computers

MDPI

Article

BSEA: A Blind Sealed-Bid E-Auction Scheme for E-Commerce Applications

Rohit Kumar Das [1], Sanjeet Kumar Nayak [2,*], Sourav Kumar Bhoi [3], Suman Kumar Choudhury [4], Banshidhar Majhi [4] and Sujata Mohanty [4]

1 Samsung Electronics Pvt Ltd., Noida 201301, India; rohit.13das@gmail.com
2 Department of Computer Science and Engineering, Indian Institute of Technology, Patna 801103, India
3 Department of Computer Science and Engineering, Parala Maharaja Engineering College, Berhampur 761003, India; souravbhoi@gmail.com
4 Department of Computer Science and Engineering, National Institute of Technology, Rourkela 769008, India; suman.winter@gmail.com (S.K.C.); bmajhi@nitrkl.ac.in (B.M.); sujata.nitr@gmail.com (S.M.)
* Correspondence: sanjeet.588@hotmail.com; Tel.: +91-947-348-0414

Academic Editor: Kartik Gopalan
Received: 4 September 2016; Accepted: 5 December 2016; Published: 14 December 2016

Abstract: Due to an increase in the number of internet users, electronic commerce has grown significantly during the last decade. Electronic auction (e-auction) is one of the famous e-commerce applications. Even so, security and robustness of e-auction schemes still remain a challenge. Requirements like anonymity and privacy of the *bid* value are under threat from the attackers. Any auction protocol must not leak the anonymity and the privacy of the *bid* value of an honest Bidder. Keeping these requirements in mind, we have firstly proposed a controlled traceable blind signature scheme (CTBSS) because e-auction schemes should be able to trace the Bidders. Using CTBSS, a blind sealed-bid electronic auction scheme is proposed (BSEA). We have incorporated the notion of blind signature to e-auction schemes. Moreover, both the schemes are based upon elliptic curve cryptography (ECC), which provides a similar level of security with a comparatively smaller key size than the discrete logarithm problem (DLP) based e-auction protocols. The analysis shows that BSEA fulfills all the requirements of e-auction protocol, and the total computation overhead is lower than the existing schemes.

Keywords: security; e-auction; e-commerce; blind signature; security in wireless networks

1. Introduction

Recent advancement in modern technologies has converted many activities of human life into the digital/electronic format—for example, paper-based ballot to electronic voting system, paper-based cash to electronic cash, paper-based prescription to electronic health record, etc. Similarly, electronic auction (e-auction) is the electronic version of selling something to a bidder with highest bid value. More formally, it is a financial transaction procedure that helps in listing the price of commodities over a distributed environment. Initially, the auctioneer offers his goods, commodities or services on an auction website over the internet. Interested parties can submit their bid value for the product to be auctioned before the stipulated deadline. Generally, the auction procedure is transparent. All of the interested parties are allowed to participate in the auction process. Prior to e-auction, people were following a centralized approach to do the bidding process. Major limitations that motivated research community to switch from the centralized approach to the distributed approach are geographic area and time. Some challenges of e-auction like bidder's anonymity and bidder's privacy have to be resolved before adapting e-auction [1–4]. Generally, e-auction schemes can be categorized into four types including English auction, Dutch auction, sealed bid auction, and Vickrey

auction [5]. Due to the simple requirements of the sealed bid auction, it is always easy to implement it in an e-auction. Essential requirements of e-auction schemes are anonymity, non-repudiation, un-forgeability, traceability, public verifiability, integrity and confidentiality, fairness, authentication, privacy, and robustness [6,7]. In real life, there are some situations where we do not want to reveal the content of the message to the signing authority. In such cases, a blind signature serves the purpose. Blind signature is a variation of the digital signature, where the signer is unaware of the content of the message to be signed by him/her [8–12]. A list of requirements that needs to be satisfied by any blind signature scheme are: *Blindness*, *Correctness*, *Authentication*, *Integrity*, *Non-Repudiation*, *Un-forgeability*, *Non-Reusability*, and *Un-traceability* [13–15]. Blind signature schemes are designed as untraceable in applications like e-voting and e-cash [16–19]. However, blind signature application in the e-auction scheme requires controlled traceability. The advantages of elliptic curve cryptography (ECC)-based crypto-system over others like discrete logarithm problem (DLP) and the integer factorization problem (IFP) are: smaller key size, reduction in storage space, reduction in transmission requirement, and reduction in processing power [20–26]. Due to the smaller size key, ECC-based schemes can be applied in smart cards and *wireless communication systems*, where the devices have less memory, bandwidth, and computational power [27].

In this paper, we proposed a blind sealed-bid e-auction scheme using ECC (BSEA). Before proposing BSEA, we proposed a controlled traceable blind signature scheme (CTBSS), which is the basic building block of the proposed BSEA. In e-auction protocols, the Bidder corresponding to the max_bid should be traceable by the auction authorities. BSEA is shown to be resistant against various kinds of adversarial attacks like key only attack, forgery attack, known and chosen message attack, replay and eavesdropping attack, identity theft attack, and impersonate attack [28–31]. We have shown that BSEA satisfies all the requirements of the e-auction protocols. Based on the requirements and total computational overhead, we have performed a comparative analysis of our scheme with the existing schemes, and showed the results.

The rest of the article is organized as follows. Some related works are provided in Section 2. The proposed CTBSS using ECC is presented in Section 3. The security analysis of CTBSS is discussed in Section 4. The proposed e-auction protocol using CTBSS (BSEA) and its security analysis are given in Section 5 and Section 6, respectively. The performance analysis of the proposed BSEA is presented in Section 7. The concluding remarks are given in Section 8.

2. Related Work

Several e-auction protocols have been designed so far; however, the security of e-auction schemes remains a challenge.

In [32], the authors proposed a sealed-bid auction protocol where a malicious bidder cannot deny his bid value. They used a verifiable signature scheme to justify their protocol. In [33], a sealed bid auction method with a time server has been proposed, where after a certain time period, the sealed bids are opened and evaluated. An e-auction scheme to improve the privacy of bids such that the winner will be determined and known only by the auctioneer is proposed in [34]. Chang et al. [35] proposed three anonymous auction protocols to ensure bidder's privacy. They used a deniable authentication scheme to check the validity of the bids, where every bidder can bid arbitrarily and anonymously. However, in [36], Jiang et al. pointed out some security weakness of [35] where the bidder cannot detect the tampered response message from the auctioneer. Hence, Jiang et al. proposed an improved scheme that prevents tampering attacks. Subsequently, an improved method is proposed for further enhancement in [4]. In [37], the authors proposed an e-auction protocol consisting of four parties, namely, bidder, third party, auctioneer and bank. This scheme aims to solve the problem of the bidder's deposit payment with a deposit deducting certificate. However, in [38], the authors mentioned a security drawback, where the bidding receipt can be forged by the bidder to claim that she is the valid auction winner. Hence, the scheme proposed in [37] was unable to preserve the privacy of the bidders. Hence, it does not preserve the anonymity property. Even malicious bidders can forge

the bid receipt sent by the third party and can claim that she is a valid winner. In [38], the authors proposed an e-auction protocol that removes the flaws of [37] and was comparatively more secure and efficient. They have used symmetric key encryption instead of asymmetric key encryption to enhance the efficiency. However, the security of their scheme totally relies on the trust of the third party as it has all the information about the bidders who may affect in the subsequent auctions. Much more emphasis has been given to the third party instead of sharing the load. In [39], Cao et al. proposed an e-auction that is based on an untrusted third party. System preparing, bidder registration and blind signature, bidding, and bid opening are the phases of this scheme. This scheme satisfies bidder anonymity, unforgeability, non-repudiation, public verifiability, secret bidding prices, and fairness. In [40], the authors propose a secure and efficient electronic auction scheme with strong anonymity. However, the schemes presented in [39,40] fails to prove that their scheme fulfills traceability requirements of e-auction, which is very necessary in the current context of e-auction protocols. In [41], the authors have proposed a cryptographic e-auction protocol using the threshold cryptosystem. This protocol offers facilities like incontrovertibility of participants, integrity of data, incontrovertibility of offers, confidence of bids, anonymity of the winning bidder, and public verification. It provides traceability as the bidders themselves sign the message, and hence they cannot deny and are traceable. However, the identity of the bidder is not preserved here. In addition to the above facts, their security relies on the difficulty of solving the DLP for the sealed bid electronic auction. Therefore, an electronic online auction using the elliptic curve discrete logarithm problem will enhance the security level, which is the basic building block for the proposed BSEA. Hence, in BSEA, complete anonymity without any repudiation has been achieved.

3. Proposed Controlled Traceable Blind Signature Scheme

In this section, we discussed the proposed CTBSS. Three entities, namely, Signer, Requester (Sender), and Verifier participate in CTBSS. The objective of CTBSS is that the Requester has to get a blind signature of the Signer on the message and the Verifier can verify the authenticity of the signature present in the message, and this is shown in Figure 1. Before CTBSS starts, all the entities have to agree on the security parameters, i.e., an elliptic curve $E_p(a, b)$ of order p. The scheme uses some symbols and the meanings of these symbols are listed in Table 1. The CTBSS consists of four phases, such as key generation, blinding, signing, and unblinding with verification, which are described below via several algorithms. These phases are shown in Algorithms 1–4, respectively. The overall flow of the proposed CTBSS is given in Figure 2.

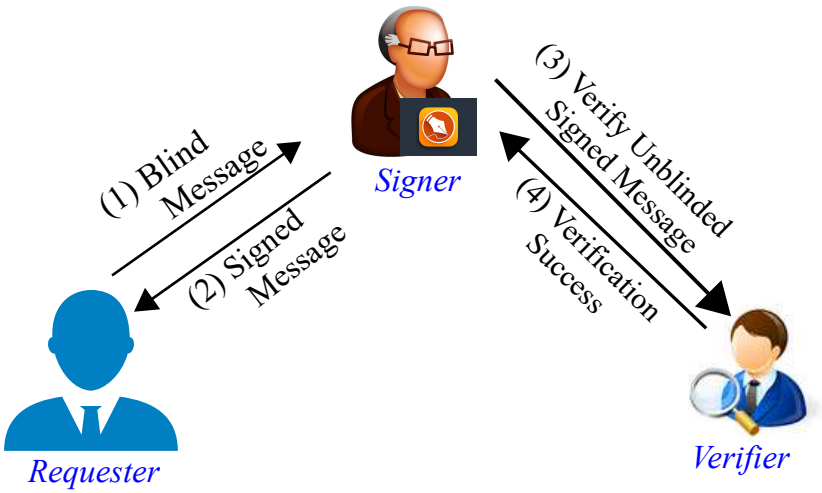

Figure 1. System model of CTBSS.

Table 1. Symbols used in CTBSS.

Symbols	Meaning
P	base point of large order, such that $nP = O$
n	number of points on $E_p(a, b)$
O	point at infinity
$r1_s, r2_s$	random numbers chosen by the Signer
$r1_r, r2_r$	random numbers chosen by the Requester
m	message
$H(.)$	secure hash function

Algorithm 1 Key Generation Phase

1: The Signer generates two random numbers $r1_s$ and $r2_s \mid r1_s, r2_s \in {Z_p}^*$.
2: She computes $X = r1_s P$, $Y = r2_s P$, and $Z = (Y + X)$.
3: Signer publishes his/her public parameters as $\langle X, Y, Z \rangle$ and keeps $r1_s$ and $r2_s$ as secret.

Algorithm 2 Blinding Phase

1: Requester generates two random numbers $r1_r$ and $r2_r \mid r1_r, r2_r \in {Z_p}^*$ ▷ $r1_r$ is the blinding factor used by the Requester.
2: She computes $M = r2_r Z$.
3: She computes $N = r2_r P$.
4: She calculates $u_1 = H(m)$ and $u_2 = (u_1 - r2_r) {r1_r}^{-1}$.
5: Sender publishes his/her public parameters as $\langle M, N \rangle$ and keeps $r1_r$ and $r2_r$ as secret.
6: Requester sends the blind message (u_2) to the Signer.

Algorithm 3 Signing Phase

1: After receiving u_2 from the Requester, the Signer signs the message by computing the following equation:

$$s = (r2_s + r1_s) u_2, \tag{1}$$

▷ s is the Signer's signature on the blind message.
2: Signer sends s to the Sender.

Algorithm 4 Unblinding with Verification Phase

1: After receiving s, the Sender unblinds the message by computing the following equation:

$$S = (s r1_r + r2_r) P. \tag{2}$$

2: The signed message of m by the Signer is S.
3: This can be verified by the Verifier using the following equation:

$$S + M - N \stackrel{?}{=} u_1 Z. \tag{3}$$

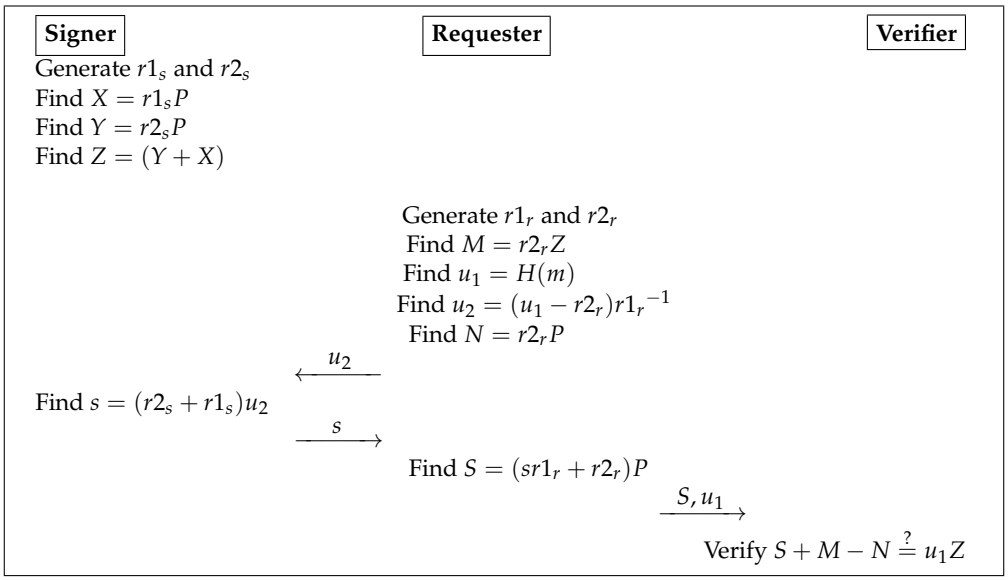

Figure 2. Schematic diagram of CTBSS.

4. Security Analysis of CTBSS

In this section, the security analysis of the proposed CTBSS is performed by considering various properties like correctness, blindness, traceability, and universally verifiable. CTBSS satisfies these properties on the assumption that elliptic curve discrete logarithm problem (ECDLP) is hard to break and the hash function $H(.)$ is secure and collision resistant.

4.1. Correctness Proof

The correctness of the proposed CTBSS is proved as follows. Here, we have shown that $S + M - N$ and $u_1 Z$ are same. Hence, the Verifier can be able to check the authenticity of the signature using Equation (3). Substituting the value of S from Equation (2) in left hand side (LHS) of Equation (3), we will obtain

$$S + M - N = (sr1_r + r2_r)P + M - N = sr1_r P + r2_r P + M - N.$$

Now, solving using the value of N,

$$\Rightarrow S + M - N = sr1_r P + N + M - N = sr1_r P + M.$$

Substituting the value of s using Equation (1),

$$\Rightarrow S + M - N = (r2_s + r1_s) u_2 r1_r P + M = (r2_s P + r1_s P)(u_2) r1_r + M.$$

Now, using the value of u_2,

$$\begin{aligned} \Rightarrow S + M - N &= (r2_s P + r1_s P)(u_1 - r2_r) r1_r{}^{-1} r1_r + M \\ &= (r2_s P + r1_s P)(u_1 - r2_r) + M \end{aligned}.$$

The above equation can be further simplified using X and Y and results in

$$\Rightarrow S + M - N = (Y + X)(u_1 - r2_r) + M.$$

Using the value of Z,

$$\Rightarrow S + M - N = Z(u_1 - r2_r) + M = u_1 Z - r2_r Z + M.$$

Now, using the value of M,

$$\Rightarrow S + M - N = u_1 Z - M + M = u_1 Z.$$

Hence, the correctness of the proposed CTBSS is proved.

4.2. Blindness

Given two signature pairs (S and S^*) out of which one is valid and one is previously stored, it is very difficult for the adversary to find the blinding factor $r1_r$ from S and S^*. From Z and M, it is very difficult for the adversary to find the value of $r2_r$. This happens due to the difficulty in solving the ECDLP problem.

4.3. Traceability

In blinding phase, the Requester sends the blind message to the Signer. Thus, the Signer can keep a list that contains values of type (u_2, s). Afterwards, the Requester sends the pair (S, u_1) to the Verifier for the message m, and the Signer can collect this value. By collecting these values, she will not be able to find the value of $r1_r$ and $r2_r$. However, using Equation (2) in the expression $S - N$, $S - N = (sr1_r + r2_r)P - r2_r P = sr1_r P$. This happens because the value of N is the public parameter of the Requester. Let $r1_r P = P^{'}$, and then $S - N = sP^{'}$. Now, the Signer will have the value of $S - N$. She can find the value of s^{-1}. $P^{'}$ can be found as $P^{'} = s^{-1}(S - N)$. Then, she compares, for every $P^{'}$, if $S - N = sP^{'}$. Hence, the Signer can trace the signature s for m, which depends on the number of blind signatures signed by the Signer.

4.4. Universally Verifiable

The blind signature can be verified by using the signature-message pair (S, u_1) and publicly available parameters (M, N, Z) for message m. Anyone can check its authenticity using Equation (3), once the Sender reveals the signature-message pair (S, u_1). Hence, CTBSS is universally verifiable.

5. Proposed Blind Sealed-Bid Electronic-Auction Scheme

In this section, we discussed the proposed blind sealed-bid e-auction scheme using elliptic curve cryptography (BSEA). CTBSS scheme is used in BSEA. The system model for the proposed BSEA is shown in Figure 3. BSEA consists of the advertisement phase, the registration setup phase, the registration confirmation phase, the bidding phase and the winner determination phase. These phases are described below.

In the advertisement phase, the Auctioneer will publish an advertisement and announce the start of the auction process. She will choose the system parameters such as $E_p(a, b)$ as the elliptic curve of order p and P as the base point. She will choose s_a as his/her private key. Then, she will find his/her public key P_a as $P_a = s_a P$. After this, the auction message M_a will be signed by the Auctioneer using his/her private key as $\text{Sign}_{s_a}(M_a)$. $\text{Sign}_{s_a}(M_a)$ is sent to the Third Party to publish on the web, so that the auction message will be available to the public. This signed message can be verified by anyone using the Auctioneer's public key.

The registration setup phase facilitates interested Bidders to register to the system before submission of their *bid*. Registration Manager (RM) is an entity with which every individual Bidder has to register. RM provides anonymity to each and every individual Bidder. In order to register, several steps are carried out by both the RM and the Bidder as mentioned in Algorithm 5. The overall flow of this phase is given in Figure 4.

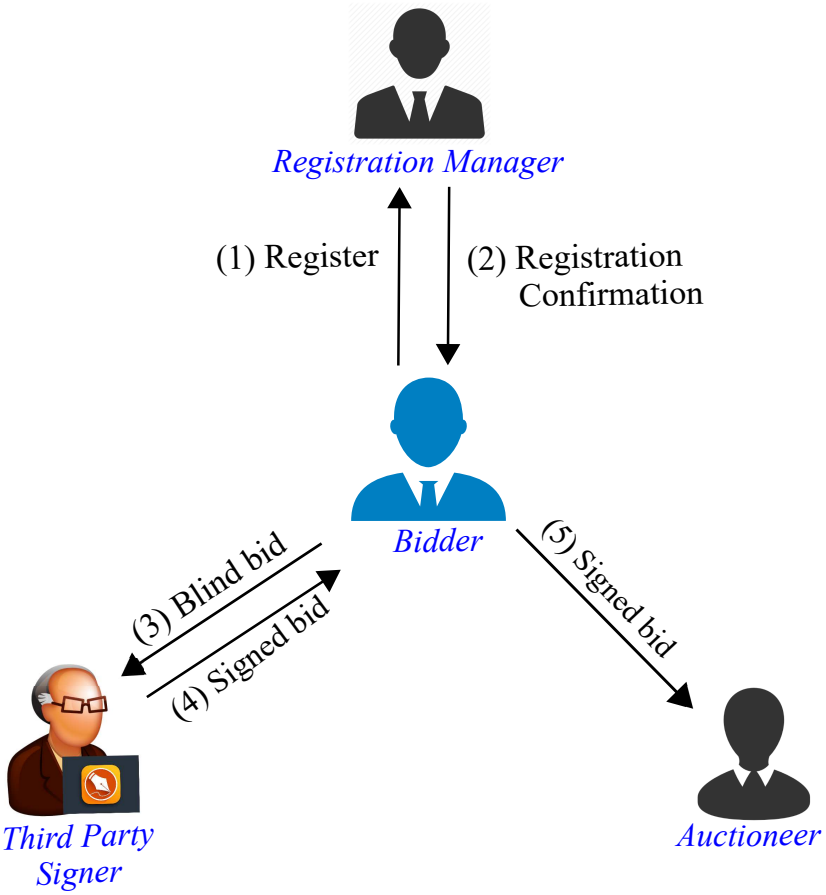

Figure 3. System model of BSEA.

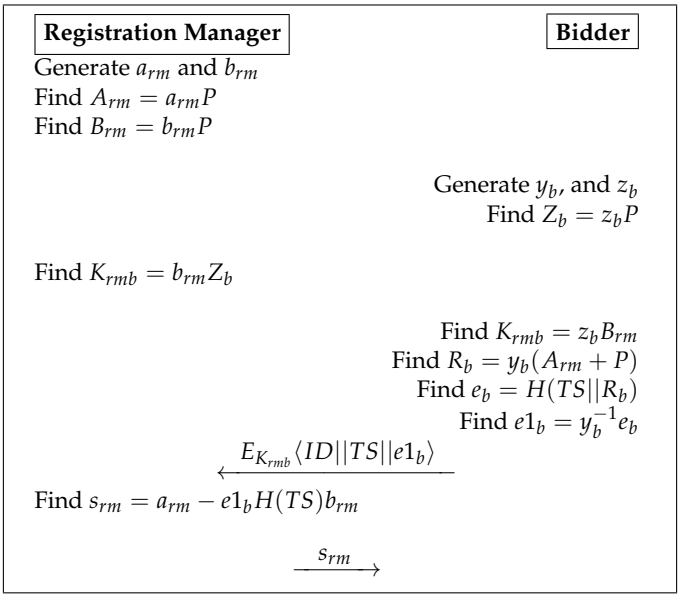

Figure 4. Schematic diagram of the registration phase of BSEA.

Algorithm 5 Registration Setup Phase

1: RM chooses his/her private keys as $a_{rm}, b_{rm} \in {Z_p}^*$.
2: She computes $A_{rm} = a_{rm}P$ and $B_{rm} = b_{rm}P$.
3: RM publishes his/her public key as $\langle A_{rm}, B_{rm} \rangle$.
4: Like step 1, here the Bidder chooses his/her private parameters as $y_b, z_b \in {Z_p}^*$.
5: She computes the following equation:

$$Z_b = z_b P, \tag{4}$$

and publishes $\langle Z_b \rangle$ as his/her public parameter.
6: RM computes K_{rmb} as

$$K_{rmb} = b_{rm} Z_b. \tag{5}$$

7: The Bidder also finds the same key K_{rmb} as

$$K_{rmb} = z_b B_{rm}. \tag{6}$$

8: She computes $R_b = y_b(A_{rm} + P)$, $e_b = H(TS||R_b)$, and $e1_b = y_b^{-1} e_b$.
9: Bidder encrypts the tuple $\langle ID||TS||e1_b \rangle$ using the secret key K_{rmb} and sends it to the RM.
10: RM decrypts the corresponding message using the same shared secret key K_{rmb} and computes s_{rm} as follows:

$$s_{rm} = a_{rm} - e1_b H(TS) b_{rm}. \tag{7}$$

11: RM signs the s_{rm} with b_{rm} as $\text{Sign}_{b_{rm}}(s_{rm})$ and sends it to the Bidder.

The steps of the registration confirmation phase are mentioned in Algorithm 6, and a pictorial representation of the same is shown in Figure 5. The Bidding phase consists of several steps as mentioned in Algorithm 7, and a pictorial representation of the same is shown in Figure 6. The steps of the winner determination phase are mentioned in Algorithm 8.

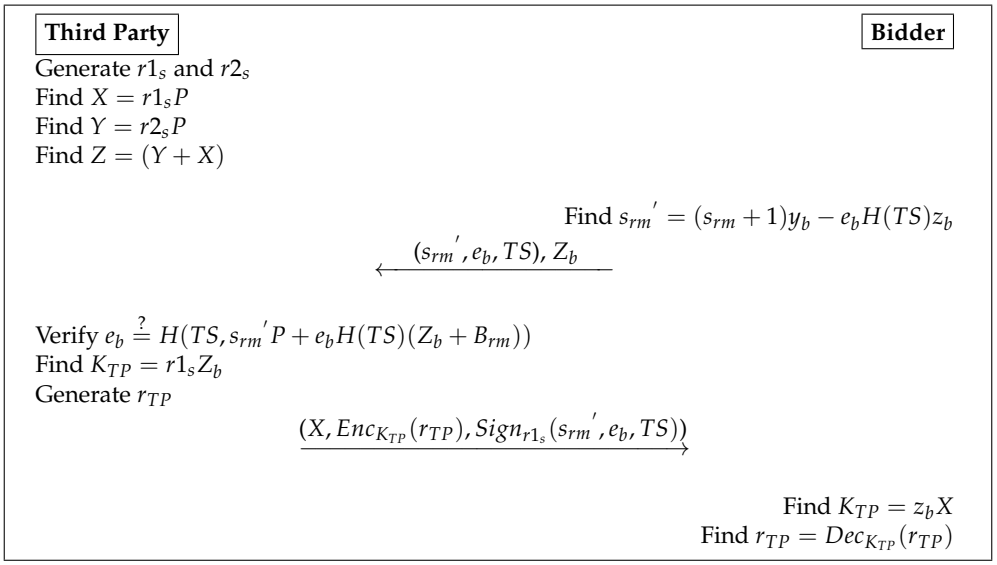

Figure 5. Schematic diagram of the Registration Confirmation Phase of BSEA.

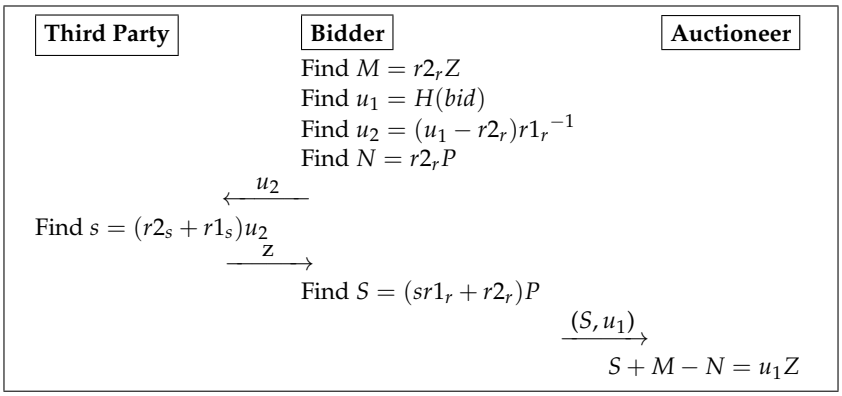

Figure 6. Schematic diagram of the Bidding Phase of BSEA.

Algorithm 6 Registration Confirmation Phase

1: The third party (TP) generates two random numbers $r1_s$ and $r2_s$. ▷ which act as his/her private keys such that $r1_s, r2_s \in Z_p{}^*$.
2: She computes $X = r1_s P$, $Y = r2_s P$, and $Z = (Y + X)$.
3: She publishes $\langle X, Y, Z \rangle$ as public parameters and keeps $r1_s$ and $r2_s$ secret.
4: The Bidder decrypts s_{rm} using K_{rmb} after receiving s_{rm} from the RM.
5: After decryption, the Bidder finds $s_{rm}{}'$ as per the following equation:

$$s_{rm}{}' = (s_{rm} + 1) y_b - e_b H(TS) z_b. \tag{8}$$

6: Now, the Bidder sends the tuple $(s_{rm}{}', e_b, TS)$ along with Z_b to the TP.
7: TP verifies the signature $s_{rm}{}'$ using the following equation:

$$e_b = H(TS, s_{rm}{}' P + e_b H(TS)(Z_b + B_{rm})). \tag{9}$$

8: If Equation (9) holds up well, then the TP finds a secret key K_{TP} according to the following equation:

$$K_{TP} = r1_s Z_b. \tag{10}$$

9: TP generates a random number r_{TP} and encrypts r_{TP} using K_{TP} as $\mathrm{Enc}_{K_{TP}}(r_{TP})$.
10: TP puts his/her signature on the tuple $(s_{rm}{}', e_b, TS)$ as $\mathrm{Sign}_{r1_s}(s_{rm}{}', e_b, TS)$.
11: TP sends the tuple $(X, Enc_{K_{TP}}(r_{TP}), Sign_{r1_s}(s_{rm}{}', e_b, TS))$ to the Bidder.
12: When the Bidder receives the tuple $(X, Enc_{K_{TP}}(r_{TP}), Sign_{r1_s}(s_{rm}{}', e_b, TS))$, she can find the value of K_{TP} using X.
13: Using K_{TP}, she finds the value of r_{TP}.

Algorithm 7 Bidding Phase

1: The Bidder generates two random numbers $r1_r$ and $r2_r$ such that $r1_r, r2_r \in {Z_p}^*$ ▷ where $r1_r$ is the blinding factor.
2: The Bidder computes his/her public key $M = r2_r Z$.
3: She computes $N = r2_r P$.
4: Using the blinding factor, she blinds his/her *bid* value.
5: She computes $u_1 = H(bid)$ and $u_2 = (u_1 - r2_r){r1_r}^{-1}$.
6: The Bidder sends u_2 to the TP to get his/her signature.
7: The TP finds the signature on the blind message corresponding to *bid* of the Bidder using the following equation:

$$s = (r2_s + r1_s)u_2. \tag{11}$$

▷ Here, the TP can not find anything about the *bid* value.
8: The TP sends the blind signature on the *bid* value s to the Bidder.
9: After receiving s from the TP, the Bidder unblinds the message s to get the signature on the original *bid* value. The Bidder can find this using the following equation:

$$S = (sr1_r + r2_r)P. \tag{12}$$

▷ The signed *bid* value by the TP is S.
10: The signature can be verified using the following equation:

$$S + M - N \stackrel{?}{=} u_1 Z. \tag{13}$$

▷ Here, without revealing the *bid* value, it can be verified.

Algorithm 8 Winner Determination Phase

1: Every Bidder sends their encrypted *bid* message to the TP along with the signed message S and the random number r_{TP} issued to him/her by the TP, encrypting with K_{TP}, which can be represented as $\mathrm{Enc}_{K_{TP}}(r_{TP}, bid, S)$.
2: After receiving the corresponding encrypted tuple from the Bidders, the TP decrypts the message using K_{TP} and checks the validity of the random number r_{TP} and retrieves *bid* and S.
3: The third party finds $H(bid) = u_1^{'}$ and verifies whether $S + M - N \stackrel{?}{=} u_1^{'} Z$ or not.
4: **if** the condition in step 3 is satisfied, **then**
5: She accepts the *bid* and finds *max_bid* among all of the Bidders.
6: The TP sends $\mathrm{Enc}_{K_{TP}}(max\_bid, Sign_{r1_s}(r_{TP}))$ to the corresponding Bidder and publishes the tuple (max_bid, S), so that it can be verified by anyone.
7: **end if**
8: The corresponding Bidder can claim himself/herself as the winner of the auction process.

6. Security and Requirement Analysis of BSEA

In this section, the security analysis of the proposed BSEA is performed by considering various attacks.

6.1. Correctness Proof

For correctness of BSEA, we have to check for the correctness of the blind signature and the registration done by the Bidder. Now, using Equation (7) in Equation (8), we will get,

$$s_{rm}{}' = ((a_{rm} - e1_b H(TS) b_{rm}) + 1) y_b - e_b H(TS) z_b.$$

Now, using the value of $e1_b$ in the above equation, it can be written as

$$\begin{aligned} & s_{rm}{}' = (a_{rm} + 1) y_b - y_b^{-1} e_b y_b H(TS) b_{rm} - e_b H(TS) z_b, \\ \Rightarrow\ & s_{rm}{}' = (a_{rm} + 1) y_b - e_b H(TS) b_{rm} - e_b H(TS) z_b, \\ \Rightarrow\ & s_{rm}{}' = (a_{rm} + 1) y_b - e_b H(TS)(b_{rm} + z_b). \end{aligned}$$

Using the above value of $s_{rm}{}'$ in right hand side (RHS) of Equation (9), we will get

$$\begin{aligned} & H(TS||s_{rm}{}' P + e_b H(TS)(Z_b + B_{rm})) \\ =\ & H(TS||((a_{rm} + 1) y_b - e_b H(TS)(b_{rm} + z_b)) P + e_b H(TS)(Z_b + B_{rm})). \end{aligned}$$

Using the values of b_{rm} and Z_b, we will get

$$\begin{aligned} & H(TS||(a_{rm} + 1) y_b - e_b H(TS)(b_{rm} + z_b) P + e_b H(TS)(Z_b + B_{rm})) \\ =\ & H(TS||(a_{rm} + 1) y_b - e_b H(TS)(b_{rm} + z_b) P + e_b H(TS)(z_b + b_{rm}) P) \\ =\ & H(TS||(a_{rm} + 1) y_b P - e_b H(TS)(b_{rm} + z_b) P + e_b H(TS)(b_{rm} + z_b) P) \\ =\ & H(TS||(a_{rm} + 1) y_b P). \end{aligned}$$

Using the value of R_b,

$$\begin{aligned} & R_b = y_b (A_{rm} + P), \\ \Rightarrow\ & R_b = y_b (a_{rm} P + P), \\ \Rightarrow\ & R_b = y_b (a_{rm} + 1) P. \end{aligned}$$

Using this value in the simplified version of RHS of Equation (9), we will get

$$\begin{aligned} & H(TS||(a_{rm} + 1) y_b P) \\ =\ & H(TS||R_b) \\ =\ & e_b. \end{aligned}$$

e_b is in the LHS of Equation (9). Hence, the correctness of the registration of the Bidder is proved.

6.2. Security Analysis

The security of the proposed BSEA depends on the strength of the secure hash function $H(.)$ and the crypto-graphically computational hard problem ECDLP. Here, some of the attacks that can be withstood by BSEA have been discussed.

1. **Key only attack:** In order to successfully launch a key only attack, the attacker needs to get a valid signature. Even if she gets a valid signature, then she is also unable to unblind the signature, as she does not know the blinding factor and the private key of the Bidder (i.e., $r1_r$ and $r2_r$). The difficulty of finding $r2_r$ depends on the difficulty of ECDLP and finding the value of $r1_r$ depends on the difficulty of solving IFP.
2. **Known message attack:** In the known message attack, the attacker generates a valid signature for his own message bid'. Here, she has access to two or more message-signature pairs like (S', u_1')

and $(S^{''}, u_1^{''})$. Here, the attacker can generate another signature $S^{'''} = S^{'} + S^{''}$ for message *bid*, if she can find $H(bid) = H(bid^{'}) + H(bid^{''})$. This is very difficult if the hash function is preimage resistant. Moreover, she also needs to find the value of u_2 for which she has to find $r1_r$ and $r2_r$.

3. **Chosen message attack:** In case of chosen message attack, the attacker can make the TP to sign for two *bid* messages, $bid^{'}$ and $bid^{''}$. Then, she can calculate a new signature $S^{'''} = S^{'} + S^{''}$. If the attacker can find $H(bid) = H(bid^{'}) + H(bid^{''})$ and the blind message u_2 for his/her message *bid*, then she can do a chosen message attack on BSEA. However, it is very difficult to find the hash value of a message *bid* that is the same as the hash value of the given messages $bid^{'}$ and $bid^{''}$.
4. **Forgery attack:** Given X and P, finding $r1_s$ is difficult due to the difficulty in solving the ECDLP problem. Hence, the private key of the TP can never be guessed correctly. It will be difficult for the attacker to unblind the message because $r1_r$ and $r2_r$ are the private components of the Bidder.
5. **Replay attack:** An attacker cannot retrieve the *id* of the Bidder as the message sent to the RM is encrypted with the session key K_{rmb}. She would not be able to find either $e1_b$ or s_{rm}. Similarly, due to the session key K_{TP} that is only with the Bidder and the TP, the attacker would not be able to find the random number r_{TP}.
6. **Eavesdropping attack:** Even if the attacker wants to eavesdrop on the communication between any Bidder and the RM or the TP, she will not get enough advantage. The reason for this is that the data that flows are encrypted with the session keys K_{rmb} and K_{TP} and are also being signed by the respective entities.
7. **Identity theft attack:** In the proposed BSEA, the Bidder's *id* is not used for authentication. Instead, timestamp (TS) is being used for authentication, which prevents the Bidder from the risk of identity theft. In addition to this, the random number r_{TP} provided by the TP is only known to them. However, in case the TP is corrupted, she may reveal the random number r_{TP}, but the real identity of the Bidder is still concealed.
8. **Impersonate attack:** It is impossible to impersonate either the Bidder or the RM or the TP because all have used either their session key to encrypt the messages or the private keys to sign the messages.

As BSEA is resistant to the above mentioned attacks, BSEA is secure.

6.3. Requirement Analysis

Here, we have analyzed all the requirements those need to be fulfilled by e-auction protocols. By this, we want to show that BSEA also satisfies the requirements of e-auction protocols.

1. **Anonymity:** The information about every Bidder must be hidden from other Bidders. The TP will authenticate the Bidders and will assign a random number to each of them. Every Bidder blinds their *bid* value and sends to the TP to get his/her signature. Thus, all the information about the Bidder, including his/her *bid* value, is hidden from everyone until the auction process is closed. In the winner determination phase, the Bidder sends his/her *bid* value only to the TP to determine the *max_bid*. Thus, anonymity is preserved for all the Bidders even if the TP is corrupted.
2. **Un-forgeability:** Any attempt by the attacker to forge bid value will fail as she can not find u_2. For this, she has to find $r1_r$ and $r2_r$, and, for this, she has to solve ECDLP. Moreover, all the necessary information is encrypted with the session key and/or signed by the Sender. Hence, forgery attack is not possible.
3. **Non-Repudiation:** The Bidder as well as the TP must not be able to deny the act that they have done during the execution of the phases of BSEA. The Bidder cannot deny casting the *bid* because the signed *bid* value S can be verified using Equation (13), where M is the public key of the Bidder. Similarly, the TP can not deny receiving the *bid*, as the same signature is also verified by using his public key Z.
4. **Public Verifiability:** The signature S can be verified by everyone after publishing the signature parameter (S, u_1). Moreover, the final winner's *bid* can also be verified by everyone once the

TP publishes the tuple (S, max_bid). As anyone can now find $u_1 = H(max\_bid)$ and verify the signature S. The authenticity of every Bidder can also be verified by everyone.

5. **Traceability:** The winning Bidder or any other Bidder who does not follow the auction rule can be identifiable because the proposed BSEA is traceable (the explanation is given in Section 4.3).
6. **Fairness and Robustness:** BSEA satisfies the fairness property because even if the malicious Bidder or Auctioneer colludes with the TP, they will not gain any information about the honest Bidder, which can harm him/her in the running auction process or any future auction process.
7. **Privacy:** BSEA maintains the privacy of every Bidder during the auction process. It also preserves the privacy of the losing Bidder even after the winner determination phase is over.
8. **Integrity and Confidentiality:** The integrity and confidentiality of BSEA are achieved through blind signature and the session key. No one can find the *bid* value before the winner determination phase is over due to the blindness property of the proposed BSEA. No one can change the *bid* value once signed by the TP because, even if it is modified, it cannot be verified by Equation (13).

In Table 2, we have compared the requirement evaluation results of BSEA with some of the previously proposed e-auction schemes. Here, R_i represents the requirement number mentioned above. Our scheme satisfies all the requirements, which are needed for an electronic auction.

Table 2. Comparison for analysis of requirements.

	R_1	R_2	R_3	R_4	R_5	R_6	R_7	R_8
Liaw et al. [37]	√	√	×	√	√	×	×	√
Wu et al. [38]	√	√	√	√	√	√	×	√
Cao et al. [39]	√	√	√	√	×	√	×	√
Ksiezopolski et al. [41]	√	√	√	√	√	×	×	√
Cao [40]	√	√	√	√	×	√	√	√
BSEA	√	√	√	√	√	√	√	√

7. Performance Analysis of BSEA

As per Table 2, the proposed BSEA protocol fulfills all the requirements needed to be satisfied by an e-auction protocol. Moreover, it saves a considerable amount of space in terms of key size as it is implemented using ECC. The performance of BSEA is discussed in terms of computational overhead by comparing it with the some of the popular existing schemes. The performance comparison results of BSEA are shown in Table 3 in comparison to Liaw et al. [37], Wu et al. [38] and Cao et al. [39].

Table 3. Comparison for total computational overhead.

Schemes/Phases	Advertisement	Registration	Bidding	Winner Determination
Liaw et al. [37]	nT_e	$2nT_e + 5nT_h$	$5nT_e$	$T_e + T_h$
Wu et al. [38]	$nT_e + nT_h$	$2nT_e + 2nT_s + 3nT_h$	$nT_e + 4nT_e$	$nT_e + nT_e + 2nT_s$
Cao et al. [39]	$2T_m + T_e$	$3nT_e + nT_m + 2nT_s + 5nT_h$	$2nT_e$	nT_e
BSEA	$T_e + T_h$	$2nT_m + 2nT_e + 2nT_s + 5nT_h$	$4nT_m + nT_h$	$nT_m + 4nT_s + nT_h$

n : Number of *bid*s in the auction process, T_e : Time to compute exponential operation, T_s : Time to compute symmetric key encryption, T_h : Time to compute one-way hash operation, T_m : Time to compute scalar multiplication operation.

To verify the efficiency of BSEA in terms of time, we implemented Liaw et al. [37], Wu et al. [38], Cao et al. [39] and BSEA using the pairing based cryptography (PBC) library [42] with *type A* pairing from the PBC archive. We used SHA-1 as the hash function. Figure 7 shows the average computation time consumed by the schemes. Results show that our proposed scheme BSEA outperforms the existing schemes like Liaw et al. [37], Wu et al. [38] and Cao et al. [39]. Moreover, it saves a considerable amount of space in terms of key size, as it is implemented using ECC. Hence, the proposed scheme is efficient.

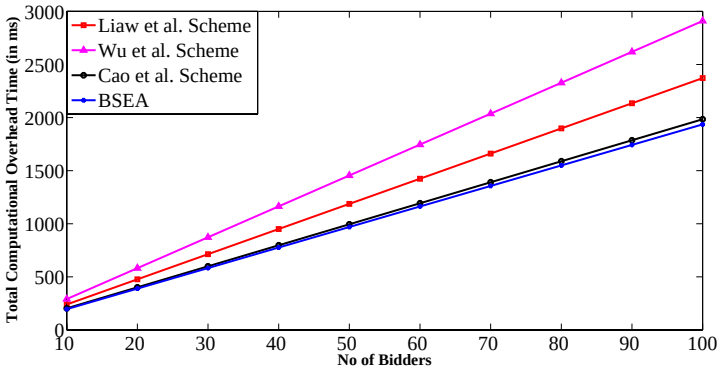

Figure 7. Computation overhead comparision.

8. Conclusions

In this paper, we have proposed an electronic auction scheme using a blind signature protocol. We first proposed a blind signature protocol according to the requirements of the e-auction (CTBSS) and then employ it to design a sealed-bid electronic auction scheme (BSEA). Both protocols are based on elliptic curve cryptography. Moreover, an ECC based protocol is more efficient in terms of space in comparison to its counterparts, which are based on DLP. The proposed BSEA fulfills all the requirements of the e-auction protocol, and the computation overhead is low as compared to the existing schemes. The efficiency of BSEA can be further improved using very-large-scale integration (VLSI) implementation.

Acknowledgments: We want to thank the Department of Computer Science and Engineering of the National Institute of Technology, Rourkela, India for providing infrastructure to conduct the experiments. We did not receive any funds for covering the costs to publish in open access.

Author Contributions: Rohit Kumar Das, Sanjeet Kumar Nayak, Banshidhar Majhi and Sujata Mohanty found the problem and designed the CTBSS and BSEA schemes. Sourav Kumar Bhoi and Suman Kumar Choudhury analyzed the security aspects of the proposed schemes. Rohit Kumar Das and Sanjeet Kumar Nayak conducted the experiments to evaluate the performance of the proposed schemes. Rohit Kumar Das analyzed the requirement aspects of the BSEA scheme and wrote the paper. Banshidhar Majhi and Sujata Mohanty guided the work. All authors have read and approved the final manuscript.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

BSEA	blind sealed-bid electronic auction
CTBSS	controlled traceable blind signature scheme
DLP	discrete logarithm problem
ECC	elliptic curve cryptography
ECDLP	elliptic curve discrete logarithm problem

References

1. Omote, K. A Study on Electronic Auctions. Ph.D. Thesis, Japan Advanced Institute of Science and Technology, Nomi, Japan, 2002.
2. Kleusberg, P. *E-Collaboration und E-Reverse Auctions: Sicherung von Wettbewerbsvorteilen im Verarbeitenden Gewerbe*; VDM Publishing: Saarbrucken, Germany, 2009. (In German)
3. Engelbrecht-Wiggans, R.; Katok, E. E-sourcing in Procurement: Theory and Behavior in Reverse Auctions with Noncompetitive Contracts. *Manag. Sci.* **2006**, *52*, 581–596.
4. Chang, Y.F.; Chang, C.C. Enhanced anonymous auction protocols with freewheeling bids. In Proceedings of the 20th International Conference on Advanced Information Networking and Applications, Vienna, Austria, 18–20 April 2006; Volume 1, pp. 6–11.

5. Vickrey, W. Counterspeculation, auctions, and competitive sealed tenders. *J. Financ.* **1961**, *16*, 8–37.
6. Liu, Y. A new secure and efficient M+1st price auction scheme based on ECC system. In Proceedings of the 3rd International Conference on Anti-counterfeiting, Security, and Identification in Communication, Hong Kong, China, 20–22 August 2009; pp. 489–492.
7. Lee, B.; Kim, K.; Ma, J. Efficient Public Auction with One-Time Registration and Public Verifiability. In *Progress in Cryptology—INDOCRYPT 2001*; Rangan, C., Ding, C., Eds.; Springer: Berlin/Heidelberg, Germany, 2001; Volume 2247, pp. 162–174.
8. Chaum, D. Blind Signatures for Untraceable Payments. In Proceedings of the CRYPTO '82 Advances in Cryptology, Santa Barbara, CA, USA, 23–25 August 1982; pp. 199–203.
9. Castiglione, A.; Palmieri, F.; Chen, C.L.; Chang, Y.C. A Blind Signature-Based Approach for Cross-Domain Authentication in the Cloud Environment. *Int. J. Data Warehous. Min.* **2016**, *12*, 34–48.
10. Tian, H.; Zhang, F.; Wei, B. A lattice-based partially blind signature. *Secur. Commun. Netw.* **2016**, *9*, 1820–1828.
11. Zou, X.; Qiu, D. Attack and improvements of fair quantum blind signature schemes. *Quantum Inf. Process.* **2013**, *12*, 2071–2085.
12. Nayak, S.K. Blind Signature Schemes using Elliptic Curve Cryptography. Ph.D. Thesis, National Institute of Technology, Rourkela, India, 2013.
13. Shao, Z. Improved User Efficient Blind Signatures. *Electron. Lett.* **2000**, *36*, 1372–1374.
14. Yum, D.H.; Lee, P.J. Generic Construction of Certificateless Signature. In *Information Security and Privacy*; Wang, H., Pieprzyk, J., Varadharajan, V., Eds.; Springer: Berlin/Heidelberg, Germany, 2004; Volume 3108, pp. 200–211.
15. Nayak, S.K.; Mohanty, S.; Majhi, B. CLB-ECC: Certificateless Blind Signature Using ECC. *J. Inf. Process. Syst.* **2014**, doi:10.3745/JIPS.03.0029.
16. Islam, S.; Obaidat, M.S. Design of provably secure and efficient certificateless blind signature scheme using bilinear pairing. *Secur. Commun. Netw.* **2015**, *8*, 4319–4332.
17. Jiang, S.; Zhu, X.; Guo, L.; Liu, J.; Hao, R.; Yang, B. Efficient private matching based on blind signature for proximity-based mobile social networks. In Proceedings of the 2015 IEEE International Conference on Communications (ICC), London, UK, 8–12 June 2015; pp. 3246–3251.
18. Shi, J.; Shi, R.; Guo, Y.; Peng, X.; Tang, Y. Batch proxy quantum blind signature scheme. *Sci. China Inf. Sci.* **2013**, *56*, 1–9.
19. Liu, J.; Zhang, Z.; Sun, R.; Kwak, K.S. Certificateless partially blind signature. In Proceedings of the 26th International Conference on Advanced Information Networking and Applications Workshops (WAINA), Fukuoka, Japan, 26–29 March 2012; pp. 128–133.
20. Nayak, S. K.; Majhi, B.; Mohanty, S. An ECDLP based untraceable blind signature scheme. In Proceedings of the 2nd IEEE International Conference on Circuits, Power and Computing Technologies (ICCPCT), Nagercoil, India, 20–21 March 2013; pp. 829–834.
21. Tahat, N.; Abdallah, E.E. A proxy partially blind signature approach using elliptic curve cryptosystem. *Int. J. Math. Oper. Res.* **2016**, *8*, 87–95.
22. Alam, K.; Alam, K.R.; Faruq, O.; Morimoto, Y. A comparison between RSA and ElGamal based untraceable blind signature schemes. In Proceedings of the 2016 International Conference on Networking Systems and Security (NSysS), Dhaka, Bangladesh, 7–9 January 2016; pp. 1–4.
23. Dahshan, H.; Kamal, A.; Rohiem, A. A Threshold Blind Digital Signature Scheme Using Elliptic Curve Dlog-Based Cryptosystem. In Proceedings of the 2015 IEEE 81st Vehicular Technology Conference (VTC Spring), Glasgow, UK, 11–14 May 2015; pp. 1–5.
24. Miller, V.S. Use of Elliptic Curves in Cryptography. In *Advances in Cryptology— CRYPTO '85*; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 1986; Volume 218, pp. 417–426.
25. Chaudhry, S.A.; Farash, M.S.; Naqvi, H.; Sher, M. A secure and efficient authenticated encryption for electronic payment systems using elliptic curve cryptography. *Electron. Commer.Res.* **2015**, *16*, 113–139.
26. Chen, Y.; Chou, J.S. ECC-based untraceable authentication for large-scale active-tag RFID systems. *Electron. Commer. Res.* **2015**, *15*, 97–120.
27. Lopez, J.; Dahab, R. An Overview of Elliptic Curve Cryptography. Available online: http:// citeseerx. ist.psu.edu/viewdoc/download?doi=10.1.1.37.2771&rep=rep1&type=pdf (accessed on 13 December 2016).

28. Wang, T.Y.; Wei, Z.L. Analysis of Forgery Attack on One-Time Proxy Signature and the Improvement. *Int. J. Theor. Phys.* **2016**, *55*, 743–745.
29. Cheng, L.; Wen, Q. Cryptanalysis and improvement of a certificateless partially blind signature. *Inf. Secur. IET* **2015**, *9*, 380–386.
30. Zhang, K.J.; Jia, H.Y. Cryptanalysis of a quantum proxy weak blind signature scheme. *Int. J. Theor. Phys.* **2015**, *54*, 582–588.
31. Das, R.K. Development of an ECDLP based Traceable Blind Signature Scheme and its Application to E-Auction. Ph.D. Thesis, National Institute of Technology, Rourkela, India, 2014.
32. Franklin, M.K.; Reiter, M.K. The design and implementation of a secure auction service. *IEEE Trans. Softw. Eng.* **1996**, *22*, 302–312.
33. Kudo, M. Secure electronic sealed-bid auction protocol with public key cryptography. *IEICE Trans. Fundam.* **1998**, *81*, 20–27.
34. Kikuchi, H.; Hakavy, M.; Tygar, D. Multi-round anonymous auction protocols. *IEICE Trans. Inf. Syst.* **1999**, *82*, 769–777.
35. Chang, C.C.; Chang, Y.F. Efficient anonymous auction protocols with freewheeling bids. *Comput. Secur.* **2003**, *22*, 728–734.
36. Jiang, R.; Pan, L.; Li, J.H. An improvement on efficient anonymous auction protocols. *Comput. Secur.* **2005**, *24*, 169–174.
37. Liaw, H.T.; Juang, W.S.; Lin, C.K. An electronic online bidding auction protocol with both security and efficiency. *Appl. Math. Comput.* **2006**, *174*, 1487–1497.
38. Wu, C.C.; Chang, C.C.; Lin, I.C. New Sealed-Bid Electronic Auction with Fairness, Security and Efficiency. *J. Comput. Sci. Technol.* **2008**, *23*, 253–264.
39. Cao, G.; Chen, J. Practical Electronic Auction Scheme Based on Untrusted Third-Party. In Proceedings of the 2013 Fifth International Conference on Computational and Information Sciences (ICCIS), Shiyan, China, 21–23 June 2013; pp. 493–496.
40. Cao, G. Secure and efficient electronic auction scheme with strong anonymity. *J. Netw.* **2014**, *9*, 2189–2194.
41. Ksikezopolski, B.; Kotulski, Z. Cryptographic protocol for electronic auctions with extended requirements. *Ann. UMCS Sect. AI Inf.* **2015**, *2*, 391–400.
42. Lynn, B. The Pairing-Based Cryptography Library. Available online: https://crypto.stanford.edu/pbc/ (accessed on 27 March 2013).