A taxonomy of secure electronic English auction protocols

Abubaker Wahaballa, Zhen Qin, Hu Xiong, Zhiguang Qin & Mohammed Ramadan

A taxonomy of secure electronic English auction protocols

Abubaker Wahaballa[a,b], Zhen Qin[a], Hu Xiong[a], Zhiguang Qin[a] and Mohammed Ramadan[a]

[a]School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu, P.R. China; [b]National Council of Technical and Technological Education, Khartoum, Sudan

ABSTRACT

In this paper, a taxonomy of secure electronic English auction protocols that are widely used in online Internet auctions is outlined. Firstly, these schemes are classified into three classes according to their design philosophy: group-oriented signature-based protocols, trusted third party-based protocols, and pseudonym identity-based protocols. Secondly, the pros and cons of these schemes are identified and compared in light of different viewpoints. Thirdly, we analyzed the performance of these protocols, and we proposed new directions based on the insightful analysis of the existing work. This paper can be a roadmap for beginners in understanding the basic concepts of security issues, properties, and performance in electronic English auction scheme.

KEYWORDS

Secure English electronic auction protocol; taxonomy; conditional anonymous authentication

1. Introduction

As one of the important components of electronic commerce, electronic auction (E-Auction) protocols provide a very competitive way to sell a variety of goods and services conveniently and have received a lot of attention recently. [1] E-Auction protocols can be classified according to the mechanism of bidding [2,3] into four main types: English auction, Dutch auction, first-price sealed-bid auction, and Vickrey auction. Also e-marketplace is open for other e-auction types, such as Japanese auction, Penny auction, reserve auction, $(M+1)$ and st-price auction.[4]

Among the existing E-Auction protocols, the English auction is regarded as the most commonly known type. In the electronic English auction, two kinds of participants, namely bidder and auctioneer, will be involved such that the auctioneer will announce the information of the products under the hammer, receive the bids submitted by the bidder, and publish the highest bid as the winning price. There are four main stages [5] in an online English auction:

(1) **Initialization**: The auctioneer sets up the auction and advertises it, i.e. type of goods being auctioned, starting time, etc.
(2) **Registration**: In order to participate in the auction, bidders must first register with the auctioneer.
(3) **Bidding**: A registered bidder computes his/her bid and submits it to the auctioneer. The auctioneer checks the bid received to ensure that it conforms to the auction rules.
(3) **Winner Determination**: The auctioneer determines the winner from the participating bidders according to the auction rules. The rules that determine the termination of an Online English auction are the following:
(a) *Expiration Time*: The auction closes at a predetermined expiration time.
(b) *Timeout*: The auction closes when no bids higher than the current highest bid are made within a predetermined timeout interval.
(c) *Combination of Expiration and Timeout*: The auction closes when there is a timeout after the expiration time.

Figure 1 describes the combinatorial auction market design process with three phases framework. To design an auction market, a market architecture and auction rules should be specified. According to the auction rules, the auction process proceeds step by step. Another important thing in designing an auction market is winner determination for bid selection and auctioneer selection.

1.1. Motivation

Security and privacy should be considered in every kind of online transactions and will result in the corresponding challenges when these electronic transactions have been applied in practice. The security requirements in an electronic auction system are even more challenging because the technology for e-commerce is rapidly developing and has become more complex and widespread.

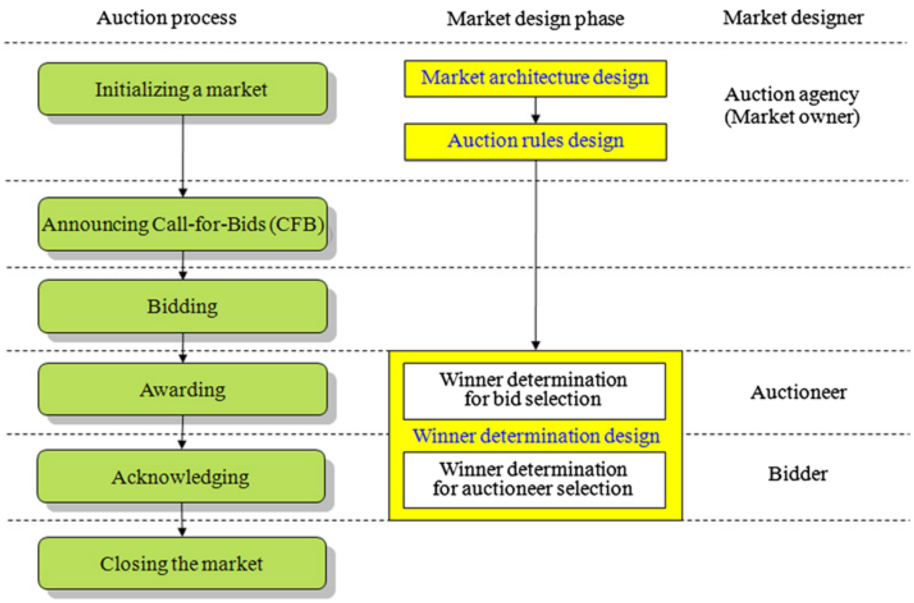
Auction process
Market design phase
Market designer
Initializing a market
Market architecture design
Auction rules design
Auction agency (Market owner)
Announcing Call-for-Bids (CFB)
Bidding
Awarding
Winner determination for bid selection
Winner determination design
Winner determination for auctioneer selection
Auctioneer
Acknowledging
Bidder
Closing the market

Figure 1. The combinatorial auction market design process.[6]

The main aims of this paper are twofold:

(1) To present a comprehensive survey of secure electronic English auction protocols in order to confirm how these protocols meet the security requirements.

(2) To check whether the improvement on the dependability and efficiency of these protocols will influence the security or not.These findings will be of interest to the research community as it will ensure auction houses maintain control, giving bidders the opportunity to participate anonymously and also allow all bids to be fairly dealt with.

This article can also be a roadmap for beginners in understanding the basic concepts of security issues, properties, and performance of the English auction protocols.

1.2. Security issues in online English auctions

Online auctioning is regarded as the fastest growing exchange medium that has emerged from e-commerce technology with millions of people logging on to buy and sell a vast array of products. The best known auction sites are eBay, uBid, and Yahoo! in America, Taobao in china, and QXl in Europe. Unfortunately, these sites encounter many threats, frauds, and risks.[7] Furthermore, online auctions have the largest percentage frauds among other e-commerce applications, and almost close to the other dangerous online frauds, which are shown in Figure 2.

Protecting privacy on e-auction is vital to defend the auction against fraudsters, malicious bidders, and auctioneers. The *conditional anonymous authentication* protocol is a solution to this problem. The conditional anonymous authentication protocol works on top of an anonymous routing method that guarantees both user anonymity and unlinkability, that allows the server to authenticate the user, to prove that s/he is an authorized user.[8,9] The importance of conditional anonymous authentication in an auction system are:

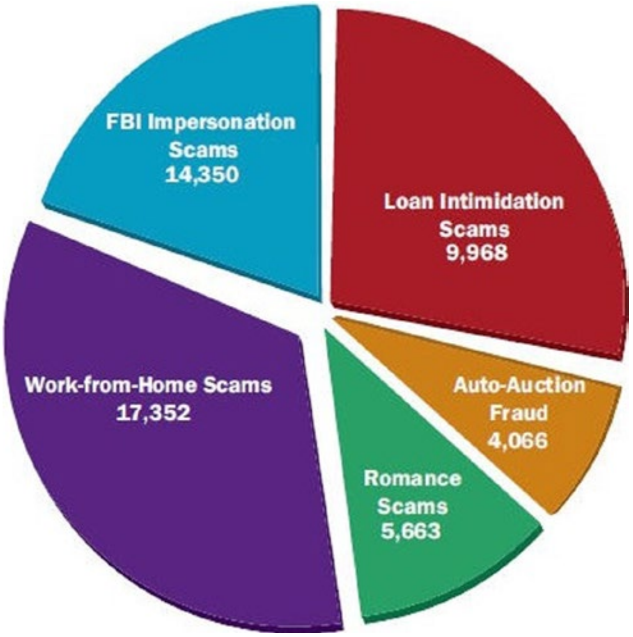

Figure 2. Online major fraud types reported by FBI in 2011.

(1) To authenticate the identity of user;

(2) To protect the privacy of bidder's personal information;

(3) To trace the actual identity of the malicious bidders and auctioneers in case of dispute.

According to pervious researchers [10–15], the security requirements of English auction are summarized as follows:

- **Unforgeability**: Bids must be unforgeable, otherwise the bids cannot be trusted.
- **Verifiability**: There must be publicly available information by which all parties can verify as having

correctly followed the auction protocol. This should include evidence of registration, bidding, and proof of the winner of the auction.

- **Non-repudiation**: No bidding winners should be able to deny their bid price after the auction close. Similarly, auctioneers should be unable to repudiate the origin of the corresponding products that they uploaded to the agent center.
- **Fairness**: Regardless of whether in a traditional or electronic auction, fairness is always considered an important requirement for ensuring the integrity and correctness of the auction process. All bidders should verify whether their own bids have been correctly included in the auction.
- **Anonymity**: The relationship between the bidder and corresponding bid must be concealed so that no bidder can be associated or identified with the bid they submit.
- **One-time registration**: Registration is a one-off procedure, which means that once a bidder has registered, they can participate in future auctions held by the auctioneer.
- **Unlinkability**: Bids within one auction or plural auctions should be unlinkable.
- **Traceability**: Once a bidder has submitted a bid, s/he should not be able to repudiate it. Otherwise if a bidder wins and does not want to pay, s/he might deny that s/he submitted the winning bid. In this case, the identity of the targeted bidder who submitted the bid in question can be revealed.
- **Revocation**: Malicious bidders can be easily revoked from all future auctions.

The paper is organized as follows: In the next section, we give a survey of the literature on English e-auction protocols. Security properties and performance are analyzed in Section 3. In Section 4, we give some proposals of new research directions. We finally conclude the paper in Section 5.

2. A survey of the literature

During the last decades, many secure English E-auction schemes have been suggested in order to improve their efficiency and security levels. In this section, we review briefly of these schemes. Specifically, these schemes are classified into three classes according to their design philosophy as follows:

2.1. Group-oriented signature-based protocols

A group signature scheme is a method introduced by Chaum and van Heyst [16], which allows any member of a group to sign on behalf of the group and keeps their identity secret. In other hands, it allows any member of a group to digitally sign a document such that a verifier can confirm that it came from the group but does not know which individual in the group signed the document. However, the identity of the signer will be disclosed in case of dispute.

Chang et al. [17] in the 2003 proposed auction scheme, which enhances the anonymity with freewheeling bids. However, they are many handshaking transmission processes in the session key leading to increase in the computational and the communication cost, thereby making the system inefficient. In order to reduce the communication cost, Chang et al. [18] proposed an efficient anonymous auction protocol which is called C-C protocol. In C-C protocol, the efficiency is enhanced significantly by decreasing the number of communication rounds from 4 to 3. However, in the initiation phase of the C-C protocol, there is no mechanism to protect the bidder's identity, obviously. In order to improve the above mentioned matter, Yang et al. [13] proposed an efficient anonymous auction protocol to protect all bidders' identities in both initiation and auction phases with low levels of computation and communication. However, their scheme does not satisfy some security requirements such as: unforgeability, one-time registration, and unlinkability.

In 2012, Xiong et al. [10] proposed an efficient and conditional privacy preserving English auction protocol; the advantages of this scheme are enhanced computational efficiency and the provision of a dispute protocol for the first time. However, this protocol is not like a real e-auction system such as Yahoo!, eBay, and uBid.[19–21] A user in these systems can be a bidder, or an auctioneer. Moreover, Chang et al. [11] discovered two problems with this scheme in the dispute phase. Firstly, auction manager (AM) needs to repeat the bilinear operation many times until it finds the corresponding public key (PKi) which is the malicious bidder's public key. Such a process is inefficient. Secondly, a further pitfall of this protocol is that an attacker can frame a request to delete a user account in this auction system, and in order to solve this problem, they proposed an English auction scheme with a secure on-shelf mechanism.

2.2. Trusted third party-based protocols

A trusted third party (TTP) in cryptography is an entity that facilitates the interaction between two parties that both trust the TTP.[22] TTPs are common in a number of commercial transactions, cryptography digital transactions as well as in some cryptographic protocols. For example, a certificate authority (CA) would issue a digital identity certificate to each of the two parties in order to initiate interactions between them.[23]

In 2008, Chung et al. [24] proposed anonymous English auction scheme with privacy and public verifiability; this scheme has three entities, which are the registration manager, the AM, and the bidder, and these entities work on seven stages: initialization, bidder registration, auction key generation, auction setup, bidding, verification, and winning-bidder announcement. The advantages of this scheme are (i) it satisfies the security requirements of the English auction scheme. (ii) The scheme is consistent with the actual practice of online transactions. However, the computational and communication costs significantly increased in this scheme, as shown in Table 3.

In 2011, Li et al. [9] proposed a scheme with strong anonymity and privacy bidding, and this scheme can be applied to multiple auction types. Since this survey focuses solely on English auctions, we have omitted discussions of other non-English types. In an English auction, this scheme has four entities: registration manager (RM), an auction manager (AM), a bidder (B), and an auctioneer (A). The idea of two mangers in this scheme was borrowed from Omote and Miyaji [25,27]; this idea preserves the anonymity of bidders in a resilient manner, by dispersing the power between the AM and RM. Furthermore, there is a cooperation between AM and RM in order to determine the winner; however, when we compare this scheme with an actual e-auction system (Yahoo!, eBay, and uBid), it was found that most of the power is possessed by the auction agent, the users can merely register as a bidder or auctioneer. Moreover, the security analysis of this work only took into consideration three types of attacks: replay attacks, man-in-the-middle attacks, and forgery attacks. These security measures are not enough to ensure that the scheme is secure, for example, a denial of service (DoS) attack may be achieved in this scheme. However, in the registration phase, the author uses a Diffie–Hellman (DH) exchange protocol; however, this protocol is vulnerable to a 'man-in the-middle' attack, and also the author bound the exchange key to users' identities in the registration phase, thereby binding all subsequent steps. If an adversary is aware of the ID, then the DH parameters are open to attack making the key vulnerable, or at the very least, the connection may be rejected. These vulnerabilities can affect the decision of the winner; in general, this scheme is not fully compatible with the auction systems.

Recently, Chang et al. [11] proposed an English auction scheme with a secure on-shelf mechanism. This scheme works in five phases, three phases are familiar to most schemes, and they are: registration, bidding, and product claiming phase (winner determination). The other two phases actually represent an additional contribution to auction security schemes and these are: the on-shelf, and dispute phases. This work is represented by an AES algorithm with ECC. The ECC technique provides a low power, low bandwidth, and good security especially for keys. However, there are many handshaking transmission processes within this scheme, especially in the on-shelf phase, it makes the system increasingly complex, as well as increases the computational cost, bandwidth, and power consumption. On the other hand, the scheme proposed by Chang et al. used ECC to provide the above features; however, the handshaking negotiation process causes the same problem.

2.3. *Pseudonym-based protocols*

A pseudonym is a name that a person or group assumes for a particular purpose, which differs from his or her original or true name. Pseudonym systems were introduced by Chaum [28] in 1985 as a way of allowing a user to work effectively, but anonymously, with multiple organizations.

In 2001 and 2002, Omote and Miyaji [25,26] proposed an English auction scheme without using a group signature based on pseudonym on bulletin boards which realize both anonymity and traceability of bidders. However, their scheme does not satisfy some security requirements such as the information compromises privacy, including anonymity, fairness, and non-linkability on auction life cycle in all rounds.

In 2009, Chung et al. [29] proposed using an elliptic curve cryptosystem in Huang's [30] mobile auction agent model (MoAAM). This scheme has four entities and they are: registration manager, agent house, auctioneer, and bidder and these entities work in six phases which are: initialization, registration, transaction public key generation, signature, auction bidding, and winner announcement. The advantages of this work are lowering the computational cost of mobile devices and the provision of a small key. However, Nikooghadam et al. [31] proved the insecurity of this scheme against 'man-in-the-middle' attack, anyone having access to the agent can easily replace the original public parameters by the forged ones.

3. Security requirements and performance analysis

In this section, we will compare the pervious literature to identify whether these protocols satisfy security requirements and resistance attacks or not in the form of tables. In Table 1, we show the comparison of participants and resistant attacks in the English E-Auction protocols, while Table 2 highlights the comparisons of the security requirements. Furthermore, the efficiency of these schemes against one another is compared in Table 3. For convenience, we define the following notations: T_x (time complexity of exponentiation operation); T_m (time complexity of modules multiplication operation); T_i (time complexity of inverse operation); T_H (time complexity of one-way hash function); T_p (time complexity of pairing operation); T_Z (time complexity of Zero knowledge proof operation); T_E (time complexity of encryption operation); T_D (time complexity of decryption operation); T_σ (time complexity of signature operation); T_v (time complexity

Table 1. Comparison of participants and resistant attacks in English E-Auction protocols.

Design philosophy	English auction protocol	Participants	Authority center	Resistance to impersonation attacks	Resistance to (DoS) attack	Resistance to man-in-middle attack
Group-oriented signature-based protocols	[17]	3 system participants (CA, B, A)	✓	×	×	✓
	[18]	3 system participants (CA, B, A)	✓	✓	×	✓
	[13]	2 system participants (B, A)	×	✓	×	✓
	[10]	3 system participants (RM, AM, B)	✓	✓	×	✓
Trusted third party-based protocols	[24]	3 system participants (RM, AM, B)	✓	✓	✓	✓
	[9]	4 system participants (RM, AM, B, A)	✓	✓	×	×
	[11]	2 system participants (AC, A, B)	✓	✓	✓	✓
Pseudonym-based protocols	[25,26]	3 system participants (RM, AM, B)	✓	✓	×	✓
	[29]	4 system participants (RM, AH, B, A)	✓	✓	×	×

of verifying operation); n (number of users); B (bidder); A (auctioneer); CA (certificate authority); RM (register manager); AC (agent center); AM (auction manager); AH (agent house).

From the security requirements and resistance attacks, comparisons outlined , we found that [11] and [24], kinds of TTP-based protocol satisfy all security requirements of the electronic English auction as identified in Section 1.2. Furthermore, these protocols resist all attacks (e.g. man-in- the-middle, impersonation attacks, and denial-of-service attack).

To preserve strong anonymity for the bidders, some of English E-Auction protocols have two managers: the RM and the AM. This idea disperses the power between the AM and RM. Furthermore, there is a cooperation between AM and RM in order to determine the winner. However, for authentication to take place, we found that except [13] all the protocols have an authority center to authenticate the identity of the user.

With regards to efficiency comparison as shown in Table 3, we found that group-oriented signature-based protocols do not have a registration phase, and [9,11] that belong to the TTP-based protocols do not have an initial phase. This means that any of these two phases can replace the other in some protocols. On the other hand, we found that group-oriented signature-based protocols have the highest efficiency, with [10] been the highest among all the categories. These protocols also allow for an AM, as well as any users (bidder or auctioneer) wishing to verify published values to perform multiple signature verifications together in one operation. This process helps reduce the computational costs associated with these protocols. Moreover, we found that TTP-based protocols have the lowest efficiency, with [11] been the lowest efficiency among all the categories.

In general, we found that most these protocols aim at reducing the computational and communication costs, particularly in combination with the security requirements above, and some of them attempt to make a trade-off between the effectiveness and the robustness. Unfortunately, each protocol has a limitation in some aspect.

4. Some proposals of new directions

In this section, we propose some new directions that could be regarded as a good contribution in improving the security, efficiency, and trust challenges that still militate against the success of e-auctions using the consumer-to-consumer (C2C) model as a case study.

The C2C model of auction [32] is a type of e-commerce application involving the electronically facilitated transaction between consumers through some third party, in which a consumer posts an item for sale and other bids to purchase it; the third party generally charges a flat fee or commission. The sites are only intermediaries, just there to match customers. They do not have to check the quality of the products being offered. At the beginning of e-commerce, the business to consumer (B2C) model was dominant; nowadays, the trend is increasingly embracing the C2C model. Thus, based on this survey, we proposed two new directions for the C2C model.

4.1. *Reducing trust on third party*

The requirements for bidder accountability and fairness cannot easily be achieved as there is a conflict of interest between these two requirements. For example, the bidders accountability requirements such as guidelines on procurement, confidentiality, conflicts of interest, and disclosure of contracts, as well as the *Better Practice Guide on Fairness and Transparency in Purchasing Decisions* published by the ANAO in August 2007 [33] in one hand and fairness as mentioned in Section I on the other hand have a great tendency to conflict each other. Achieving one may lead to sacrificing the other. In general, all English E-Auc-

Table 2. Comparison of security requirements.

	Design philosophy								
	Pseudonym protocols		Trusted third party protocols			Group-oriented signature protocols			
Security requirement properties	Omote et al. [26]	Chung et al. [29]	Chang et al. [11]	Li et al. [9]	Chung et al. [24]	Xiong et al. [10]	Chang [17]	Chang[18]	Yang et al. [13]
Unforgeability	✓	✓	✓	✓	✓	✓	×	×	×
Verifiability	✓	✓	✓	✓	✓	✓	✓	✓	✓
Non-repudiation	✓	✓	✓	*	✓	✓	✓	✓	✓
Fairness	*	✓	✓	✓	✓	✓	✓	✓	✓
Anonymity	*	✓	✓	✓	✓	✓	✓	✓	✓
One-time registration	✓	✓	✓	✓	✓	✓	×	×	×
Unlinkability	x	✓	✓	✓	✓	✓	×	×	×
Traceability	✓	✓	✓	✓	✓	✓	*	*	*
Revocation	*	*	✓	*	✓	*	✓	✓	✓
✓	The scheme satisfies the corresponding property								
*	The scheme partially fulfills the property								
×	The scheme does not support the property								

tion protocols in the literature are classified according to how they deal with the trust problem into [1]:

(1) *Honest Third Party*: As long as the auctioneer is a beneficiary, the assumption that s/he follows the auction protocol may not be realistic. An alternative could be that a *honest third party* or TTP. Here, the communication between bidders and auctioneers is not directly, but through the TTP. Therefore, when disputes occur, the TTP can be called upon to resolve the problem.

(2) *Threshold trust*: This mechanism protects the E-Auction protocol against malicious auctioneer by distributing the role of auctioneer across n servers. The auction can be considered secure unless threshold t of auction servers collude (where $t < n$). However, this mechanism requires high communication between bidders and auction servers, as well as between the servers themselves.

(3) *Two-servers trust*: This mechanism divides trust among two servers owned by different entities. Here, the auction outcomes can be fair as long as the two entities do not collude. This mechanism is more efficient than threshold trust. However, if one of two servers decides not to cooperate, then the auction result cannot be computed.

(4) *Distributed bidder trust*: In this protocols, the auctioneer is not adopted. Instead, the bidders compute the auction result cooperatively. This mechanism prevents the collusion effectively unless all bidders are malicious. However, the weakness of this mechanism is that all bidders must participate during the winner determination phase. This not reasonable, as when the number of bidders is large.Verifiable secret sharing (VSS) is a cryptographic primitive proposed in [34] to achieve security against cheating participants. A verification protocol allows the honest participants to ensure that they can recover a unique secret. Harkavy et al. [35] and Schoenmakers [36] used VSS in their schemes. This immediately reduces the trust required in the third party and prevents malicious participants; hence, it reduces the overhead of communication mentioned above. Recently, Tian et al. [37] proposed efficient publicly VSS scheme using bilinear pairings, this scheme seems well suited for auction applications. It has extensions to the case without a dealer (or without a trusted center). This means that is more suited to C2C auction model mentioned above. Moreover, in the distribution shares phase of this scheme, only using bilinearity of bilinear paring, anybody can verify that the participants received whether correct shares without implementing interactive or the non-interactive protocol and without constructing the so-called witness of shares applied in the Fiat–Shamir's technique.[38]

4.2. Improving efficiency

Many of English auction protocols with robust security properties have high computations and/or communications cost,[10,22,42] therefore essential to improve their efficiency to make them practical. Protocols which use digital signatures, such as those protocols that have been classified in group-oriented signature, are well suited to exploit batch verification.[10,13,17,18] These protocols allow an AM, as well as any users (bidder or auctioneer) wishing to verify published values to perform multiple signature verifications together in one operation in order to obtain significant computational savings.

In order to improve the efficiency, certificateless public key cryptography (CL-PKC) simplifies the complex certificate management in the traditional public key cryptography. Also it reduces the trust assumptions made of the TTP significantly[39] that are discussed in previous subsection. Furthermore, CL-PKC provides the following features [40]:

- CL-PKC simplifies the complex certificate management in the traditional public key cryptography;
- The key generation center (KGC) in CL-PKC is incapable to generate the user's whole private key, which does not have the highest priority for key generation;
- CL-PCK provides lower computational costs and communication overheads.

Table 3. Efficiency comparison.

	Design philosophy								
	Pseudonym-based protocols		Trusted third party-based protocols			Group-oriented signature-based protocols			
Auction phase	Omote et al. [26]	Chung et al. [29]	Chang et al. [11]	Li et al.[9]	Chung et al. [24]	Xiong et al. [10]	Chang et al. [17]	Chang et al. [18]	Yang et al. [13]
Initial phase		T_m			$(3n+1)T_x + nT_m + nT_H$	$T_m + T_H$	$4T_m + 2T_E + 2T_D + 6T_x$		$2T_m + 4T_x + T_D + T_E + 4T_H$
								$4T_m + 2T_E + 2T_D + 4T_x + 2T_H$	
Regis-tration phase	$(2n+1)T_m + (2n+1)T_x + nT_\sigma + 2nT_v$	$nT_m + nT_H + 2T_v$	$(4n+1)T_m + nT_v$	$2nT_x + 2nT_m + (n+1)T_\sigma$	$4T_x + 2T_m + 2T_H$				
Bidding Phase	$nT_\sigma + nT_v$	$nT_\sigma + 2nT_m + nT_c$		nT_Z	$3T_x + 6T_m + T_H$	$2T_H + 3T_x + (2n+2)T_m + T_p$		$2T_E + 2T_D + 2T_H$	$4T_H$
			$7nT_m + nT_E + nT_D + 2T_v + nT_i$				$2T_E + 2T_D + 5T_H$		
Winner deter-mina-tion phase	$T_\sigma + T_v$	$T_H + nT_v$	$5T_m + 2T_i + T_v$	T_Z	$2T_x + T_m + T_H$	$nT_H + nT_p$	$2T_i + T_D$	$2T_i + T_D$	T_v

Finally, we note that CL-PCK provides lower computational costs and communication overheads. Therefore, it is well suited for E-Auction protocols. The setup of CL-PKC needs third party which possesses a public key and a secret master key. In an electronic English auction, we can consider the auction agent center (AAC) as a third party among users, who is a combination of auctioneers and bidders. The AAC uses the secret master key along with the bitstring of the user's identity to compute the users' partial private key. This step is done in pairing based ID-PKC [41] and the generated private key is the private key that corresponds to the bitstring of user's identity. That is why certificates are no longer needed in CL-PKC.

5. Conclusion

Nowadays, the e-auction has successfully replaced the traditional version; this article conducts a survey on electronic English auction security protocols, and classifies these protocols into three main schemes: group-oriented signature-based protocols, TTP-based protocols, and pseudonym-based protocols. These schemes are discussed and compared with each other together with the security policy for actual e-auction systems such as eBay, Yahoo!, and uBid.

Finally, based on this survey, we proposed two new directions for the C2C model, these directions go directly to address two important issues in auction schemes; these include improving e-auction efficiency and reduction of trust on third party.

Acknowledgments

The author would like to acknowledge National Natural Science Foundation of China under Grant Nos. 61003230, 61370026 and 61202445, the Fundamental Research Funds for the Central Universities under Grant No. ZYGX2013J073 and ZYGX2012J067.

Disclosure statement

No potential conflict of interest was reported by the authors.

Notes on contributors

Abubaker Wahaballa is currently working as a Postdoctoral Fellow at School of Informa-tion and Software Engineering, University of Electronic Science and Technology of China UESTC. He received his PhD degree from UESTC in 2015. His current research interests include information security, cryptography, steganographyand DevOps.

Zhen Qin was born in 1983. He is currently a lecturer in School of Information and Software Engineering, University of Electronic Science and Technology of China. He received his BSc degree in communication engineering from University of Electronic Science and Technol-ogy of China in 2005, and a MSc degree in electronic engineering from Queen Mary University of London in 2007, and a MSc and a

PhD degree in communication and information system from University of Electronic Science and Technology of China in 2008 and 2012, respectively. His current research interests include network measurement, wireless sensor networks, content distribution networks, and mobile social networks.

Hu Xiong is an associate professor in the School of Information and Software Engi-neering, UESTC. He received his PhD degree from UESTC in 2009. His research interests include information security and cryptography.

Zhiguang Qin is a professor in School of Information and Software Engineering, Uni-versity of Electronic Science and Technology of China. His research interests include net-work security and social network. He has pub-lished more than 100 papers on international journals and conference among which more than 50 are indexed by SCI and EI. He has been principal investor of two NSF key projects, two sub-topics of national major projects, and six national 863 projects.

Mohammed Ramadan received the BS degree in Communication Engineering from Karary University in 2007, Khartoum, Sudan, and the MS degree in MSc in Computer Engineering , Information Security from University of Elec-tronic Science and Technology of China in 2013, Chengdu, China. He is currently work-ing toward the PhD degree in Information Security, Mobile Communication Security

from University of Electronic Science and Technology of China. His current research interests include mobile communication and GSM security.

References

[1] Jarrod T. Security, anonymity and trust in electronic auctions. ACM Crossroads. 2005; Spring Edition; Vol. 11.3: p. 3–9.

[2] IBM Web Sphere Studio. Auction scenario: B2C online auction site using EJB tools. International Business Machines Corporation; 2002.

[3] Hirakiuchi D, Sakurait K. English vs. sealed bid in anonymous electronic auction protocols. In: Proceedings of the 10th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, 2001. WET ICE 2001; Cambridge (MA): IEEE; 2001.

[4] Trevathan J, Read W, Ghodosi H. Design issues for electronic auctions. Second International Conference on e-Business and Telecommunication Networks; 2005October 3--7; Reading (UK); p. 340–347.

[5] Jarrod T, Read W. Detecting shill bidding in online English auctions. In: Gupta M, Sharman R, editors. Handbook of research on social and organizational liabilities in information security. New York (NY): IGI Global; 2009. p. 446–470.

[6] Choi J, Lim G, Chang K. An agent based market design methodology for combinatorial auctions. J. Artif. Soc. Soc. Simul. 2010;13:2.

[7] Federal Bureau of Investigation. 2011 Internet crime Report; 2011 [cited 2013 May 28]. Available from: http://www.ic3.gov/media/annualreport/2011_ic3report.pdf

[8] Lindell Y. Anonymous authentication. J. Privacy Confidentiality. 2010;2:35–63.

[9] Li MJ, Juan JS, Tsai JH. Practical electronic auction scheme with strong anonymity and bidding privacy. Inform. Sci. 2011;181:2576–2586.

[10] Xiong H, Chen Z, Li F. Bidder-anonymous English auction protocol based on revocable ring signature. Expert Syst. Appl. 2012;39:7062–7066.

[11] Chang CC, Cheng TF, Chen WY. A novel electronic English auction system with a secure on-shelf mechanism. IEEE Trans. Inform. Forensic. Secur. 2013;8:657–668.

[12] Nguyen K, Traoré J. An online public auction protocol protecting bidder privacy. 5th Australasian Conference, ACISP 2000; 2000 Jul 10--12; Brisbane: Springer; 2000.

[13] Yang FY, Liao CM. An anonymous auction protocol based on GDH assumption. Int. J. Network. 2011;12:171–177.

[14] Xiong H, Qin Z, Zhang F, Yang Y, Zhao Y. A sealed-bid electronic auction protocol based on ring signature. International Conference on Communications, Circuits and Systems: [ICCCAS 2007]; 2007 Jul 11--13; Kokura; 2007. p. 480–483.

[15] Wu TC, Chen KY, Lin ZY. An English auction mechanism for internet environment. In: Proceeding of ISC; Oxford (UK): 2002. p. 331–337.

[16] Chaum D, van Heyst E. Group signatures, advances in cryptography -- Eurocrypt 91. Vol. 547, Lecture notes in computer science. Workshop on the Theory and Application of Cryptographic Techniques . 1991 April 8--11; Brighton (UK):Springer-Verlag; 1991. p. 257–265.

[17] Chang CC, Chang YF. Efficient anonymous auction protocols with freewheeling bids. Comput. Secur. 2003;22:728–734.

[18] Chang YF, Chang CC. Enhanced anonymous auction protocols with freewheeling bids. In: Proceedings of the 20th International Conference on Advanced Information Networking and Applications (AINA'06); Washington (DC): IEEE; 2006.

[19] http://www.yahoo.com/.

[20] http://www.ebay.com/.

[21] https://www.ubid.com.

[22] Castell S. Code of practice and management guidelines for trusted third party services. INFOSEC Project

Report S2101/02 In: Castell S editor. Ver. 1.0, Castell, Spain, 1993 October; 1993.

[23] Jiang P, Jones DB, Javie S. How third-party certification programs relate to consumer trust in online transactions: an exploratory study. Psychol. Market. 2008;25:839–858.

[24] Chung YF, Huang KH, Lee HH, Lai F, Chen TS. Bidder-anonymous English auction scheme with privacy and public verifiability. J. Syst. Software. 2008;81:113–119.

[25] Omote K, Miyaji A. A practical English auction with one-time registration. In: Australasian Conference on Information Security and Privacy; Sydney, Australia; 2001.

[26] Omote K, Miyaji A. A practical English auction with simple revocation. IEICE Trans. Fundamentals. 2002; E85A:1054–1061.

[27] Omote K, Miyaji A. A second-price sealed-bid auction with verifiable discriminant of p 0-th root. Vol. 2357, Lecture notes in computer science; Southampton: Springer; 2003. p. 57–71.

[28] Chaum D. Security without identification: transaction systems to make big brother obsolete. Commun. ACM. 1985;28:1030–1044.

[29] Chung Y, Chen Y, Chen T, Chen T. An agent-based English auction protocol using elliptic curve cryptosystem for mobile commerce. Expert Syst. Appl. 2011;38:214–225. Elsevier.

[30] Huan K. Mobile auction agent model using agent-based English auction protocol [doctoral dissertation]. Taipei: National Taiwan University; 2008.

[31] Nikooghadam M, Zakerolhosseini A. Secure communication of medical information using mobile agents. J. Med. Syst. 2012;36:3839–3850.

[32] Haag S, Maeve C, Donald MJ, Alain P, Richard D. Management information systems: for the information age. 3rd Canadian ed. New York (NY): McGraw-Hill Ryerson; 2006.

[33] Australian National Audit Office. Fairness and transparency in purchasing decisions. Canberra: ANAO; 2007.

[34] Chor B, Goldwasser S, Micali S, Awerbuch B. Verifiable secret sharing and achieving simultaneity in the presence of faults. In: Proceedings of the 26th IEEE Symposium on the Foundations of Computer Science (E'OCS); Washington (DC); 1985. p. 383–395.

[35] Harkavy M, Tygar JD, Kikuchi H. Electronic auctions with private bids. In: 3rd Usenix Workshop on Electronic Commerce; Berkeley (CA); 1998. p. 61–83.

[36] Schoenmakers B. A simple publicly verifiable secret sharing scheme and its application to Electronic Voting. In: Wiener M, editor. Advances in cryptology -- Crypto'99, LNCS 1666. Berlin: Springer-Verlag; 1999. p. 148–164.

[37] Tian Y, Peng C, Ma J. Publicly verifiable secret sharing schemes using bilinear pairings. Int. J. Network Security. 2012;14:142–148.

[38] Fiat A, Shamir A. How to prove yourself: practical solutions to identification and signature problems. In: Odlyzko AM, editor. Advances in cryptology -- Crypto'86. Santa Barbara (CA): Springer-Verlag; 1987. p. 186–194.

[39] Al-Riyami SS, Paterson KG. Certificateless public key cryptography. In: Proceedings of the Cryptography-Asiacrypt 2003 LNCS. Taipei: Springer-Verlag; 2003. p. 452–473.

[40] Al Housani H, Baek J, Chan YY. Survey on certificateless public key cryptography. In: International Conference of Internet Technology and Secured Transactions (ICITST); 2011 Dec 11--14; Abu Dhabi. p. 53–58.

[41] Boneh D, Franklin M. Identity-based encryption from the weil pairing. SIAM J. Comput. 2003;32:586–615.

[42] Boyd C, Mao W. Security issues for electronic auctions. Bristol (UK): Hewlett-Packard Laboratories; 2000.