JOURNAL OF INFORMATION SCIENCE AND ENGINEERING 37, 635-652 (2021)
DOI: 10.6688/JISE.202105_37(3).0009

Efficient First-Price Sealed-Bid Auction Scheme*

QIAN MENG[1,3,4], JIANFENG MA[2,+], KEFEI CHEN[4], YINBIN MIAO[2]
AND TENGFEI YANG[2]
[1]*School of Telecommunication Engineering*
[2]*School of Cyber Engineering*
Xidian University
Xi'an, 710071 P.R. China
[3]*State Key Laboratory of Cryptology*
P. O. Box 5159, Beijing, 100878 P.R. China
[4]*School of Science*
Hangzhou Normal University
Hangzhou, 311121 P.R. China
E-mail: mengqian@stu.xidian.edu.cn; jfma@mail.xidian.edu.cn; kfchen@hznu.edu.cn;
ybmiao@xidian.edu.cn; yangtf@stu.xidian.edu.cn

Electronic auction has opened up a popular research topic in electronic commerce over the past few years. It can be widely utilized in various circumstances, as it provides a flexible way to improve the transaction rate and save the costs. Despite its advantages in transactions, current electronic auction protocols incur high communication rounds as well as storage and computational overhead among auctioneer(s) and multiple bidders, especially for resource-limited devices. In this paper, by leveraging Short Comparable Encryption scheme based on Sliding Window method (SCESW) and multilinear maps, we construct an Efficient First-price Sealed-bid Auction scheme (EFSA) to address the aforementioned problem. The novelty lies in that we provide a more efficient construction in electronic auction system, which just needs one round communication and drastically decreases the computational and storage costs in the bidder side when compared with existing schemes. The formal security analysis proves that EFSA scheme can achieve weak indistinguishability in standard model. Moreover, simulation results show that EFSA scheme is efficient and feasible in practice.

Keywords: comparable encryption, sliding window method, auction system, efficient first-price sealed-bid auction, weak indistinguishability

1. INTRODUCTION

With the proliferation of increasing intelligent devices [1, 2] (*i.e.*, palm computer, smartphones, *etc*.), resource-limited devices have a pivotal role in sharing services and provide data storage in electronic transactions. In reality, the drawbacks of traditional auction activities bring many inconveniences to the auction [3], such as time, place, number of bidders and so on. With the rapid development of the Internet [4, 5], people are

Received January 21, 2019; revised April 4, 2019; accepted May 14, 2019.
Communicated by Xiaohong Jiang.

[+] Corresponding author.

[*] This work was supported by the Key Program of NSFC (No. U1405255), the Shaanxi Science & Technology Coordination & Innovation Project (No. 2016TZC-G-6-3), the National Natural Science Foundation of China (No. 61702404), the China Postdoctoral Science Foundation Funded Project (No. 2017M613080).

eager for auction activities to be carried out online, in order to avoid all kinds of drawbacks in the real auction, and make the auction activities flexible, convenient and fast. Moreover, deceptive issues occur frequently in the e-auction and this situation fails to promote the progress of the electronic auction. As a consequence, the security issues on E-auction, especially the sealed-bid auction, have become a nominating form in preserving the privacy of bid. Thus, exploring novel auction protocols, which enable intelligent users to securely and efficiently do auction transactions according to bidders needs, is of prime importance in both practice and academic fields [6–8].

Comparable encryption can be used to the auction scene to gain the highest bid among bidders. The origin of ciphertexts' comparison is the millionaires' problem. Yao provided a fundamental solution to tackle millionaires' problem. After that, a considerable amount of schemes have been discussed. To reduce computational and storage overhead, Chen *et al.* [9] proposed an efficient request-based comparable encryption scheme by using sliding window method. To improve work efficiency and relief overhead, Meng *et al.* discussed an Short Comparable Encryption scheme based on Sliding Window method (SCESW) in Internet of Everything [10]. When we discuss the auction system, security problem is a fundamental issue to be considered.

A considerable amount of schemes have been published on security problems in auction system, which mainly use the method of the secure multiparty computation (MPC), secret sharing (SS), homomorphic secret sharing, *etc.* However, it inevitably incurs different levels of security problems and high round communications among bidders and the auctioneer. In auction system, how to allow multi-bidders to participate in the auction system and exchange a master key shared among all bidders is a significant problem to be considered in practice. To overcome these problems, Zhu *et al.* [11] proposed a auction protocol which utilized cryptographic multilinear maps. Therefore, it is vital important to consider the security and efficiency of e-auction system. The important issue is how to design the e-auction scheme with privacy preserving to cater to modern auction system.

In this paper, inspired by Zhu's scheme [11] and sliding window method, we devise a basic Efficient First-price Sealed-bid Auction scheme (EFSA) to improve efficiency. With utilizing sliding window method, EFSA system can lighten the computational and storage burden of bidders in electronic auction. However, how to exchange a common master key among all bidders is a significant task. When considering multi-bidders settings [12], we can tackle this issue by using multilinear maps. Furthermore, with the privacy [13,14] and confidentiality of bids kept, EFSA system needs only one communication round among the auctioneer and bidders. Specifically, the main contribution of our paper are depicted as follows:

- **One-round communication:** For a typical multiple bidders auction scheme, our proposed scheme model requires only one auctioneer in contrast to a majority of works requiring multiple auctioneers. That is to say, our scheme is significantly useful in virtual auction environment due to less communication workload. EFSA system allows multiple bidders to participate in this auction occasion and only needs one-round communication, which the privacy and confidentiality of bids are guaranteed and only one communication round is required between the auctioneer and bidders.

- **Lightweight computation on bidders:** With the help of sliding window method, EFSA system reliefs the high computational and storage overhead of bidders in terms of files encryption, token generation and ciphertexts generation.

- **Security and practicability:** Bids are keeping private and secret in the process of auction. The auctioneer cannot get the real value of each encrypted bid. No one can fake the winning identity, which ensures the fairness of auction. Formal security analysis shows that EFSA system is secure against weak indistinguishability in standard model. Extensive experiments demonstrate that EFSA system is efficient and feasible in electronic auction environment.

2. RELATED WORKS

The private comparison has long been a topic of great interest in a wide range of fields. A considerable amount of work has been proposed on private comparison. It is known that millionaires' problem is the origin of ciphertexts' comparison. Surveys such as that conducted by Yao(1986) [15] have shown that a fundamental solution was proposed to tackle millionaires' problem. After that, for the purpose of protecting data privacy in the comparison process, Order Preserving Encryption(OPE) scheme [16, 17] was proposed. However, disadvantages of OPE schemes are depicted as follows. Firstly, there exist many interactions between the client and the server in OPE schemes. Secondly, if all numbers are encrypted by OPE schemes, plaintexts can be easily derived from ciphertexts. Therefore, it is urgent to enhance OPE schemes' security. To address this problem, Furukawa *et al.* introduced a request-based comparable encryption scheme [18] which could be much more securer than OPE scheme and only needed one round communication. To further reduce computational and storage overhead, Chen *et al.* [9] proposed an efficient request-based comparable encryption scheme by using sliding window method. To improve work efficiency and relief overhead, Meng *et al.* discussed an Short Comparable Encryption scheme based on Sliding Window method (SCESW) in Internet of Everything [10]. Hence, with satisfying needs of comparable operations, comparable encryption schemes can be applied in many practical fields (*i.e.*, auction scenes, image retrieval, *etc.*).

In a secure auction system, it is significantly important to keep the confidentiality and privacy of bids. Studies show that various of protocols were proposed in the following schemes [19–23]. Homomorphic encryption [24,25] is a fundamental way of keeping the auction privacy. Peng *et al.* [26] described a new first-bid e-auction scheme based on secret sharing to achieve bids privacy. In an analysis of performing sealed-bid auctions, Franklin *et al.* [27] proposed the design and implementation of a distribute service. The study by Li *et al.* [28] offers probably an analysis of an anonymity auction scheme by utilizing zero knowledge proof. In a large longitudinal study, Brandt *et al.* [29,30] investigated the bid privacy problem in sealed-bid auction, proving that the first-price sealed-bid auction could be emulated by an unconditionally fully private protocol. Unfortunately, the main defects in existing schemes are high round communications between bidders and the auctioneer.

Another well-known problem among all bidders is that how to exchange a common master key. Using the traditional key to share the master key can cause the increase of communication rounds. To reduce the communication rounds, Zhu *et al*. proposed a primitive which utilizes cryptographic multilinear map [11,31]. Therefore, we proposed an efficient first-price sealed-bid auction scheme based on SCESW scheme which tries to obtain the maximum security level with the minimum communication round(s), and relieve computational and storage overhead. Meanwhile, we consider that multiple bidders participate in auction scheme. Our proposed scheme model requires only one auctioneer in contrast to a majority of existing works requiring multiple auctioneers, where not only the privacy and confidentiality of bids are kept, but also only one communication round is required between the auctioneer and bidders.

Although the latest multiple auction system can achieve the comparable operation and gain the highest bids in auction scene, its computational and storage overhead will increase with the number of bidders. Our proposed scheme greatly reduces the computational and storage costs in practice. To achieve practicability and feasibility in auction system, we propose an Efficient First-price Sealed-bid Auction scheme (EFSA). Compared with several auction systems [11,24,28,32], EFSA system only needs one auctioneer and one-round communication, which is shown in Table 1.

Table 1. Auction protocol comparison.

Protocol	Auctioneer	Verifiability	Fairness	Privacy	Round
NS14 [33]	m	✓	✓	✓	$o(n)$
LJT11 [28]	3	✓	✓	✓	$o(n)$
PRS08 [34]	1	X	X	✓	$o(n)$
Zhu's scheme [11]	1	✓	✓	✓	$o(1)$
Our construction	1	✓	✓	✓	$o(1)$

3. PRELIMINARIES

Here, we give a brief review of background as the basis of EFSA system, which includes sealed-bid auction, multilinear maps, sliding window method and weak indistinguishability.

3.1 Sealed-bid Auction

The main form of sealed-bid auction includes first-price sealed-bid auction and Vickrey auction [11]. The process of the first-price sealed-bid auction indicates that bidders will seal their bids without knowing any other's bids. After the auction, the auctioneer opens tenders and announces the highest bid. That is to say, the bidder who owns the highest bid will pay the price and obtain the goods. Moreover, the Vickrey auction is identical to the first-bid sealed-bid auction except that the first-price bidder is the winning bidder who pays the second-highest bid rather than his/her own.

3.2 Multilinear Maps

The first serious discussions and analysis of multilinear map has emerged in 2013 by Garg *et al*. In paper [31], it has commonly been assumed that there exists a group generator ρ, where inputs are a security parameter λ and a positive integer k in order to illustrate the number of the allowed pairing operations. $\rho(1^{\lambda},k)$ outputs a sequence of groups $\vec{\mathbb{G}} = (\mathbb{G}_1,\ldots,\mathbb{G}_k)$ each of large prime order $p > 2^{\lambda}$. In addition, let g_i be a canonical generator of $\mathbb{G}_i$ and $g = g_1$.

They assume the existence of a set of bilinear maps $\hat{e}_{i,j} : \mathbb{G}_i \times \mathbb{G}_j \longrightarrow \mathbb{G}_{i+j} \mid i,j \geq 1; i+j \leq k$, where $e_{i,j}$ satisfies the following relation

$$\hat{e}_{i,j}(g_i^a,g_j^b) = g_{i+j}^{ab}, \quad \forall a,b \in \mathbb{Z}_p.$$

When the context is obvious, they will always drop subscripts i,j. For example, they simply write $\hat{e}(g_i^a,g_j^b) = g_{i+j}^{ab}$.

3.3 Sliding Window Method

Koc proposed sliding window method [35] which was one of extensively utilized methods for exponentiation. For instance, when we compute x^e, e usually is rewritten by using its binary code, such as $e = (b_{n-1},\ldots,b_1,b_0)$, $b_i \in \{0,1\}$, $i = 0,1,\ldots,n-1$. Moreover, $(b_{n-1},\ldots,b_1,b_0)$ is divided into a tuple of zero windows and nonzero windows according to the value of b_i. The result of adopting sliding window technology indicates the reduction of computation and management costs. Details of sliding window method is illustrated in [10].

In our proposed scheme, numeric numbers or bids are considered as a sequence of binary codes. Besides, we suppose that all the windows have the same window size without distinguishing zero windows or nonzero windows. In order to gain a trade-off between the security and the efficiency of our scheme in practice, the fixed window size is chosen according to user's security level requirements [10].

3.4 Weak Indistinguishability

This section first introduces weak indistinguishability of SCESW scheme, intended to prove that EFSA scheme meets weak indistinguishability in standard model.

Definition 1 *[36] A comparable encryption scheme is weakly indistinguishable, for every polynomial time adversary $\mathscr{A}$, if $Adv^2n_{\{\mathscr{C},\mathscr{A}\}} := |Pr[Exp^2n_{\{\mathscr{C},\mathscr{A}\}} = 0] - Pr[Exp^2n_{\{\mathscr{C},\mathscr{A}\}} = 1]|$ is negligible in weak distinguishing game. We give an detail description of weak distinguishing game. The weak distinguishing game is conducted between challenger $\mathscr{C}$ and adversary $\mathscr{A}$ [36]. When $\mathscr{C}$ receives a security parameter $k \in N$ and a range parameter $n \in N$, it runs $(parameter, mkey) \leftarrow Gen(k,n)$, and gives $parameter$ to $\mathscr{A}$. $\mathscr{C}$ responds to queries from $\mathscr{A}$ in the game as follows;*

- *Receiving a number $0 \leq num < 2^n$, $\mathscr{C}$ returns a token $token = Der(parameter, mkey, num)$.*
- *Receiving a number $0 \leq num < 2^n$, $\mathscr{C}$ returns a ciphertext $ciph = Enc(parameter, mkey, num)$.*
- *$\mathscr{C}$ receives a pair of numbers num_0, num_1 such that $0 \leq num_0 < num_1 < 2^n$ only once in the game.*
- *Receiving this message, $\mathscr{C}$ randomly chooses $b \in \{0,1\}$ and returns $ciph = Enc(parameter, mkey, num_b)$.*

During the weak distinguishing game, $\mathscr{A}$ is not allowed to make such following query: $\exists\,(0 < l < n)\; s.t.\; ((\alpha_1,\dots,\alpha_{n-1}) = (\beta_1,\dots,\beta_{n-1}) = (\gamma_1,\dots,\gamma_{n-1})) \wedge (\beta_{n-1} < \gamma_{n-1})$, where $num = \sum_{0\le i\le n-1} \alpha_i 2^i, num_0 = \sum_{0\le i\le n-1} \beta_i 2^i, num_1 = \sum_{0\le i\le n-1} \gamma_i 2^i$ such that $\alpha_i, \beta_i, \gamma_i \in \{0,1\}$ for all i. At the end of the game, $\mathscr{A}$ sends $b' \in \{0,1\}$ to $\mathscr{C}$. The result of the game $Exp^2 n_{\{\mathscr{C},\mathscr{A}\}}$ is 1 if $b = b'$; otherwise 0.

4. PROBLEM FORMULATION

In this section, we give the system model, SCESW scheme and overview of EFSA protocol, respectively.

4.1 System Model

We consider a first-price sealed-bid auction scenario, involved with four main entities, namely Key Generator Center(KGC), AUctioneer(AU), bidders and Cloud Server Provide(CSP), which are demonstrated in Fig. 1 (a). KGC first generates keys and distributes keys to bidders, as shown in step ①. In step ②, bidders then send their encrypted bids to CSP without loss of confidentiality. With almost unlimited storage and computational capacities, CSP can store ciphertexts and tokens for the following operations with the step ③. AU performs some comparable operations for gaining the highest bid and fulfills one time auction, which is demonstrated by step ④. The specific role of each entity is depicted as follows:

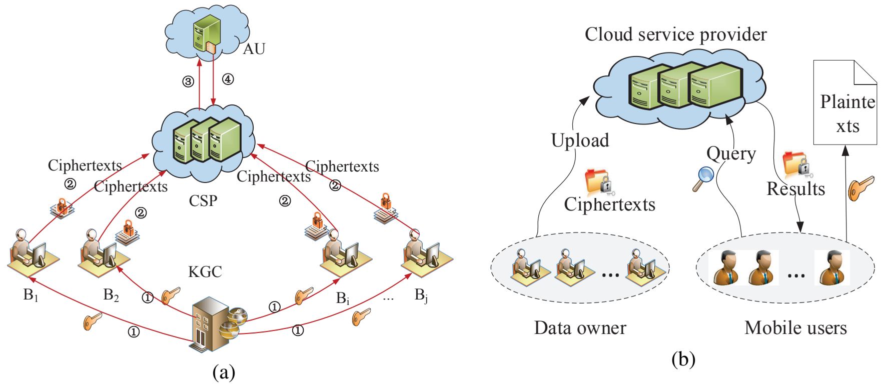


Fig. 1. (a) The infrastructure of auction system; (b) The infrastructure of SCESW scheme.

- Key Generator Center: KGC is responsible for generating system parameters, generating the secret key and the master key $\mathscr{MSK}$ and then distributing secret keys for bidders.
- AUctioneer: AU is responsible for constructing the auction system and then does comparable operations.
- Bidders: In order to keep the privacy of bids, bidders encrypt the data with the master key and generate tokens with their random values before sending them to CSP.

- Cloud Server Provide: CSP owns almost unlimited computational and storage capacities to store files.

In this paper, it is worth noticing that AU and KGC are fully trusted entities and CSP is an honest-but-curious third-party which honestly executes the specified protocols but is curious to deduce sensitive data from stored ciphertexts. Besides, we assume bidders do not collude with AU.

4.2 SCESW Scheme

First, we give a description of our basic SCESW scheme [10] involving five algorithms **KeyGen, Par, Der, Enc and Cmp**. The system of SCESW scheme is demonstrated in Fig. 1 (b), which consists of Cloud Server Provider(CSP), User and Data Owner(DO). Before presenting concrete construction of the following scheme, we show some notations utilized in the whole paper in Table 2.

Table 2. Notation descriptions in SCESW scheme.

Notations	Descriptions
$\mathscr{MSK}$	Master key
$\mathscr{PP}$	Public parameters
t	Window size
m	Number of window blocks
$\mathscr{TK}$	Token of number
H_i	$Hash_i(i = 1,2,3,4,5)$ function

The overview of SCESW scheme [10] is presented in Fig. 2:

This algorithm fails to work when **Cmp** produces c_j such that $c_j \neq 0$ or when $c_j = 0$ for all $i = m-1, m-2, \ldots, 0$. If $\mathbb{N} > \mathbb{N}^*$, then $1 \leq c_j \leq 2^t - 1$ holds. If $\mathbb{N} < \mathbb{N}^*$, then $2^t \leq c_j \leq 2^{(t+1)} - 2$ holds. If $\mathbb{N} = \mathbb{N}^*$, then $c_j \equiv 0$ holds.

Remarks: SCESW scheme can shift computational and storage overhead of DOs and users in cloud computing environment, which can be applied in a broad range of applications. Furthermore, we extend the basic SCESW scheme to cater to the auction scene so that EFSA scheme can allow multi-bidder participating in this auction system by adopting multilinear maps. Compared with other auction protocols, EFSA scheme not only reduces computational and storage overhead but also needs only one round communication.

4.3 Overview of EFSA System

In order to allow multiple bidders participating in auction system, we utilize multilinear maps and SCESW scheme to construct EFSA scheme. We give a general description for EFSA system in Fig. 3, which consists of several algorithms, namely **Setup, Key Generation, Token Generation, Bidding Comparison and Winner Opening**. As for the process in different algorithms in EFSA system, we will give a detailed introduction in Section 4.

EFSA scheme definition

The overview of SCESW scheme is presented as follows:

- **KeyGen**(1^k): Given the security parameter $k \in \mathscr{N}$, the range parameter $n \in \mathscr{N}$ and the master key $\mathscr{MSK}$, DO first randomly chooses hash functions: $H_1(.), H_2(.), H_3(.)$, then returns public parameter $\mathscr{PP}$ and the master key $\mathscr{MSK}$.

- **Par**$(\mathbb{N})$: Given the number $\mathbb{N}$, DO runs the algorithm to output the number $\mathbb{N}'$ defined with its binary code by utilizing sliding window method.

- **Der**$(\mathscr{PP}, \mathscr{MSK}, \mathbb{N})$: Given the master key $\mathscr{MSK}$, the number $\mathbb{N}$ and the public parameter $\mathscr{PP}$, DO outputs a token written by $\mathscr{TK}$.

- **Enc**$(k, n, \mathscr{MSK}, \mathbb{N})$: Given the $\mathscr{PP}$, the master key $\mathscr{MSK}$ and the number $\mathbb{N}$, DO randomly picks token $\mathscr{TK}$ and a random number $I \in \{0,1\}^k$. DO finally outputs ciphertexts $\mathscr{CP}$. DO submits $\mathscr{CP}$ to CSP.

- **Cmp**$(\mathscr{PP}, \mathscr{CP}, \mathscr{CP}^*, \mathscr{TK})$: Given two ciphertexts which are represented by $\mathscr{CP}$, $\mathscr{CP}^*$ and a token $\mathscr{TK}$, DO sets $j = m - 1$ and keeps producing c_j by decreasing j by 1 at each step.

Fig. 2. SCESW scheme definition.

EFSA scheme definition

The overview of EFSA scheme is presented as follows:

- **Setup**(1^k)**:** Given the security parameters k and groups $\mathbb{G}$ in multilinear maps, KGC outputs the secret key s_i and the master key $\mathscr{MSK}$.

- **Key Generation**$(\mathscr{MSK}, bid)$**:** Given the master key $\mathscr{MSK}$ and the bid *bid*, KGC generates the public parameter $\mathscr{PP}$.

- **Token Generation**$(\mathscr{PP}, \mathscr{MSK}, bid)$**:** Given the public parameter $\mathscr{PP}$, the master key $\mathscr{MSK}$ and the bid *bid*, bidders generate tokens of his/her encrypted data and send ciphertexts file set $\mathscr{CP}$ and tokens $\mathscr{TK}$ to CSP.

- **Bidding Comparison** $(\mathscr{TK}, \mathscr{CP}, \mathscr{CP}_i)$**:** AU conducts some computations of tokens and finds out the first different value of ciphertexts in CSP. And then, the bidding result is returned to AU.

- **Winner Opening**$(I_i, \mathscr{CP}_i)$**:** After receiving the bidding result, AU publishes the token of the highest bid. The bidder who wins the auction should send ciphertexts $\mathscr{CP}$ to AU as a proof. AU checks whether the bidder is the winner or not with the random number provided by the bidder.

Fig. 3. EFSA scheme definition

5. OUR CONSTRUCTION OF EFSA SCHEME

In this section, we will propose a novel first-price sealed-bid auction protocol based on comparable encryption. We only consider protocols in semi-honest model. It is worth noticing that bidders do not collude with AU.

In this section, we demonstrate the concrete construction of EFSA system in auction environment. With utilizing sliding window method to relieve high computational and storage costs, resources-limited bidders can gain auction results as soon as possible. Besides, our construction only needs one-round communication in multiparty key exchange. Compared with prior auction schemes [11,24,28,32], EFSA system can not only achieve high efficiency but also alleviate computational and storage overhead by utilizing sliding window method. In the following, we demonstrate the main algorithms in EFSA system, namely **Setup, Key Generation, Token Generation, Bidding Comparison and Winner Opening**.

A bulletin board is to allow every bidder to write their own bids. Besides, the content of the bulletin board cannot be revised once it is written on it. Next, we use multilinear maps to generate the master key $\mathscr{MSK}$ among all bidders. We set the window size as t, which means that each block has t bits. Auction system consists of w bidders and one AU. We assume that *bid* represents an arbitrary number with n bits. n is a multiple of t. If n is not a multiple of t, we make n to be a multiple of t by adding zero in the end of the n's binary code.

Setup(1^k): When we choose $w-1$ groups represented by $(\mathbb{G}_1,\mathbb{G}_2,\ldots,\mathbb{G}_{w-1})$ in multilinear maps, KGC randomly chooses $s_i \leftarrow \{0,1\}^k$ and then publishes g^{s_i} to share with all bidders in the auction system. After that, KGC computes the secure master key $\mathscr{MSK}$ which can be shared by bidders. Specifically, the i-th bidder computes:

$$e(g^{s_1},\ldots,g^{s_{i-1}},g^{s_{i+1}},\ldots,g^{s_w}) = e(g,\ldots,g,g,\ldots,g)^{s_1\ldots s_{i-1}s_{i+1}\ldots s_w} = g_{w-1}^{s_1\ldots s_{i-1}s_{i+1}\ldots s_w}. \tag{1}$$

Then KGC returns $\mathscr{MSK}$ to all bidders with setting $\mathscr{MSK} = g_{w-1}^{(s_1\ldots s_{i-1}s_{i+1}\ldots s_w)^{s_i}}$, where s_i represents the secret random number of the i-th bidder.

Key Generation($\mathscr{MSK}$,*bid*): When a certain bidder joins into EFSA system, KGC first selects the security parameter $k \in \mathscr{N}$, the range parameter $n \in \mathscr{N}$, then randomly chooses Hash functions which are defined as $H_1(.),H_2(.),H_3(.) : \{0,1\}^k \times \{0,1\}^* \to \{0,1\}^k$. Next, KGC distributes $\mathscr{PP} = (n,H_1,H_2,H_3)$ to bidders, where n represents the length of bid.

The i-th bid *bid* can be rewritten through its binary code by utilizing sliding window method. Eq. (2) defines $bid = bid'$,and t denotes the window size and $m = n/t$ represents the number of blocks.

$$bid = (b_0,\ldots,b_{n-1}) = \sum_{0\le i\le n-1} b_i 2^i; bid' = (B_0,\ldots,B_{m-1}) = \sum_{0\le i\le m-1} B_i (2^t)^i. \tag{2}$$

Finally, KGC returns the public key $\mathscr{PP} = (n,H_1,H_2,H_3)$ and secret keys s_i owned by the i-th bidder.

Token Generation($\mathscr{PP}$,$\mathscr{MSK}$,*bid*): Given a public parameter $\mathscr{PP}$, the master key $\mathscr{MSK}$ and the bid of bidder *bid*, bidder first generates tokens, where $B_0 = (b_0,\ldots,b_{t-1}),\ldots,B_{m-1} = (b_{n-t},\ldots,b_{n-1}),B_m = 0$ and $d_{i,j} = H_1(\mathscr{MSK},B_{i,m},\ldots,B_{i,j}), j = 1,2,\ldots,m$.

The i-th bidder outputs the token $\mathscr{T}\mathscr{K}_i = (d_{i,1}, \dots, d_{i,m})$ and ciphertext through Eq.(3).

$$f_{i,j} = H_3(d_{i,j+1}, I) + H_2(\mathscr{M}\mathscr{S}\mathscr{K}, d_{i,j+1}) + B_{i,j} \mod (2^{(t+1)} - 1)(j = m-1, \dots, 0). \tag{3}$$

Finally, the bidder outputs ciphertexts $\mathscr{C}\mathscr{P}_i = (I_i, (f_{i,0}, f_{i,1}, \dots, f_{i,m-1}))$ and sends $\mathscr{C}\mathscr{P}$ to CSP. Besides, the process of token generation is shown in Fig. 4 (a).

Here, $(f_{i,0}, f_{i,1}, \dots, f_{i,m-1})$ can be encoded into an integer for making ciphertexts short with the following equation $F_t = \sum_{0 \le i \le m-1} f_{i,j}(2^{(t+1)} - 1))^i$.

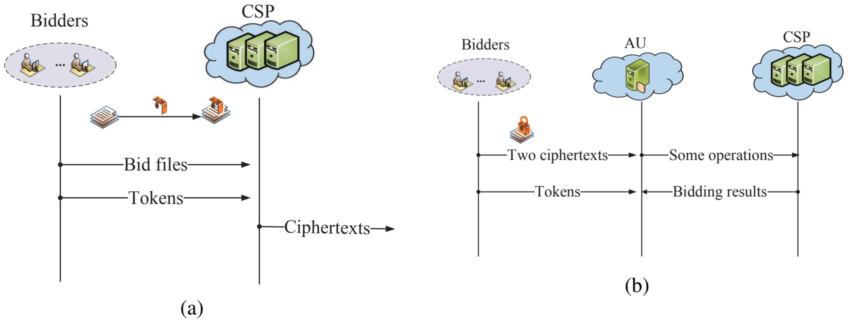


Fig. 4. (a) Process of token generation; (b) Process of bidding comparison.

Bidding Comparison($\mathscr{T}\mathscr{K}$,$\mathscr{C}\mathscr{P}$,$\mathscr{C}\mathscr{P}_i$): Each bidder sends her ciphertext $\mathscr{C}\mathscr{P}_i$ and token $\mathscr{T}\mathscr{K}_i$ to CSP. First, AU performs some operations in CSP and compares the relationship of two bids bid_1 and bid_2 in terms of the following process:

We assume that there exist a pair of ciphertexts $\mathscr{C}\mathscr{P}_1 = (I_1, (f_{1,0}, f_{1,1}, \dots, f_{1,m-1}))$, $\mathscr{C}\mathscr{P}_2 = (I_2, (f_{2,0}, f_{2,1}, \dots, f_{2,m-1}))$ and a token of the ciphertext $\mathscr{T}\mathscr{K} = (d_1, d_2, \dots, d_m)$.

- We set $j = m-1$ and keep producing c_j by decreasing j by 1 at each step.

$$\partial = f_{1,j} - f_{2,j} - H_3(d_{1,j+1}, I) + H_3(d_{2,j+1}, I') \mod (2^{(t+1)} - 1).$$

This repetition fails to work when bidding comparison phase generates ∂ such that $\partial \neq 0$ or when $\partial = 0$ for all $j = m-1, m-2, \dots, 0$. If $1 \le \partial \le 2^t - 1$, then it means $bid_1 > bid_2$. If $2^t \le \partial \le 2^{(t+1)} - 2$, then it means $bid_1 < bid_2$. If the equation holds $\partial \equiv 0$, then it means $bid_1 = bid_2$. Then we have Eq. (4).

$$\varpi = \begin{cases} -1 & if \quad 1 \le \partial \le 2^t - 1; \\ 0 & if \quad \partial \equiv 0; \\ 1 & if \quad 2^t \le \partial \le 2^{(t+1)} - 2. \end{cases} \tag{4}$$

After comparing the relationship of $\mathscr{C}\mathscr{P}_1$ and $\mathscr{C}\mathscr{P}_2$ in CSP, CSP returns the relevant result to AU. Next AU chooses either $\mathscr{C}\mathscr{P}_1$ or $\mathscr{C}\mathscr{P}_2$ to compare with next ciphertext

$\mathscr{CP}_3$ in CSP. The abovementioned process will not stop until $\mathscr{CP}_w$ is compared and then the AU outputs the highest bid. Besides, the process of bidding comparison is shown in Fig. 4 (b).

Winner Opening(I_i,$\mathscr{CP}_i$): After passing the above comparison steps, AU publishes $\mathscr{TK}_i$ of the highest bid on the bulletin board. The bidder who claims that she is the exact winner should send her bid to AU as the winning bid and her ciphertext as her proof. Next, AU checks whether the bidder is the winner or not through the I_i in ciphertexts $\mathscr{CP}_i$. If the bidder is verified, AU publishes the winner's bid on the bulletin board. At this time, if there is at least one honest bidder, the winner cannot cheat by acclaiming a relatively smaller bid.

6. SECURITY AND PERFORMANCE ANALYSIS

In this section, we first give the formal security analysis of EFSA system with the following theorems, then demonstrate its performance in terms of theoretical and practical costs.

6.1 Security Analysis

As for EFSA system, EFSA system can ensure that bids will not be revealed in the comparison process of EFSA system and no one can forge the winning identity, and the winner cannot change the winning bid.

Theorem 1 Bids of bidders will not be revealed in the comparison process of EFSA system.

Proof 1 *We denote that $\mathscr{CP}$ and $\mathscr{CP}^*$ are generated from bid and bid*, respectively.*

$$bid = \sum_{0\leq i\leq n-1} b_i 2^i = \sum_{0\leq i\leq m-1} B_i (2^t)^i ; bid^* = \sum_{0\leq i\leq n-1} \beta_i 2^i = \sum_{0\leq i\leq m-1} B_i' (2^t)^i,$$

where t is the window size, $m = n/t$ denotes the number of blocks via utilizing sliding window technology.

Bids can be regarded as bid $= (b_{m-1}, \ldots, b_1, b_0)$. The token and the ciphertext of the bid can be represented by $\mathscr{TK} = (d_0, d_1, \ldots, d_{m-1})$ and $\mathscr{CP} = (I, (f_0, f_1, \ldots, f_{m-1}))$, where

$$d_j = H_1(\mathscr{MSK}, B_m, \ldots, B_j), j = 1, 2, \ldots, m;$$

$$f_j = H_3(d_{j+1}, I) + H_2(\mathscr{MSK}, d_{j+1}) + B_j \mod (2^{(t+1)} - 1)(j = m-1, \ldots, 0).$$

Note that the master key $\mathscr{MSK}$ is unknown to AU. Thus, due to the fact that AU cannot generate a correct and valid token, AU cannot test the bids with other values. Besides, AU knows the first difference of two bids which can mean that the difference of two bids is less than 2^j. If AU continues comparable operations, AU cannot obtain any knowledge about bids. In the comparison phase, AU computes ∂ as follows: set j from $m-1$ to 0, if $\forall k, j < k \leq m-1$,

$$\partial = f_{1,j} - f_{2,j} - H_3(d_{1,j+1}, I) + H_3(d_{2,j+1}, I') \bmod (2^{(t+1)} - 1).$$

If $\partial \neq 0$, it means that j is the first different block.

If AU keeps on comparing with the rest of the information, we can have $d_{j+1} = d'_{j+1}$ and $d_j \neq d'_j$, which means

$$\begin{aligned}
c_j =& f_j - f'_j - H_3(d_{j+1}, I) + H_3(d_{j+1}, I') \mod (2^{(t+1)} - 1)\\
=& (f_j - H_3(d_{j+1}, I)) - (f'_j - H_3(d_{j+1}, I')) \mod (2^{(t+1)} - 1)\\
=& (H_3(d_{j+1}, I) + H_2(\mathscr{MSK}, d_{j+1}) + B_j - H_3(d_{j+1}, I)) -\\
& (H_3(d_{j'+1}, I) + H_2(\mathscr{MSK}, d_{j'+1}) + B'_j - H_3(d_{j+1}, I')) \mod (2^{(t+1)} - 1)\\
\neq& B_j - B'_j \mod (2^{(t+1)} - 1).
\end{aligned}$$

Therefore, AU stops doing any further comparison.

Besides, to guarantee the correctness of EFSA system, EFSA system should satisfy the following theorem.

Theorem 2 The winning identity cannot be forged by bidders, and the winning bid cannot be changed by the winner in EFSA scheme.

Proof 2 *Once receiving the information that any bidder other than the winner says that he/she is the winner in EFSA scheme, he/she should produce the same ciphertext which is corresponding to winning bid. On account of having no information of random value I and $H_i(.), (i = 1, 2, 3)$ which is the non-collision hash function, we deem that the probability of $H_i(I) = H_i(I')$ is negligible in EFSA scheme.*

In addition, if the winner can transform the winning bid of the bidder, he/she should generate a valid and correct ciphertext. The ciphertext should be less than the winning bid and more than other bids. Unfortunately, since $H_i(.), (i = 1, 2, 3)$ is the non-collision hash function, it is impossible to generate the ciphertext and the random value equals the winning proof $H_i(I||f_0||f_1||\ldots||f_{m-1}), (i = 1, 2, 3)$.

In order to guarantee the security of EFSA system, EFSA system should satisfy the following theorem.

Theorem 3 EFSA scheme is weakly indistinguishable if H_1, H_2 and H_3 are pseudorandom functions [10].

Proof 3 *it is worth noticing that challengers are $\mathscr{C}, \mathscr{C}_A$ and $\mathscr{C}_B$. Assume that adversary $\mathscr{A}$ participates weak distinguishing game which can be satisfied with the following equation $Adv^1 1_{\{\mathscr{C},\mathscr{A}\}} := |Pr(Exp^k_{\{\mathscr{C},\mathscr{A}\}} = 0) - Pr(Exp^k_{\{\mathscr{C},\mathscr{A}\}} = 1)| \geq \varepsilon$. Since Hash function is distinguishable from the random function, it is against the assumption that Hash functions are pseudorandom. Especially, we consider a sequence of games by challengers $\mathscr{C}, \mathscr{C}_A$, and $\mathscr{C}_B$, which refers to reference [36].*

From SCE scheme [36], we know the fact that $|Adv^1 1_{\{\mathscr{C},\mathscr{A}\}} - Adv^1 1_{\{\mathscr{C}_B,\mathscr{A}\}}| < \varepsilon$ as long as Hash functions are pseudorandom and $Adv^1 1_{\{\mathscr{C}_B,\mathscr{A}\}} = 0$. This completes the proof of $Adv^1 1_{\{\mathscr{C},\mathscr{A}\}} < \varepsilon$ and Theorem 3 is proved.

6.2 Performance Analysis

As for the performance analysis of EFSA system, we mainly present its theoretical and actual performance by comparing with Zhu's scheme [11]. Note that we assume the i-th bid without using sliding window method can be written by $bid = \sum_{0\leq i\leq n-1} b_i 2^i$ and the i-th bid with using sliding window method can be written by $bid = \sum_{0\leq i\leq m-1} B_i(2^t)^i$. Furthermore, EFSA scheme has fewer computational costs than Zhu's scheme in auction system, which is shown in Table 3. The L bit of bids $bid_1 = (\beta_0, \ldots, \beta_{m-1})$ and $bid_2 = (\gamma_0, \ldots, \gamma_{m-1})$ can be represented by L with satisfying $(\beta_L, \ldots, \beta_{m-1}) = (\gamma_L, \ldots, \gamma_{m-1}), \beta_{L-1} < \gamma_{L-1}$ for two bids. For the whole comparison, we randomly choose k and n, where $k = 160$ bits, n and m vary from 32 bits to 1024 bits in experimental simulations. Experimental tests are conducted for 100 times.

Table 3. Comparison of computational cost in various schemes.

Computational cost	EFSA scheme	Zhu's scheme [11]
Encryption cost	$3m \cdot a$	$(4n+1) \cdot a$
Comparison cost	$(m-L+1) \cdot a$	$(n-L+2) \cdot a$

Table 4. Comparison of storage cost in various schemes.

Scheme	ciphertext length	token length
Zhu's scheme [11]	$(n+1) \cdot k + 2n$	$(n+1) \cdot k$
EFSA scheme	$m \cdot k$	$k + (ln(2^{t+1}-1)/ln(t+1)) \cdot m$

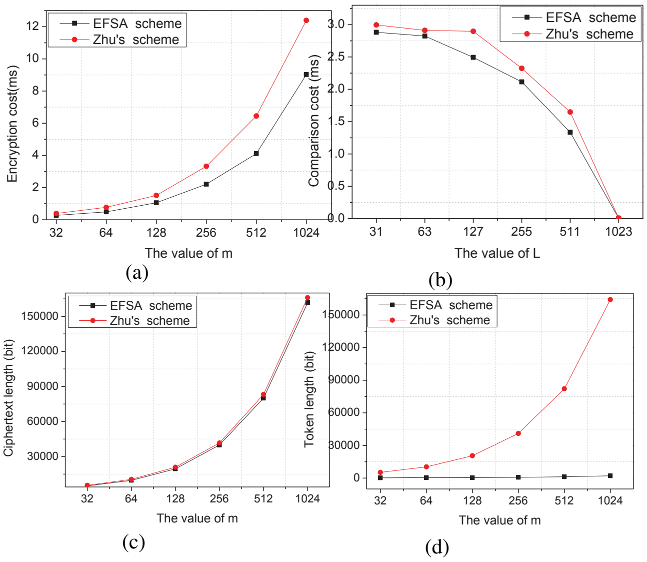
With regard to theoretical analysis, we first compute the computational cost in Table 3, where m, n, a are defined as sliding widow numbers of bid, original widow numbers of bid, hash operations, respectively. We just only consider several time-consuming operations, such as exponentiation operation "E", $Hash_i, (i = 1, \ldots, 5)$ operations. Hence, compared with Zhu's scheme [11], EFSA scheme can further reduce bidder's computational burden.

Besides, we present storage costs of various schemes in Table 4, where m, n, k are defined as sliding widow numbers of bid, original widow numbers of bid, output bits of hash operations, respectively. With the same reason shown in Table 3, EFSA system still outperforms Zhu's scheme in terms of storage costs in different algorithms.

As for the actual performance analysis, we conduct experimental simulations on an Ubuntu Server 15.04 with Intel Core i5 Processor 2.3 GHz by using C and Paring Based Cryptography (PBC) Library. In Fig. 5, we show the actual performance of encryption costs and comparison costs in different schemes(*i.e.*, EFSA scheme, Zhu' scheme [11]). As for the encryption costs and comparison costs of two schemes, EFSA scheme has less computational burden than Zhu's scheme. This is because EFSA scheme utilizes sliding window method. The theoretical costs of two schemes are $3ma$, $4(n+1)a$, $(m-L+1)a$, $(n-L+2)a$, respectively. Note that we test the performance of EFSA scheme by setting $n = m$. For instance, when setting $m = n = 512$, EFSA system takes 4.112 ms to generate ciphertext, while Zhu's scheme takes 6.447 ms to conduct that same operations in Fig. 5 (a). In Fig. 5 (b), we set $m = n = 1024$ and varies L from 31 bits to 1023 bits.

For example, when setting $L = 255$, EFSA system takes 2.115 ms to fulfill comparison operation, while Zhu's scheme takes 2.325ms to conduct that same operations. Although the time of fulfill comparable operation in EFSA scheme is approximately as same as that of Zhu's scheme, the advantage of EFSA scheme is obvious when we set $n = t \cdot m, (t > 1)$. Hence, the result shows that EFSA scheme has less computational burden than Zhu's scheme in practice applications, where $n = t \cdot m, (t > 1)$. Aboveall, EFSA scheme outperforms Zhu's scheme in term of computational overhead.

In Fig. 5, we show the storage overhead of ciphertext length and token length in above two schemes. As for ciphertext length and token length of two schemes, EFSA scheme has less storage burden than Zhu's scheme. This is because EFSA scheme utilizes sliding window method. Moreover, $(f_0, f_1, \ldots, f_{m-1})$ can be encoded into F_t to reduce storage space. The ciphertext length and the token length of two schemes are $(n+1) \cdot k + 2n$,mk,$(n+1)k$,$k + (ln(2^{t+1} - 1)/ln(t+1)) \cdot m$, respectively. Note that we set $n = m$ to test the performance of EFSA scheme. For instance, when setting $m = n = 128$, the ciphertext length of EFSA system are 19474 bits, while the ciphertext length of Zhu's scheme are 20904 bits to conduct that same operation in Fig. 5 (c). Although the time of fulfilling comparable operation in EFSA scheme is approximately as same as that of Zhu's scheme, the advantage of EFSA scheme is obvious when we set $n = t \cdot m, (t > 1)$. In Fig. 5 (d), we set that $m = n$ varing from 32 bits to 10243 bits. For example, when setting $m = n = 256$, the token length of EFSA system are 685 bits and the token length of Zhu's scheme are 41123 bits to conduct the same operations. Hence, the result shows that EFSA scheme has less storage cost on condition that $n = m$ and EFSA scheme has lower storage overhead than Zhu's scheme in practice applications where $n = t \cdot m, (t > 1)$. Above all, EFSA scheme not only has better performance but also can gain a broad range of applications in practice.



(a) (b)

(c) (d)

Fig. 5. (a) Encryption costs; (b) Comparison costs; (c) Ciphertext length; (d) Token length.

To lighten the computational and storage burden of bidders in electronic auction, we devise EFSA scheme based on sliding window method and multilinear maps. As for the obvious results, we just analyze the actual computational and storage overhead of our scheme by comparing with Zhu's scheme. Actual performances assessment of the above schemes are completely in accord with the theoretical analysis shown in Table 3 and Table 4. Compared with Zhu's scheme, EFSA scheme does not incur much computational and storage overhead on bidders in auction system. Hence, EFSA system is much more efficient than Zhu's scheme in practice applications.

7. CONCLUDING REMARKS

In this paper, we proposed an EFSA scheme for resource-limited bidders in auction environment. On the one hand, the basic EFSA system could largely relieve the computational and storage burden without leaking sensitive information of bidders; on the other hand, EFSA system only needed one-round communication. Furthermore, empirical experiments utilizing a real-world environment demonstrated the efficiency and feasibility of EFSA system. As a part of our future work, we will concentrate on expressive search and further improve the efficiency and feasibility in order to gain a broad range of applications in practice.

REFERENCES

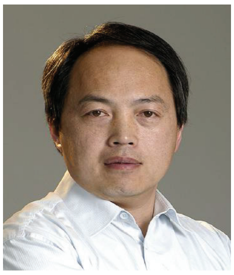
1. Y. Miao, J. Ma, X. Liu, X. Li, Q. Jiang, and J. Zhang, "Attribute-based keyword search over hierarchical data in cloud computing," *IEEE Transactions on Services Computing*, Vol. 13, 2020, pp. 985-998.
2. D. Wu, Z. Feng, H. Wang, and R. Wang, "Security-oriented opportunistic data forwarding in mobile social networks," *Future Generation Computer Systems*, Vol. 87, 2018, pp. 803-815.
3. Z. Guo, Y. Fu, and C. Cao, "Secure first-price sealed-bid auction scheme," *EURASIP Journal on Information Security*, Vol. 2017, 2017, p. 16.
4. Y. Miao, J. Ma, X. Liu, X. Li, Z. Liu, and H. Li, "Practical attribute-based multi-keyword search scheme in mobile crowdsourcing," *IEEE Internet of Things Journal*, Vol. 5, 2018, pp. 3008-3018.
5. D. Wu, Q. Liu, H. Wang, D. Wu, and R. Wang, "Socially aware energy-efficient mobile edge collaboration for video distribution," *IEEE Transactions on Multimedia*, Vol. 19, 2017, pp. 2197-2209.
6. G. Zhou, J. Wu, C. Long, G. Jiang, and S. K. Lam, "Efficient three-stage auction schemes for cloudlets deployment in wireless access network," *Wireless Networks*, Vol. 25, 2019, pp. 3335-3349.
7. V. K. Singh, S. Mukhopadhyay, and F. Xhafa, "Hire the experts: Combinatorial auction based scheme for experts selection in e-healthcare," *arXiv*, 2018, arXiv:1801.04544.

8. Y. Jiao, W. Ping, D. Niyato, and K. Suankaewmanee, "Auction mechanisms in cloud/fog computing resource allocation for public blockchain networks," *IEEE Transactions on Parallel and Distributed Systems*, Vol. 30, 2019, pp. 1975-1989.
9. P. Chen, J. Ye, and X. Chen, "A new efficient request-based comparable encryption scheme," in *Advanced Information Networking and Applications Workshops*, 2015, pp. 436-439.
10. Q. Meng, J. Ma, K. Chen, Y. Miao, and T. Yang, "Comparable encryption scheme over encrypted cloud data in internet of everything," *Security and Communication Networks*, Vol. 2017, 2017, pp. 1-11.
11. Y. Zhu, L. Liu, and X. Chen, "Efficient first-price sealed-bid auction protocols from modified comparable encryption," in *Proceedings of International Conference on Broadband and Wireless Computing, Communication and Applications*, 2015, pp. 417-421.
12. Y. Miao, J. Ma, X. Liu, J. Weng, H. Li, and H. Li, "Lightweight fine-grained search over encrypted data in fog computing," *IEEE Transactions on Services Computing*, Vol. 12, 2019, pp. 772-785.
13. D. Wu, S. Si, S. Wu, and R. Wang, "Dynamic trust relationships aware data privacy protection in mobile crowd-sensing," *IEEE Internet of Things Journal*, Vol. 5, 2018, pp. 2958-2970.
14. Y. Miao, X. Liu, R. H. Deng, H. Wu, H. Li, J. Li, and D. Wu, "Hybrid keyword-field search with efficient key management for industrial internet of things," *IEEE Transactions on Industrial Informatics*, Vol. 15, 2019, pp. 3206-3217.
15. A. C.-C. Yao, "How to generate and exchange secrets," in *Foundations of Computer Science*, Vol. 10, 1986, pp. 162-167.
16. C. Mavroforakis, N. Chenette, A. O'Neill, G. Kollios, and R. Canetti, "Modular order-preserving encryption, revisited," in *Proceedings of Annual ACM International Conference on Management of Data*, 2015, pp. 763-777.
17. Z. Liu, X. Chen, J. Yang, C. Jia, and I. You, "New order preserving encryption model for outsourced databases in cloud environments," *Journal of Network and Computer Applications*, Vol. 59, 2016, pp. 198-207.
18. J. Furukawa, "Request-based comparable encryption," in *European Symposium on Research in Computer Security*, 2013, pp. 129-146.
19. A. C.-C. Yao, "An n-to-1 bidder reduction for multi-item auctions and its applications," in *Proceedings of Annual ACM Symposium on Discrete Algorithms*, 2014, pp. 92-109.
20. M. Budde and S. Minner, "First-and second-price sealed-bid auctions applied to push and pull supply contracts," *European Journal of Operational Research*, Vol. 237, 2014, pp. 370-382.
21. N. Chen, N. Gravin, and P. Lu, "Optimal competitive auctions," in *Proceedings of Annual ACM symposium on Theory of computing (STOC'14)*, 2014, pp. 253-262.
22. Y. F. Chung, K. H. Huang, H. H. Lee, F. Lai, and T. S. Chen, "Bidder-anonymous english auction scheme with privacy and public verifiability," *Journal of Systems and Software*, Vol. 81, 2008, pp. 113-119.
23. L. Pham, J. Teich, H. Wallenius, and J. Wallenius, "Multi-attribute online reverse auctions: Recent research trends," *European Journal of Operational Research*, Vol. 242, 2015, pp. 1-9.

24. O. Baudron and J. Stern, "Non-interactive private auctions," in *Proceedings of International Conference on Financial Cryptography*, Vol. 2339, 2001, pp. 364-377.
25. X. Wang, Y. Ji, H. Zhou, Z. Liu, Y. Gu, and J. Li, "A privacy preserving truthful spectrum auction scheme using homomorphic encryption," in *Proceedings of Global Communications Conference*, 2015, pp. 1-6.
26. K. Peng, C. Boyd, and E. Dawson, "Optimization of electronic first-bid sealed-bid auction based on homomorphic secret sharing," in *Proceedings of International Conference on Cryptology in Malaysia*, 2005, pp. 84-98.
27. M. K. Franklin and M. K. Reiter, "The design and implementation of a secure auction service," *IEEE Transactions on Software Engineering*, Vol. 22, 1996, pp. 302-312.
28. M.-J. Li, J. S.-T. Juan, and J. H.-C. Tsai, "Practical electronic auction scheme with strong anonymity and bidding privacy," *Information Sciences*, Vol. 181, 2011, pp. 2576-2586.
29. F. Brandt and T. Sandholm, "(im) possibility of unconditionally privacy-preserving auctions," in *Proceedings of International Joint Conference on Autonomous Agents and Multiagent Systems*, 2004, pp. 810-817.
30. F. Brandt, "On the existence of unconditionally privacy-preserving auction protocols," *ACM Transactions on Information and System Security*, Vol. 11, 2008, p. 6.
31. S. Garg, C. Gentry, and S. Halevi, "Candidate multilinear maps from ideal lattices," in *Proceedings of International Conference on the Theory and Applications of Cryptographic Techniques*, 2013, pp. 1-17.
32. F. Brandt, "How to obtain full privacy in auctions," *International Journal of Information Security*, Vol. 5, 2006, pp. 201-216.
33. M. Nojoumian and D. R. Stinson, "Efficient sealed-bid auction protocols using verifiable secret sharing," in *Proceedings of International Conference on Information Security Practice and Experience*, 2014, pp. 302-317.
34. D. C. Parkes, M. O. Rabin, S. M. Shieber, and C. A. Thorpe, "Practical secrecy-preserving, verifiably correct and trustworthy auctions," in *Proceedings of International Conference on Electronic Commerce*, 2006, pp. 70-81.
35. Ç. K. Koç, "Analysis of sliding window techniques for exponentiation," *Computers & Mathematics with Applications*, Vol. 30, 1995, pp. 17-24.
36. J. Furukawa, "Short comparable encryption," in *Proceedings of International Conference on Cryptology and Network Security*, 2014, pp. 337-352.

Qian Meng received the M.S. degree with School of Science from Hangzhou Normal University, Hangzhou, China, in 2016. She is currently pursuing the Ph.D. degree with the Department of Telecommunication Engineering in Xidian University, Xi'an, China. Her research interests include information security and applied cryptography.

Jian-Feng Ma received the B.S. and M.S. degrees in Department of Mathematics from Shaanxi Normal University in 1985 and in Department of Computer Science from Xidian University in 1988, respectively, and the Ph.D. degree in Computer Software and Telecommunication Engineering from Xidian University, Xi'an, China, in 1995. From 1999 to 2001, he was a Research Fellow with Nanyang Technological University of Singapore. He is currently a Professor with the Department of Computer Science and Technology, Xidian University, Xi'an, China. His current research interests include information and network security, wireless and mobile computing systems, and compute networks.



Ke-Fei Chen received B.S. degree, M.S. degree from Xidian University in 1982, 1985, and Ph.D. degree from Justus Liebig University Giessen, Germany in 1994. His main research areas include cryptography, theory and technology of network security. He is currently a Professor at School of Science, Hangzhou Normal University.

Yin-Bin Miao received the B.S. degree with Department of Telecommunication Engineering from Jilin University, Changchun, China, in 2011, and Ph.D. degree with Department of Telecommunication Engineering from Xidian University, Xi'an, China, in 2016. He is currently a Lecturer with Department of Cyber Engineering in Xidian University, Xi'an, China. His research interests include information security and applied cryptography.

Teng-Fei Yang received the M.S. degree with School of Physics and Information Technology from Shaanxi Normal University, Xi'an, China, in 2016, He is currently pursuing the Ph.D. degree with School of Cyber Engineering in Xidian University, Xi'an, China. His research interests include multimedia security and applied cryptography.