key cryptosystems based on ECC, and apply them to the on-line English auction, as shown in Section 3.

Table 2: The comparisons of ECDSA (Elliptic Curve Digital Signature Algorithm) and other public key cryptosystems

	ECDSA [9]	ElGamal [5]	RSA [14]	Schnorr [17]
Encryption/decryption	Two keys	Two keys	Two keys	Two keys
Digital signature scheme	Yes	Yes	Yes	Yes
Key length	Short	Long	Long	Long
Encryption/decryption algorithm	Public	Public	Public	Public
Security basis	The security of solving discrete logarithm	The security of solving discrete logarithm	The security of solving discrete logarithm	The security of solving discrete logarithm

Table 3: The comparisons of certificate-based and self-certified public key cryptosystems

	Certificate-based	Self-certified
Public key directory	Need store the identity, public key and digital certification, and need make the consistence between the public key and the digital certification	Just need store the identity and public key
Validity of public key	Before using the public key, we must valid the public key	When using the public key, it valid the public key at the same time
Verification efficiency of public key	Validating the public key before it can be used	Validating the public key when it is using
Authentication efficiency when hierarchical CAs	All certificates have to be verified recursively throughout the hierarchy	As efficient as the computation of a single self-certified keys

3. THE SECURE ON-LINE AUCTION SCHEMES USING SELF-CERTIFIED PUBLIC KEY CRYPTOSYSTEMS

In this section, we develop self-certified public cryptosystems using ECC, and then apply them to the on-line English auction. First, we define some symbols as follows:

E: the elliptic curve, $y^2 = x^3 + ax + b$ $(4a^3+27b^2 \neq 0)$

K: a finite group, and K^2 is (x, y) satisfying E. The E(K) means $E \cup \{O\}$, O is the infinite point for E.

B: the generator of E

P_i: user U_i's public key

S_i: user U_i's secret key

I_i: user U_i's identity

ID_i: user U_i's auction identity

S_{CA}: CA's secret key

P_{CA}: CA's public key

3.1 The Proposed Security Schemes Based on ECC

[Self-certified public key cryptosystems based on ECC]

The steps are executed as follows:

1. User U_i selects his/her secret key S_i and computes $W_i = (S_i + I_i) * B \bmod K$, where W_i must be the generator of E. then U_i transmits it to CA.

2. CA computes $P_i = S_{CA} * W_i \bmod K$, and then transmits P_i to U_i.

3. U_i verifies $P_i = P_{CA} * (S_i + I_i) \bmod K$. If the result is correct, then U_i's public key is P_i and secret key is S_i.

[Session key]

By Diffie-Hellman's [4] and Botes-Penzhorn's [2] scheme, we derive the session key as follows:

1. Alice holds her secret key S_A, public key P_A and identity I_A, and Bob has his secret key S_B, public key P_B and identity I_B.

2. Alice sends P_A and I_A to Bob; Bob sends P_B and I_B to Alice.

3. The following session key S_{AB} is computed by Alice and Bob , respectively:

$$S_{AB} = P_B * (S_A + I_A) \bmod K$$
$$= S_{CA} * (S_A + I_A) * (S_B + I_B) \bmod K$$
$$S_{BA} = P_A * (S_B + I_B) \bmod K = S_{AB}$$

[Digital signature]

(a) The signature generation phase

We modify the ECDSA (Elliptic Curve Digital Signature Algorithm) [9] as follows:

1. U_a randomly selects a number k, and computes $k*P_{CA} \bmod K = (X_a, Y_a)$

2. Let $r = X_a$, U_a computes $s = k^{-1}(h(m) + S_a + I_a) * r)$, where $k*k^{-1} = 1 \bmod K$

3. The signature is (m,r,s)

(b) The signature verification phase

1. U_b computes $w = s^{-1}$ and h(m) , where $s*s^{-1} = 1 \bmod K$

2. Let $u_1 = w*h(m)$ and $u_2 = r*w$. U_b computes

$u_1 * P_{ca} + u_2 * P_a$

$= w*h(m)* P_{ca} + r*w*(S_a + I_a)* P_{ca}$

$= P_{ca}* s^{-1} *(h(m) + (S_a + I_a)* r) =(X_1, Y_1)$

3. If $r = X_1$, then the signature is correct.

[Auction key; AK]

Based on Wu's [22] conference key distribution systems, we propose an auction key (AK) for securing the English auction, which can avoid the pre-computation and save storage space as compared with Wu's [22] scheme. The steps are executed as follows:

(a) The system setup stage

Suppose that there are *m* users in the system and there are *n* users to join the auction ($n \leq m$). *h()* is the public hash function.

1. By using above session key, the auction chairman U_c computes the session key $SK_{ci} = P_i * (S_c + I_c) \bmod K$ shared with U_i ($1 \leq i \leq n$).

2. U_c randomly selects AK and the timestamp *t*.

3. U_c solves $A_i = \Delta_i / \Delta$ from the following equation system, where $h_i = h(SK_{ci} \| t) \| m$.

$$\begin{cases} A_1 * h_1 + A_2 * h_1^2 + A_3 * h_1^3 + \ldots + A_n * h_1^n = AK \bmod K \\ A_1 * h_2 + A_2 * h_2^2 + A_3 * h_2^3 + \ldots + A_n * h_2^n = AK \bmod K \\ \ldots \\ A_1 * h_n + A_2 * h_n^2 + A_3 * h_n^3 + \ldots + A_n * h_n^n = AK \bmod K \end{cases} \quad \text{Eqs. (1)}$$

$$\Delta = \begin{vmatrix} h_1 h_1^2 \ldots h_1^n \\ h_2 h_2^2 \ldots h_2^n \\ \ldots \\ h_n h_n^2 \ldots h_n^n \end{vmatrix} \qquad \Delta_i = \begin{vmatrix} h_1 \ldots h_1^{i-1} AK h_1^{i+1} \ldots h_1^n \\ h_2 \ldots h_2^{i-1} AK h_2^{i+1} \ldots h_2^n \\ \ldots \\ h_n \ldots h_n^{i-1} AK h_n^{i+1} \ldots h_n^n \end{vmatrix}$$

4. Let $F(x) = AK + A_1 * h_i + A_2 * h_i^2 + A_3 * h_i^3 + \ldots + A_n * h^n \bmod K$. If there exits any h_j ($n+1 \leq j \leq m$) satisfying $W(h_j) = 0$, then repeat Step 2.

5. U_c computes F(1),F(2),. .,.and F(*n*).

6. U_c boradcasts $\{t, P_c, I_c, F(1), F(2), \ldots, F(n)\}$.

(b) The auction key recovery stage

1. U_i computes the session key $SK_{ci} = P_c * (S_i + I_i) \bmod K$, and computes $h_i = h(SK_{ci} \| t) \| m$.

2. U_i solves AK from the following equation system by using Cramer's [15] rule.

$$\begin{cases} A_1 * h_i + A_2 * h_i^2 \ \ldots + A_n * h_i^n = AK \bmod K \\ A_1 * 1 + A_2 * 1^2 + \ldots + A_n * 1^n = F(1) + AK \bmod K \\ \ldots \\ A_1 * n + A_2 * n^2 + \ldots + A_n * n^n = F(n) + AK \bmod K \end{cases} \quad \text{Eqs. (2)}$$

3.2 Secure Schemes for the on-Line English Auction

We divide the English auction into the following four phases: the setup phase, the registration phase, the bidding phase, and the announcement phase.

[The setup phase]

CA keeps its secret key and publishes all the public information, including the elliptic curve E, generator B, and its public key P_{CA}. Each user U_i gets his/her public key P_i from CA by the above schemes.

[The registration phase]

CA announces the auction information and selects the chairman. Each registered bidder U_i gets an auction identity ID_i from CA.

[The bidding phase]

CA gives the chairman U_c both public keys and ID_is of all the registered users. By using the above proposed scheme, U_c then generates AK and each legal user U_i can get AK correctly. U_i can bid by encrypting both the price and his ID_i using AK after signing it with by his/her secret key. All the other legal user U_j, $1 \leqq j \leqq n$ and $j \neq i$, can decrypt it with AK to know the current price. Moreover, U_c can verify U_i's signature it by the U_i's public key from CA.

[The announcement phase]

If U_x wins the auction, U_c must make both ID_x and the least bidding price signed by the remaining bidders. U_c then transmits the signature to CA and claims the winner's bidding price. Finally, CA verifies the signature, gets the real identity I_x from ID_x, and closes the auction.

4. SECURITY ANALYSIS

4.1 The Proposed Self-Certified Public Key Cryptosystems Using ECC

[Secure ECC-based Self-certified public key cryptosystems]

Attackers can get the information P_{CA}, W_i and P_i, but he/she cannot get the secret key of both CA and each user.

Since $P_{CA} = S_{CA} * B \bmod K$, attackers cannot get S_{CA} due to the difficulty of solving ECDLP.

Since $W_i = (S_i + I_i) * B \bmod K$, attackers cannot get $(S_i + I_i)$ due to the difficulty of solving ECDLP.

$P_i = S_{CA} * W_i \bmod K$

$=(S_i + I_i) * P_{CA} \bmod K$

$=S_{CA} * (S_i + I_i) * B \bmod K$, attackers also cannot get S_{CA}, $(S_i + I_i)$, and $S_{CA} * (S_i + I_i)$ due to the difficulty of solving ECDLP.

[The proposed cryptosystems reach trust level 3]

1. Because the secret key is selected by user himself/herself and is not transmitted via a public channel. CA does not know the user's secret key.

2. In generating one's public key, CA must get the data W_i in advance from the user. That is, CA cannot decide users' public keys by self, and cannot impersonate any user.

3. If CA wants to forge a user, it must generate a pair of public key P_i' and secret key S_i'. However, this will lead to the fact that there are two public keys in the public key directory for one user. Thus, the dishonesty of CA is detectable.

[Session key]

When two users generate their session key, the attacker can get the P_a, I_a, P_b, I_b in the public channel. But attackers still cannot get their secret keys, because

$P_a = P_{CA} * (S_a + I_a) \bmod K$,

$P_b = P_{CA} * (S_b + I_b) \bmod K$,

$S_{ab} = P_{CA} * (S_a + I_a) * (S_b + I_b) \bmod K$.

That is, it is hardly possible for attackers to get the secret keys of users owing to the difficulty of solving ECDLP.

[On-line English auction with trust level 4]

Based on Petersen's and Hoster's [13] scheme, bidders user pseudonym for anonymity in the auction conference. When U_c distributes the auction key, attackers can get t, P_c, I_c, F(1), F(2), ..., and F(n) via the public channel, but he/she cannot recover AK by using only n points to solve Eqs(2). U_c generates AK without using any users' identity, so none can get other users' real identities from recovering AK. In the auction conference, although all bidders can know ID_i's auction price, they cannot know the real identity (I_i) of ID_i.

4.2 The Proposed on-Line English Auction

[CA or attackers cannot impersonate any other user]

Since the proposed schemes reach trust level 3 at least, the frauds of CA are detectable. Attackers still cannot get other users' secret keys due to the difficulty of solving ECDLP.

[Bidders cannot collude in the auction]

Because all bidders use ID_i to reach the trust level 4, all bidders are anonymous. In other words, they cannot collude in the auction conference.

[The chairman and the bidders cannot collude]

The chairman can gets only each registered user's ID_i and P_i when generating the AK. He/she doesn't know the relationship between I_i and ID_i, so the chairman and the bidders cannot collude.

[Illegal user cannot bid in auction conference]

The illegal user cannot get the (n+1)th point to recover AK, so he/she cannot bid in the auction conference.

[The winner cannot deny the bidding]

Since all legal bidding price is combined with the signature of the bidding user, the winner cannot deny his/her bidding.

[CA cannot close the auction more early]

Once CA gets the notification from the chairman, it can to close the auction. However, if CA closes the auction more early, the auction will have no result.

[The duty of both CA and the chairman is separate]

The chairman can generates only AK, but he/she cannot know who joins the auction; CA knows who joins the auction, but cannot get the AK. That is, CA still cannot intervene the auction conference.

[CA and the chairman collude]

If CA and the chairman collude, then it cannot reach level 4 in the auction conference. But the proposed schemes still reach trust level 3, in other words, CA still cannot impersonate any legal user.

5. PERFORMANCE ANALYSIS OF THE PROPOSED ENGLISH AUCTION

The following notation is used to measure the performance of the proposed English auction:

T_{ECC} is the time for ECC multiplication (P = a * Q mod K)

T_{MPY} is the time for modular multiplication

T_{DIV} is the time for division

T_H is the time for performing the one-way has function

T_{INV} is the time for computing inverse modulo K

T_{SYM} is the time for symmetry cryptosystems

It is pointed out [10] that $T_{MPY} = |K|^{\log_2 3} \cong |K|^{1.585}$, $T_{DIV} \cong T_{MPY}$, $T_{INV} \cong (0.843*\ln(K) + 1.47)* T_{DIV}$. In Table 4, we can find that more computation time is mainly spent at the phase of both generating and recovering the auction key AK, instead of the bidding phase. Hence, we can efficiently implement the on-line English auction.

[The time for generating or recovering the signature]

$T_{ECC}+T_H+T_{INV}$

[The time for generating AK]

$n*T_{ECC}$	(generating session key)
$+n*(T_H+(n-1)*T_{MPY})$	(solving Eqs.(1))
$+(n+2)*(n^2*T_{MPY})+T_{INV}$	(solving A_i and AK)
$+n*(n+1)*T_{MPY}$	(generating F(1),..F(n))

[The time for recovering AK]

T_{ECC}	(generating session key)
$+T_H+n*(n-1)*T_{MPY}$	(solving Eqs.(2))
$+2*n^2*T_{MPY}+T_{INV}$	(solving AK)

[The time for once bidding]

$T_{ECC}+T_H+T_{INV}+T_{SYM}$

Table 4: The time of four auction phases

	Setup phase	registration phase	Bidding phase		Announcement phase
			AK	Once bidding	
CA	T_{ECC}	$T_{ECC} + T_{SYM}$	0	0	$T_{ECC} + T_{SYM} + n(T_{ECC} + T_H + T_{INV})$
Chairman	0	0	$nT_{ECC} + n(T_H + (n-1)T_{MPY}) + (n+2)(n^2 * T_{MPY}) + T_{INV} + n(n+1)T_{MPY}$	$T_{ECC} + T_H + T_{INV} + T_{SYM}$	$T_{ECC} + T_{SYM}$
Bidder	$2T_{ECC}$	$T_{ECC} + T_{SYM}$	$T_{ECC} + T_H + n(n-1)T_{MPY} + 2n^2 T_{MPY} + T_{INV}$	$T_{ECC} + T_H + T_{INV} + T_{SYM}$	$T_{ECC} + T_H + T_{INV}$
Total	$3T_{ECC}$	$2(T_{ECC} + T_{SYM})$	$(n+1)T_{ECC} + (n+1)T_H + 2T_{INV} + (n^3+7n^2-n)T_{MPY}$	$2(T_{ECC} + T_H + T_{INV} + T_{SYM})$	$2T_{ECC} + 2T_{SYM} + 2n(T_{ECC} + T_H + T_{INV})$

6. CONCLUDING REMARKS

We have proposed self-certified public key cryptosystems using elliptic curve cryptosystems, including developing session key, digital signature, and auction key. We then apply these schemes to the on-line English auction. Compared to other public key cryptosystems using modular exponentiation, the proposed schemes not only use simpler operations but also can reach the same security degree as other public key cryptosystems by fewer bits. The proposed self-certificated public key cryptosystems are more efficient than the digital certificate scheme based on certification-based public key cryptosystems, because they can reach trust level 3 at least. Besides, due to pseudonym for anonymity, it is impossible for the auction chairman or other bidders to get the bidder's real identity. That is, the proposed scheme can reach trust level 4.

7. REFERENCE

[1] Bierman, H.S., and Fernandez, L., Game Theory with Economic Applications, Addison Wesley, 1993.

[2] Botes, J.J., and Penzhorn, W.T., "Public-Key Cryptosystems Based on Elliptic Curves," *Proceedings of the 1993 IEEE South African Symposium on Communications and Signal*, pp. 1-5, October 1993.

[3] Chang, Y.S., Wu, T.C. and Huang, S.C., "ElGamal-Like Digital Signature and Multisignature Schemes Using Self-Certified Public Keys," *The Journal of Systems and Software*, pp. 99-105, 2000.

[4] Diffie, W. and Hellman, M.E. "New Directions in Cryptography," *IEEE Transactions on Information Theory*, Vol. IT-22, No. 6, pp. 644-654, 1976.

[5] ElGamal, T., "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," *IEEE Transactions on Information Theory*, Vol. IT-31, No. 4, pp. 469-472, 1985.

[6] Franklin, M.K. and Reiter, M.K., "The Design and Implementation of a Secure Auction Service," *IEEE Transactions on Software Engineering*, Vol. 22, No. 5, pp. 302-312, May 1996.

[7] Girault, M., "Self-Certified Public Keys," *Advances in Cryptology: EUROCRYPT '91*, pp. 490-497.

[8] Huhns, M.N., and Vidal, J.M., "Online Auctions," *IEEE Internet Computing*, Vol. 3, No. 3, pp. 103-105, May-June 1999.

[9] Jurisic, A. and Menezes, A.J., "Elliptic Curves and Cryptography," *Dr. Dobb's Journal*, pp. 26-35, 1997.

[10] Knuth, D., E., The Art of Computer Programming Volume 2, Seminumerical algorithms, Addison-Wesley, 1981.

[11] Koblitz, N., "Elliptic Curve Cryptosystems," *Mathematics of Computation*, Vol. 48, No. 17, pp. 203-209, 1987.

[12] Miller, V.S., "Use of Elliptic Curves in Cryptography," *Advances in Cryptology: Crypto' 85*, pp.417-426.

[13] Petersen, H., and Horster, P., "Self-Certified Keys – Concepts and Applications", *Proceedings of Communications and Multimedia Security'97*, pp. 102-116, 1997.

[14] Rivest, R., Shamir, A. and Adleman, L.," A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Communications of the ACM*, Vol. 21, No. 2, pp. 120-126, 1978.

[15] Robinson, D.J.S., A Course in Linear Aigebra with Application, World Scientific, New Jersey, 1991.

[16] Saeednia, S., "Identity-Based and Self-Certified Key-Exchange Protocols," *Information Security and Privacy: ACISP '97*, pp. 303-313.

[17] Schnorr, C.P., "Efficient Identification and Signatures for Smart Cards," *Advances in Cryptology: Crypto' 89*, pp. 339-351.
[18] Shamir, A., "Identity-Based Cryptosystems and Signature Schemes," *Advances in Cryptology: Crypto ' 84*, pp. 47-53.
[19] Sherif, M.H., Serhrouchni, A., Gaid, A.Y., and Farazmandnia, F., "SET and SSL: Electronic Payments on the Internet," *Proceedings of Third IEEE Symposium on Computer and Communication*, pp. 353-358, 1998.
[20] Sliverman, J., The Arithmetic of Elliptic Curves, Springer-Verlag, New York, 1986.
[21] Vickrey, W., "Counterspeculation, Auctions, and Competitive Sealed Tenders," *Journal of Finance*, Vol. 16, pp. 8-37, March 1961.
[22] Wu, T.C., "Conference Key Distribution System with Use Anonymity Based on Algebraic Approach," *IEE Proceedings- Computers and Digital Techniques*, Vol. 144, No. 2, pp. 145-148, March 1997.
[23] Wu, T.C., Chang, Y.S., and Lin, T.Y. "Improvement of Saeednia's Self-Certified Key Exchange Protocols" *Electronics Letters*, Vol. 34, No. 11, pp. 1094-1095, 28 May 1998.