EMRQ: An Efficient Multi-keyword Range Query Scheme in Smart Grid Auction Market

Hongwei Li [1], Yi Yang [1], Mi Wen [2], Hongwei Luo [3], and Rongxing Lu [4]
[1] School of Computer Science & Engineering, UESTC
Chengdu, 610054 - China
[e-mail: hongwei.uestc@gmail.com, yangyi.buku@gmail.com]
[2] College of Computer Science and Technology, Shanghai University of Electric Power
Shanghai, 200090 - China
[e-mail: miwen@shiep.edu.cn]
[3] China Academy of Telecom Research, MIIT
Beijing, 100191 - China
[e-mail: luohongwei@chinattl.com]
[4] School of Electrical and Electronics Engineering, Nanyang Technological University
639798 - Singapore
[e-mail: rxlu@ntu.edu.sg]
*Corresponding author: Hongwei Li

Received August 11, 2014; revised September 11, 2014; accepted September 18, 2014; published November 30, 2014

Abstract

With the increasing electricity consumption and the wide application of renewable energy sources, energy auction attracts a lot of attention due to its economic benefits. Many schemes have been proposed to support energy auction in smart grid. However, few of them can achieve range query, ranked search and personalized search. In this paper, we propose an efficient multi-keyword range query (EMRQ) scheme, which can support range query, ranked search and personalized search simultaneously. Based on the homomorphic Paillier cryptosystem, we use two super-increasing sequences to aggregate multidimensional keywords. The first one is used to aggregate one buyer's or seller's multidimensional keywords to an aggregated number. The second one is used to create a summary number by aggregating the aggregated numbers of all sellers. As a result, the comparison between the keywords of all sellers and those of one buyer can be achieved with only one calculation. Security analysis demonstrates that EMRQ can achieve confidentiality of keywords, authentication, data integrity and query privacy. Extensive experiments show that EMRQ is more efficient compared with the scheme in [3] in terms of computation and communication overhead.

Keywords: Smart grid, energy auction, range query, multi-keyword

This manuscript is an extended version based on a conference paper published in ICC 2014 (Sydney, Australia, June 9-14, 2014.) This work is supported by the National Natural Science Foundation of China under Grants 61472065, 61350110238, 61103207, U1233108, U1333127, and 61272525, the International Science and Technology Cooperation and Exchange Program of Sichuan Province, China under Grant 2014HH0029, and China Postdoctoral Science Foundation funded project under Grant 2014M552336.

http://dx.doi.org/10.3837/tiis.2014.11.015

1. Introduction

Currently, the traditional power grid, due to its inherent limitations, cannot fully satisfy today's swift development trend. As a result, it is restructured and developed to a more intelligent power system named smart grid [1]. The smart grid mainly consists of several parts: generator(s), transmission system operator, distributor(s), retailer(s) and aggregator(s). Many technologies have been introduced into smart grid to ensure availability and economic benefits [2,3]. For instance, energy auction market introduces commercial auctions to the smart grid, where energy sellers publish their auction information, and then energy buyers bid for appropriate energy supplies. Thus, the energy auction market can adjust energy prices and provide strong support for the practical application of smart grid [4].

Though energy auction is promising, security and privacy are seriously challenged in energy auction market. Firstly, due to the confidentiality of auction information, privacy preservation is extremely important [5,6]. One solution is to introduce encrypted keyword search to smart grid, which enables the keyword search over encrypted data. But the existing encrypted keyword search schemes in smart grid auction market (e.g., [3]) cannot achieve range query of keywords, which is extremely useful in smart grid [7]. For example, with the range of price keyword, energy buyers can filter out the energy with reasonable price. In addition, the existing range query scheme in smart grid [7] cannot be directly applied to auction market, and also cannot achieve the ranked search among multidimensional keywords.

In this paper, aim at addressing the above challenges, we propose an efficient multi-keyword range query (EMRQ) scheme in smart grid auction market. The proposed scheme focuses on providing secure and efficient transactions between sellers and buyers, and supports range query, ranked search, personalized search and efficient aggregation at the same time.

Our Contributions. The contributions of this paper are twofold:

- Firstly, we propose a novel EMRQ scheme to achieve searchable encryption which not only compares whether the keywords are equal, but also accurately calculates the difference between multidimensional keywords and further achieves range query, ranked search and personalized search. Security analysis demonstrates that the EMRQ scheme can achieve confidentiality of keywords, authentication, data integrity and query privacy.
- Secondly, based on the two super-increasing sequences, the proposed scheme can compare the multidimensional keywords of one buyer with those of all sellers with only one calculation, thereby greatly reducing the computation and communication overhead. We compare EMRQ with the existing auction scheme in [3] to show its efficiency.

Compared with the preliminary conference version [1] of this paper, this journal version studies the fine-grained weight strategy to provide personalized search for buyers. Moreover, the privacy-preservation of buyers is enhanced to ensure an adversary cannot get any privacy information about the bid auction. In addition, we improve the experimental works by adding the analysis and evaluation of the new scheme.

Organization. The remainder of the paper is organized as follows: In Section 2, the network model and security requirements are formalized. We present the notation and recall Paillier cryptosystem in Section 3. In Section 4, we propose the EMRQ scheme. We analyze the

security of our scheme in Section 5, and evaluate its performance in Section 6. In Section 7, we present related works. Finally, we conclude this paper in Section 8.

2. NETWORK MODEL AND SECURITY REQUIREMENTS

In this section, we will formalize the network model, security requirements and design goals.

2.1 Network Model

In our network model, we focus on how to secretly compare keyword tags and trapdoors generated by the sellers and buyers, respectively. Specifically, we consider that our system consists of four parts, as shown in **Fig. 1**.

- **Electricity generators (sellers):** Sellers generate energy and sell it to retailers. For efficient search, they generate the search tags according to their auction keywords, and then send them to data center.
- **Retailers (buyers):** Buyers should provide energy to their own energy consumers. For economic purposes, they generate keyword trapdoors to bid the energy and send them to data center.
- **Data Center (DC):** Data center in our scheme is used as a database, it stores all tags and auction messages from sellers. If one buyer computes a trapdoor to bid some auction messages, DC will compare the trapdoor with all tags through homomorphic computing. Then, DC sends the result to filtering center.
- **Filtering Center (FC):** Filtering center is a trusted operation center which may be a supercomputer. It initiates our whole system at the beginning of energy auction. And after the comparison in DC, FC firstly filters auction keyword tags and then selects ranked results to the buyers.

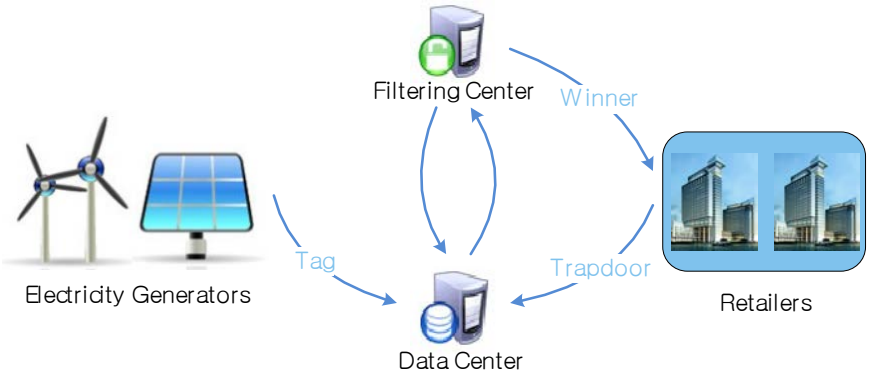

Fig. 1. Network model for smart auction market

2.2 Security Requirements

In our scheme, we assume all entities are untrustworthy except FC. An adversary *A* can intrude in smart grid and eavesdrop or modify the messages with private information. Specifically, we define security requirements as follows.

- **Confidentiality of keywords:** All keywords generated by sellers and buyers should be sent to DC for comparing and filtering. These keywords are usually trade secrets. Hence, it is necessary to guarantee the confidentiality of keywords even though the adversary *A* eavesdrops the communication links or DC's database.

- **Authentication and data integrity:** In the system, legitimate users should be authenticated and the messages altered or fabricated by the adversary A should be detected.
- **Query privacy:** When the range query contains sensitive information, e.g., $1.2 < price < 1.5$, it is indispensable to hide it. We should ensure that our scheme can achieve range query without any privacy disclosure.

2.3 Design Goals

In order to realize the auction messages filtering in our scheme, our design goals are to develop an efficient fine-grained keywords comparison with privacy preservation.

- **Security is indispensable in the proposed scheme:** If the auction market in smart grid doesn't consider the security, it cannot be used in practice. Hence, we should guarantee confidentiality of keywords, authentication and data integrity, and range query.
- **Computation and communication efficiency should be achieved in the proposed scheme:** Compared with other auction schemes, our scheme should be more efficient in terms of computation and communication overhead.
- **Keywords comparison should be fine-grained in the proposed scheme:** General schemes can only compare whether the keywords are equal. However, the difference of keywords computing will be very useful in the energy auction market. Thus, our scheme should achieve this goal.

3. Notations and Preliminaries

In this subsection, we introduce notations (**Table 1**) used throughout the remainder of this paper and review Bilinear Pairing and Paillier Cryptosystem.

3.1 Notations

Table 1. Notations

	Meaning
ID_*	the identity of entity $*$.
$m_{i,k}/m_{j,k}$	the k-th dimension keyword of $seller_i/buyer_j$'s keywords, $k \leq l$ (i.e., there are totally l types of keywords).
C_i/C'_j	the ciphertext of $seller_i/buyer_j$'s keywords.
$\vec{a}, \vec{b}$	two super-increasing sequences.
$dif_{i,j,k}$	the difference of the k-th dimension keywords between $seller_i$ and $buyer_j$.
$\boldsymbol{\mathcal{R}}$	the filtering rule sequence, denoted as a set of l rules $\boldsymbol{\mathcal{R}} = (R_1, R_2, \dots, R_l)$
$\boldsymbol{\mathcal{W}}$	the keyword weight sequence,, denoted as a set of l weights $\boldsymbol{\mathcal{W}} = (W_1, W_2, \dots, W_l)$

3.2 Bilinear Pairing

Let G_1 and G_2 be two cyclic groups of prime order q, and P be a generator of group G_1. There must exist a non-degenerated, efficiently computable bilinear map ê: $G_1 \times G_1 \to G_2$ such that $\hat{e}(P,P) \neq 1_{G_2}$. And for all $P_1, P_2 \in G_1$ and all $a, b \in \mathbb{Z}_q^*$, we have $\hat{e}(aP_1, bP_2) = \hat{e}(P_1, P_2)^{ab}$. We refer to [12] for a more comprehensive description of pairing technique, and complexity assumptions.

3.3 Paillier Cryptosystem

The Paillier cryptosystem consists of three phases as follows (refer to [9]):

- **Setup:** Given the security parameter κ_1, two large prime numbers p_1, q_1 can be chosen, where $|p_1| = |q_1| = \kappa_1$. Then calculate the RSA modulus $n = p_1 q_1$ and $\lambda = lcm(p_1 - 1, q_1 - 1)$. Define $L(u) = \frac{u-1}{n}$, and choose a generator $g \in \mathbb{Z}_{n^2}^*$. And then compute $\mu = (L(g^\lambda \bmod n^2))^{-1} \bmod n$. After that, the public key is $pk = (n, g)$, and the private key is $sk = (\lambda, \mu)$.
- **Encryption:** Given a message $\mathrm{m} \in \mathbb{Z}_\mathrm{n}$, choose a random number $\mathrm{r}_0 \in \mathbb{Z}_\mathrm{n}^*$, the ciphertext is $\mathrm{c} = \mathrm{E(m)} = \mathrm{g^m} \cdot \mathrm{r_0{}^n} \bmod \mathrm{n^2}$.
- **Decryption:** The message m can be recovered as $m = D(c) = L(c^{\lambda \bmod n^2}) \cdot \mu$, where c is the ciphertext.

4. Proposed Scheme

In this section, we propose the EMRQ scheme, which mainly consists of the following four phases: system initialization, auction message creating, trapdoor aggregating and filtering.

4.1 System Initialization

Firstly, FC computes the Paillier cryptosystem's public key (n, g), and the corresponding private key (λ, μ). Considering the multidimensional keywords of auction information, we expect that all keywords (price, quantity and location, etc.) can be aggregated to one number and the difference of all keywords can be gained by only one comparison. Therefore, we transform each dimension keyword to a positive integer. Assume that for $seller_i$, there are totally l types of auction keywords $(m_{i,1}, m_{i,2}, \cdots, m_{i,l})$ $(m_{i,j} \in \mathbb{Z}_n)$, and the value of each type $m_{i,j}$ $(j = 1,2, \cdots, l)$ is less than a constant d. Then, FC chooses a super-increasing sequence $\vec{\boldsymbol{a}} = (a_1, a_2, \cdots, a_l)$, where $a_1, a_2, \cdots, a_l$ are integers, $a_1 = 1$ and $\sum_{j=1}^{i-1} a_j \cdot d < a_i/2$ for $(i = 2, \cdots, l)$. The reason why we choose $a_i/2$ will be described in Section 4.4. Then, FC computes $(g_1, g_2, \cdots, g_l)$, where $g_i = g^{a_i}$ $(i = 1,2, \cdots, l)$.

Then we define $seller_i$'s aggregated number of multidimensional keywords is no more than a constant D, e.g., $\sum_{j=1}^{l} a_j \cdot d < D$, and FC further chooses another super-increasing sequence $\vec{\boldsymbol{b}} = (b_1, b_2, \cdots, b_I)$ (I is the number of $sellers$), where $b_1 = 1$ and $\sum_{j=1}^{i-1} b_j \cdot D < b_i/2$. The reason why we choose $b_i/2$ will also be described in Section 4.4.

For identity-based signature, we also choose master key $s \in \mathbb{Z}_q^*$, and the associated public key $P_{pub} = sP$, two hash functions $H_1, H_2: \{0,1\}^* \to G_1$, the privacy of all entities can be generated as $d = sH_1(ID) \in G_1$.

After all, FC publishes the system parameters as

$$\text{pubs} = \{n, g, g_1, g_2, \cdots, g_l, P, P_{pub}, H_1, H_2, \vec{\boldsymbol{b}}\} \tag{1}$$

and keeps the master keys $(\lambda, \mu, \vec{\boldsymbol{a}}, s)$ secretly.

Auction Message Creating

The auction message creating process is shown in Fig. 2.

(1) *Tag creating*

$Seller_i$ selects auction keywords $(m_{i,1}, m_{i,2}, \cdots, m_{i,l})$ according to corresponding auction information, then he chooses a random number $r_i \in \mathbb{Z}_n^*$ and computes his tag:

$$\begin{aligned} C_i &= (g_1^{m_{i,1}} \cdot g_2^{m_{i,2}} \cdot \cdots \cdot g_l^{m_{i,l}} \cdot r_i^n)^{b_i} \bmod n^2 \\ &= g^{(a_1 m_{i,1} + a_2 m_{i,2} + \cdots + a_l m_{i,l}) b_i} \cdot (r_i^{b_i})^n \bmod n^2 \\ &= g^{b_i M_i} \cdot (r_i^{b_i})^n \bmod n^2 \end{aligned} \tag{2}$$

where $M_i = a_1 m_{i,1} + a_2 m_{i,2} + \cdots + a_l m_{i,l}$.

(2) *Delivery*

$Seller_i$ uses identity-based signature algorithm [11] to sign C_i. Firstly, pick $r \overset{R}{\leftarrow} \mathbb{Z}_q^*$, compute $U = rP \in G_1$, then $H = H_2(ID_{S_i}, C_i || TS, U) \in G_1$ (where ID_{S_i} is $seller_i$'s identity) and $V = d_{S_i} + rH \in G_1$. Finally, output the pair: $\sigma = \langle U, V \rangle \in G_1 \times G_1$.

Therefore, the signed message can be generated as $msg_{seller_i \to DC} = (C_i || ID_{S_i} || TS || \sigma)$ (TS is the current timestamp) and it will be sent to DC.

(3) *All sellers' tags aggregation*

DC verifies all $sellers$' tags as follows: with $\sigma = \langle U, V \rangle$, compute $H = H_2(ID_{S_i}, C_i || TS, U)$, and then accept it only if $\hat{e}(P, V) = \hat{e}(P_{pub}, H_1(ID_{S_i}))\hat{e}(U, H)$. Then DC computes total tag as $C_{sel} = C_1 \cdot C_2 \cdot \cdots \cdot C_I$, where

$$\begin{aligned} C_{sel} &= C_1 \cdot C_2 \cdot \cdots \cdot C_I \\ &= \prod_{i=1}^{I} (g^{b_i M_i}) \cdot \left(\prod_{i=1}^{I} r_i^{b_i}\right)^n \bmod n^2 \\ &= g^{\sum_{i=1}^{I} b_i M_i} \cdot \left(\prod_{i=1}^{I} r_i^{b_i}\right)^n \bmod n^2 \end{aligned} \tag{3}$$

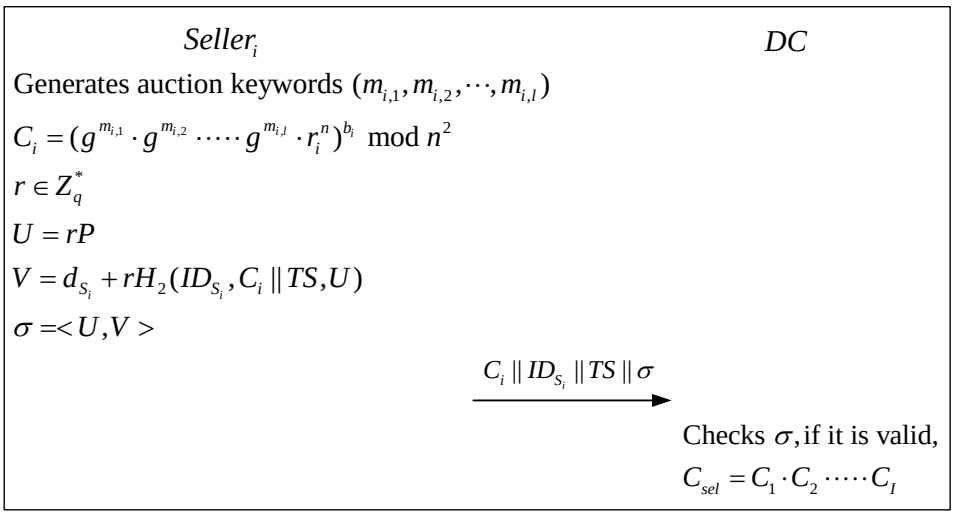

Fig. 2. Auction message creating

Trapdoor aggregating

The trapdoor aggregating process is shown in Fig. 3.

(1) *Trapdoor creation and delivery*

When $buyer_j$ wants to bid the energy, he first generates filtering keywords $(m_{j,1}, m_{j,2}, \cdots, m_{j,l})$ $(0 < m_{j,k} < d, 1 \le k \le l)$ and randomly chooses $r_j \in \mathbb{Z}_n^*$, then computes his trapdoor

$$\begin{aligned} C_i' &= g_1^{-m_{j,1}} \cdot g_2^{-m_{j,2}} \cdot \cdots \cdot g_l^{-m_{j,l}} \cdot r_j^n \bmod n^2 \\ &= g^{-M_j} \cdot r_j^n \bmod n^2 \end{aligned} \tag{4}$$

where $M_j = a_1 m_{j,1} + a_2 m_{j,2} + \cdots + a_l m_{j,l}$. And then $buyer_j$ calculates the total trapdoor as $C_{buy} = {C_j'}^{b_1+b_2+\cdots+b_I}$, where

$$\begin{aligned} C_{buy} &= {C_j'}^{b_1+b_2+\cdots+b_I} \\ &= (g^{-M_j} \cdot r_j^n)^{b_1+b_2+\cdots+b_I} \bmod n^2 \\ &= g^{-\sum_{i=1}^{I} b_i M_j} \cdot \left(\prod_{i=1}^{I} r_j^{b_i} \right)^n \bmod n^2 \end{aligned} \tag{5}$$

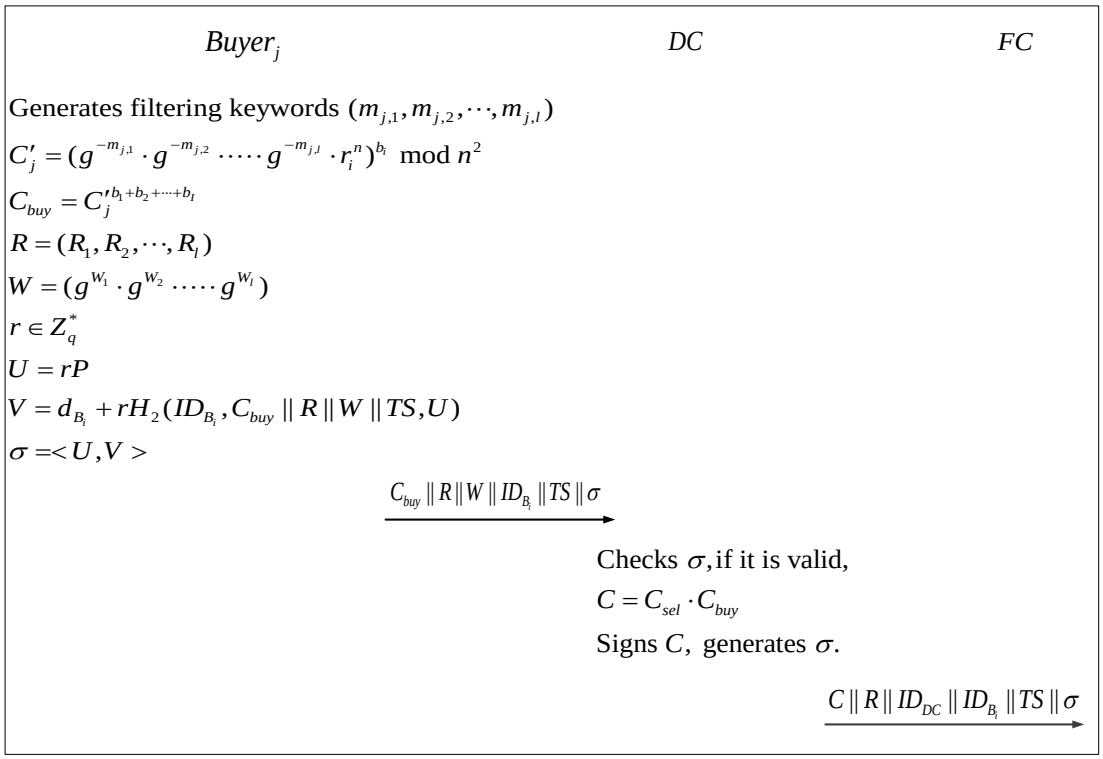

Fig. 3. Trapdoor aggregating

After that, $buyer_j$ generates a matching rule sequence $\boldsymbol{\mathcal{R}} = (R_1, R_2, \ldots, R_l)$. If $buyer_j$ defines the range of auction keyword as $v_1 \le m_{i,k} \le v_2$ $(v_1, v_2 \in \mathbb{Z}_n)$, then R_k should be a pair: $g^{v_1 - m_{j,k}}, g^{v_2 - m_{j,k}}$. Based on the filtering rules, $buyer_j$ can define a keyword weight sequence $(W_1, W_2, \ldots, W_l)$ for all auction keywords $m_{i,k}$ $(k = 1,2,\cdots,l)$, the keyword weight

W_k represents the keyword importance defined by $buyer_j$. The fine-grained weight strategy can provide personalized search for buyers. Speciafically, the weight strategy is as follows:

Weight strategy:

- $Buyer_j$ defines the weight of each keyword, the weights of some important keywords may be larger than those of other keywords. Specially, if $buyer_j$ defines all weights as the same, the more filtering rules that $seller_i$ satisfies, the higher priority $seller_i$ has.
- $Buyer_j$ sorts the keywords in ascending importance, and if $seller_i$ contains a more important keyword compared with other $sellers$, $seller_i$ has higher priority in the returned result. To achieve this goal, a super-increasing sequence $\vec{\boldsymbol{c}} = (c_1, c_2, \cdots, c_l)$ will be generated, where $c_1, c_2, \cdots, c_l \in \mathbb{Z}_n^*$, $c_1 = 1$ and $\sum_{j=1}^{i-1} c_j < c_i$ for $(i = 2, \cdots, l)$. If W_i has the largest keyword weight, $W_i = c_l$. And if W_j has the least keyword weight, $W_j = c_1$. E.g., for a keyword weight sequence $(W_1, W_2, W_3, W_4, W_5)$ and a super-increasing sequence $(1, 3, 5, 10, 20)$, if the keyword weight sequence satisfies $(W_2 > W_4 > W_5 > W_1 > W_3)$, there will be $(W_1, W_2, W_3, W_4, W_5) = (3, 20, 1, 10, 5)$.

Next, the keyword weight sequence can be encrypted as $\boldsymbol{\mathcal{W}} = (g^{W_1}, g^{W_2}, \cdots, g^{W_l})$. Then $buyer_j$ signs $(C_{buy}||\boldsymbol{\mathcal{R}}||\boldsymbol{\mathcal{W}}||TS)$ using the identity-based signature algorithm [11]. The alogrithm is as follow: pick $r \overset{R}{\leftarrow} \mathbb{Z}_q^*$, compute $U = rP \in G_1$, $H = H_2(ID_{B_i}, C_{buy}||\boldsymbol{\mathcal{R}}||\boldsymbol{\mathcal{W}}||TS, U)$ (where ID_{B_j} is $buyer_j$'s identity) and $V = d_{B_j} + rH \in G_1$. Finally, output the pair: $\sigma = \langle U, V \rangle \in G_1 \times G_1$. Then, $buyer_j$ sends the signed message $msg_{buyer_j \to DC} = (C_{buy}||\boldsymbol{\mathcal{R}}||\boldsymbol{\mathcal{W}}||ID_{B_j}||TS||\sigma)$ to DC, and DC accepts it after verifying as$\hat{e}(P, V) = \hat{e}(P_{pub}, H_1(ID_{B_i}))\hat{e}(U, H)$, where $H = H_2(ID_{B_i}, C_{buy}||\boldsymbol{\mathcal{R}}||\boldsymbol{\mathcal{W}}||TS, U)$.

(2) *Homomorphic computing for comparison*

When DC wants to compare $sellers'$ tags with $buyer_j$'s trapdoor. It can compute $C = C_{sel} \cdot C_{buy}$. Then, DC sends the signed message $msg_{DC \to FC} = (C||\boldsymbol{\mathcal{R}}||ID_{DC}||ID_{B_j}||TS||\sigma)$ to FC, where σ is the signature of $(C||\boldsymbol{\mathcal{R}}||ID_{DC}||ID_{B_j}||TS)$ using the identity-based signature algorithm [11].

Filtering

The filtering process is shown in Fig. 4.

(1) *Decrypting the result of comparison*

After receiving the message $(C||\boldsymbol{\mathcal{R}}||ID_{DC}||ID_{B_j}||TS||\sigma)$, check the signature σ using the identity-based signature algorithm [11], if it is valid, FC decrypts C, where C is formed by

$$\begin{aligned} C &= C_{sel} \cdot C_{buy} \\ &= g^{\sum_{i=1}^{I} b_i M_i} \cdot \left(\prod_{i=1}^{I} r_i^{b_i} \right)^n \cdot g^{-\sum_{i=1}^{I} b_i M_j} \cdot \left(\prod_{i=1}^{I} r_j^{b_i} \right)^n \bmod n^2 \\ &= g^{\sum_{i=1}^{I} b_i M_{i,j}} \cdot \left(\prod_{i=1}^{I} (r_i r_j)^{b_i} \right)^n \bmod n^2 \end{aligned} \quad (6)$$

$$= g^{M_{total}} \cdot \left(\prod_{i=1}^{I} (r_i r_j)^{b_i} \right)^n \bmod n^2$$

where $M_{i,j} = M_i - M_j = a_1(m_{i,1} - m_{j,1}) + a_2(m_{i,2} - m_{j,2}) + \cdots + a_l(m_{i,l} - m_{j,l})$ and $M_{total} = \sum_{i=1}^{I} b_i M_{i,j}$. FC uses sk to recover M_{total} as Section 3.3. After that, FC gets $(M_{1,j}, M_{2,j}, \cdots, M_{I,j})$ by running Algorithm 1 with input $\vec{x} = \vec{b}$ and $SUM = M_{total}$.

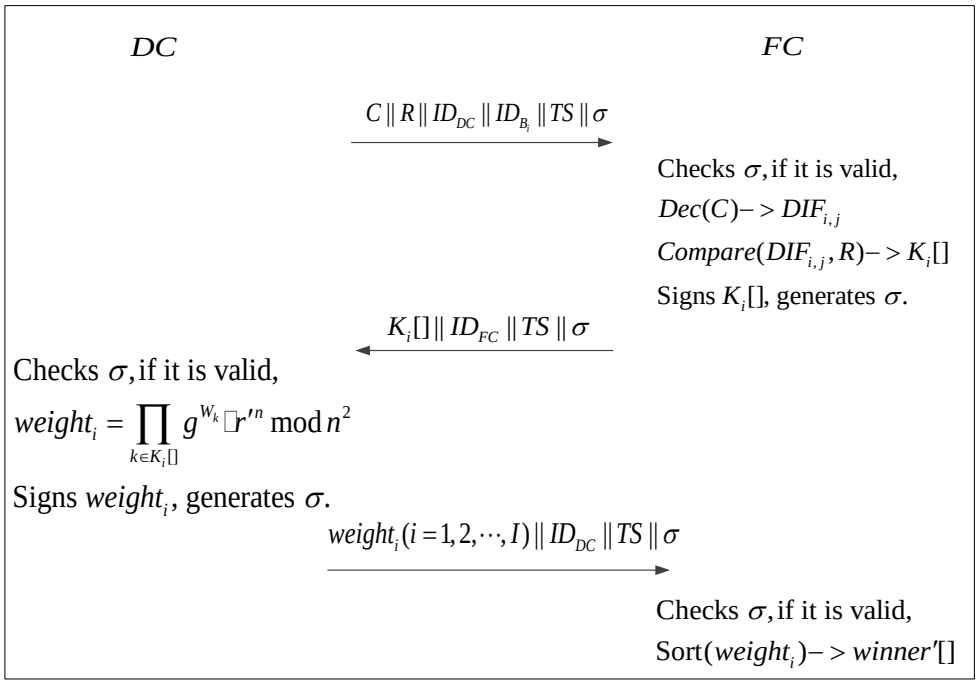

Fig. 4. Filtering

Algorithm 1	split the aggregation
Input:	$\vec{x} = (x_1, x_2, \cdots, x_l)$ and the aggregation SUM
Output:	$(D_1, D_2, \cdots, D_k)$
1:	let $sum_k = SUM$
2:	**for** $i = k$ to 2 **do**
3:	$sum_{i-1} = sum_i \bmod x_i$
4:	**if** $sum_{i-1} > x_i/2$ **then**
5:	$sum_{i-1} = sum_i - x_i$
6:	**end if**
7:	$D_i = (sum_i - sum_{i-1})/x_i$
8:	**end for**
9:	$D_1 = sum_1$
10:	**return** $(D_1, D_2, \cdots, D_k)$

As shown in Algorithm 1, we define $sum_i = b_1 M_{1,j} + b_2 M_{2,j} + \cdots + b_i M_{i,j}$ $(i = 1,2,\cdots,I)$. We compute $sum_{i-1} = sum_i \bmod x_i$, hence we have $0 \le sum_{i-1} \le x_i$. Since we have defined $\sum_{j=1}^{i-1} b_j \cdot D < b_i/2$, we have $-x_i/2 \le sum_{i-1} \le x_i/2$ (for example: $0 <$

$\varepsilon_i, \varepsilon_j < t \Rightarrow -\mathrm{t} < \varepsilon_i - \varepsilon_j < t$). Thus, in Algorithm 1, if the calculated sum_{i-1} is $0 \leq sum_{i-1} \leq x_i/2$, this is the right result; else if $x_i/2 < sum_{i-1} < x_i$, we must correct it as $sum_{i-1} = sum_{i-1} - x_i$, the true result is $-x_i/2 < sum_{i-1} < 0$. That is why we choose $b_i/2$ in $\sum_{j=1}^{i-1} b_j \cdot D < b_i/2$ and $a_i/2$ in $\sum_{j=1}^{i-1} a_j \cdot d < a_i/2$, it can split the aggregation including negative numbers.

After getting $(M_{1,j}, M_{2,j}, \cdots, M_{I,j})$, FC can use Algorithm 1 with input $\vec{\boldsymbol{x}} = \vec{\boldsymbol{a}}$ and $SUM = M_{i,j}$ $(i = 1,2,\cdots,I)$ to gain all differences of the multidimensional keywords $DIF_{i,j} = (dif_{i,j,1}, dif_{i,j,2}, \cdots, dif_{i,j,l})$ between $seller_i$ and $buyer_j$.

(2) *Choosing winners*

With the keyword difference $DIF_{i,j} = (dif_{i,j,1}, dif_{i,j,2}, \cdots, dif_{i,j,l})$ and filtering rules $(R_1, R_2, \ldots, R_l)$, we can achieve range query. If each $dif_{i,j,k}$ $(k = 1,2,\cdots,l)$ satisfies the filtering rule R_k (i.e., $v_1 - m_{j,k} \leq dif_{i,j,k} \leq v_2 - m_{j,k}$), k will be stored in an array $K_i[]$.

After getting the array $K_i[](i = 1,2,\cdots,I)$, FC further sends it to DC. Then, randomly chooses $r' \in \mathbb{Z}_n^*$, DC generates the weight of $seller_i$ as follows:

$$weight_i = \prod_{k \in K_i[]} g^{W_k} \cdot r'^n \bmod n^2 \tag{7}$$

All $weight_i$ $(i = 1,2,\cdots,I)$ will be sent to FC and decrypted according to Paillier cryptosystem [9] as shown in equation (8).

$$\begin{aligned} D(weight_i) &= D\left(\prod_{k \in K_i[]} g^{W_k} \cdot r'^n \bmod n^2\right) \\ &= D\left(g^{\sum_{k \in K_i[]} W_k} \cdot r'^n \bmod n^2\right) \\ &= \sum_{k \in K_i[]} W_k \end{aligned} \tag{8}$$

According to the weight of each $seller_i$, i.e., $\sum_{k \in K_i[]} W_k$, the ranked result array $winner'[] = (ID'_1, ID'_2, ID'_3, \cdots)$ can be obtained. Finally, FC sends the message $(winner'[]||ID_{FC}||TS)$, i.e., the ranked result, to DC through a secure channel.

Theorem 1. *For the keyword weight sequence $\boldsymbol{\mathcal{W}}' = (W_{k_1}, W_{k_2}, \ldots, W_{k_l})$ which is ordered by the ascending weights, where $W_{k_l} = c_l$. If $seller_1$ contains a more important keyword (Suppose that the largest keyword weight for $seller_1$ is c_{k_1}) compared with $seller_2$ (Suppose that the largest keyword weight for $seller_2$ is c_{k_2}), i.e., $k_1 \geq k_2 + 1$, then $seller_1$ has higher priority in the returned $winner'[]$, i.e., $weight_1 > weight_2$.*

Proof. Because $\sum_{j=1}^{i-1} c_j < c_i$, we have

$$\begin{aligned} weight_1 &= \sum_{p=1}^{k_1} c_p \\ &= c_{k_1} + \sum_{p=1}^{k_1 - 1} c_p \\ &\geq c_{k_1} + \sum_{p=1}^{k_2} c_p \\ &> \sum_{p=1}^{k_2} c_p \\ &> weight_2 \end{aligned} \tag{9}$$

5. Security Analysis

In this section, we analyze the security properties of our proposed scheme. In particular, based on the security requirements discussed in Section 2.2, our analysis focuses on how to achieve confidentiality of keywords, authentication, data integrity and query privacy.

5.1 Confidentiality of Keywords

In our proposed scheme, all the types of tag's keywords $(\boldsymbol{m_{i,1}}, \boldsymbol{m_{i,2}}, \cdots, \boldsymbol{m_{i,l}})$ $(\boldsymbol{m_{i,j}} \in \mathbb{Z}_{\boldsymbol{n}})$ are aggregated to $\boldsymbol{C_i}$ as

$$C_i = (g_1{}^{m_{i,1}} \cdot g_2{}^{m_{i,2}} \cdot \cdots \cdot g_l{}^{m_{i,l}} \cdot r_i^n)^{b_i} \bmod n^2$$
$$= g^{b_i M_i} \cdot (r_i^{b_i})^n \bmod n^2$$

That means that C_i is a ciphertext of Paillier cryptosystem, similarly, C_j, C_{buy} and C_{sel} are the same. Due to the security of Paillier cryptosystem [9], the confidentiality of keywords is protected. And in DC, since it only does homomorphic computing on C_{buy} and C_{sel}, it cannot identify the tag or trapdoor. In the end, FC will decrypt C for the range comparison of keywords. But FC cannot gain each $seller/buyer$'s keywords, because the result is only a difference, e.g., $M_{i,j} = M_i - M_j$, FC cannot recover the corresponding M_i and M_j. In addition, with the super-increasing sequence $\vec{\boldsymbol{b}} = (b_1, b_2, \cdots, b_l)$, the parameter D might be estimated. However, D is a large integer and it would not disclosure the specific keyword information. Therefore, the proposed scheme can achieve the confidentiality of keywords.

5.2 Encrypted Messages' Authentication and Data Integrity

The tags $\boldsymbol{C_i}$ $(\boldsymbol{i} = \boldsymbol{1}, \boldsymbol{2}, \cdots)$ and total trapdoor $\boldsymbol{C_{buy}}$ in our proposed scheme are encrypted by Paillier cryptosystem, therefore the adversary $\boldsymbol{A}$ cannot identify them, but if the adversary $\boldsymbol{A}$ fabricates a message and sends it to some entities, it cannot be detected. Hence, we also sign them by the signature algorithm [11]. Therefore, our proposed scheme can achieve such messages' authentication and data integrity.

5.3 Query Privacy

The range information and keyword weights are stored in two sequences $\boldsymbol{\mathcal{R}}$ and $\boldsymbol{\mathcal{W}}$, respectively, which should be encrypted to prevent the disclosure of privacy. As shown in 4.3.1, $\boldsymbol{\mathcal{R}}||\boldsymbol{\mathcal{W}}$ is encrypted by Paillier cryptosystem. Thus, only FC can use its private key $sk = (\lambda, \mu)$ to decrypt $\boldsymbol{\mathcal{R}}||\boldsymbol{\mathcal{W}}$. In addition, As shown in *(2) Choosing winners* of Section 4.4, only a part of keyword weights $weight_i = \prod_{k \in K_i[]} g^{W_k}$ are sent to the filter center, where $K_i[]$ is an array storing the keywords which satisfy the corresponding matching rules. The filter center can only get the total weight of $seller_i$, i.e., $\sum_{k \in K_i[]} W_k$, it cannot identify the weight of each keyword. Therefore, the query privacy is achieved.

Table 2. Comparison of Security Level

Properties	SESA [3]	PaRQ [8]	EMRQ
Confidentiality	√	√	√
Authentication and data integrity	√	√	√
Query privacy		√	√

In **Table 2**, we compare EMRQ with PaRQ [8] and SESA [3]. We can see all schemes achieve confidentiality of keywords, authentication and data integrity, PaRQ and EMRQ further achieve query privacy.

6. Performance Evaluation

In this section, we evaluate the performance of EMRQ in terms of functionality, computation and communication overhead.

6.1 Functionality

We compare the functionalities of EMRQ with SESA [3] and PaRQ [8]. As shown in Table 3, SESA achieves multi-keyword search in smart grid auction market, PaRQ further achieves range query, but only EMRQ scheme can achieve multi-keyword, range query, ranked search and personalized search simultaneously.

Table 3. Comparison of Functionalities

Functionality	SESA [3]	PaRQ [8]	EMRQ
Multi-keyword	√	√	√
Range query		√	√
Ranked search			√
Personalized search			√

6.2 Computation Overhead

For simplicity, the cost of a pairing operation, a multiplication operation in G_1, an exponentiation operation in $\mathbb{Z}_{n^2}$ and an exponentiation operation in $\mathbb{Z}_n$ are denoted as C_p, C_m, C_{en^2} and C_{en}, respectively. Compared with above operations, other operations in EMRQ and SESA are negligible [13].

In EMRQ, it costs $2C_m$ to sign a message, and $2C_p$ to verify if we adopt precomputed technology [11]. For $seller_i$, he needs $(l+1)C_{en^2}+C_{en}$ to create tags C_i and $2C_m$ to sign it. Therefore, all $sellers$' cost is $(2C_m+(l+1)C_{en^2}+C_{en})I$. For $buyer_j$, he costs $lC_{en^2}+C_{en}$ to create tags C'_j and C_{en^2} to create C'_{total}. Then he encrypts $(\mathcal{R}||\mathcal{W})$ with $3lC_{en^2}$. Finally, he costs $2C_m$ to sign it. Hence, all $buyers$' cost is $(2C_m+(4l+1)C_{en^2}+C_{en})J$ (assume J is the number of $buyers$). For DC, it needs $2(I+J)C_p$ to verify all messages of $sellers$ and $buyers$. For every $buyer_j$, DC needs to sign a message $msg_{DC\to FC}=(C||\mathcal{R}||\mathcal{W}||ID_{DC}||ID_{B_j}||TS)$ to FC, the signature costs $2JC_m$. Therefore, DC's cost is $2JC_m+(2I+2J)C_p$. For FC, it needs total $2JC_p$ to verify the messages from DC, then decrypts $C,\mathcal{R}$ and $weight_i$ with JC_{en^2}, $2lJC_{en^2}$ and JC_{en^2}. Hence, FC's cost is $(2l+2)JC_{en^2}+2JC_p$. Therefore, in our proposed EMRQ, the total computation overhead is $(4J+2I)C_m+((l+1)I+(6l+3)J)C_{en^2}+(J+I)C_{en}+(4J+2I)C_p$.

In the SESA scheme, we assume it adopts the same signature technology and two cyclic addition groups G_1, G_2. EB_j makes a bid to EDR_i which costs $3C_m+2C_p$, and the corresponding signature needs $2C_m$, thus all energy $buyers$' cost is $5IJC_m+2IJC_p$ where each EB expects to make a bid to each EDR because EB cannot know which bid will be accepted; EDR_i needs C_m to create a trapdoor and $2C_m$ to sign it, therefore EDR_i's cost is

$3IC_m$; AS needs $2C_p$ to verify a message which will be $IJ + I$ times, and C_p to compare each tag which will be IJ times, hence AS's cost is $(3IJ + 2I)C_p$; RS needs $C_m + C_p$ to decrypt a satisfied bid, assume that in SESA there are average N tags matching the trapdoor in once bid, therefore its total cost is $IN(C_m + C_p)$. Therefore, in SESA the total computation overhead is $(5IJ + 3I + IN)C_m + (2IJ + 2I + IN)C_p$.

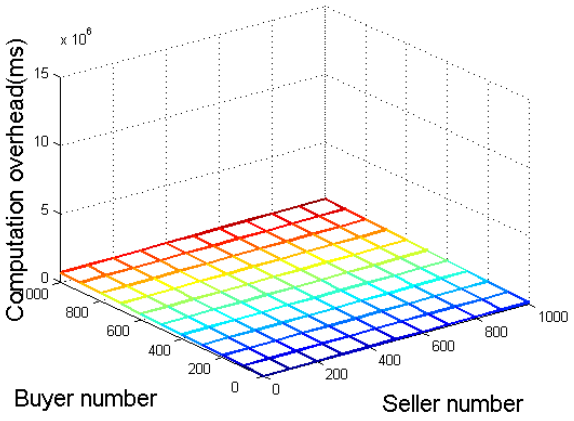

Fig. 5. Computation overhead of EMRQ

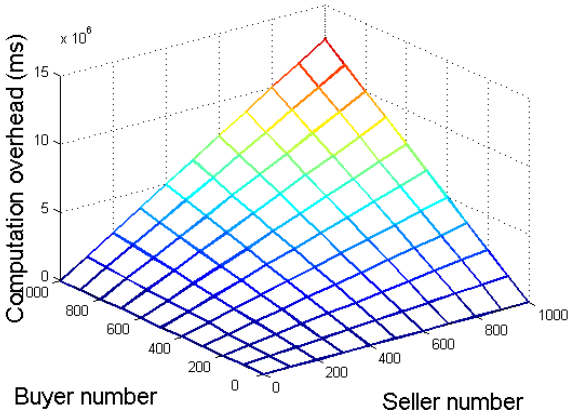

Fig. 6. Computation overhead of SESA

We conduct detailed experiments on Pentium IV 3GHz system to study the operation cost [13]. For G_1 over MNT curve, a multiplication operation in G_1 with 161 bits, and the corresponding pairing operation cost 0.6 ms and 4.5 ms. And an exponentiation operation costs 11.5 ms in $\mathbb{Z}_{n^2}$ and 2.3 ms in $\mathbb{Z}_n$. Further, we assume $N = 0.1 \times J$ in SESA and $l = 10$. As shown in Fig. 5 and Fig. 6, the proposed scheme greatly reduces the computation overhead.

6.3 Communication Overhead

We divide the communication overhead of our proposed scheme into three types, $seller - DC$, $buyer - DC$ and $DC - FC$, where the delivery of winner messages are the same in SESA and our scheme, we do not compare. The message $seller$ sends to DC is formed by $msg_{seller_i \to DC} = (C_i||ID_{S_i}||TS||\sigma)$ where the signature σ includes two elements

in G_1, therefore if we choose 1024-bit $\mathbb{Z}_n^*$ and 161-bit G_1, the total size of $seller - DC$ communication overhead is $(2048 + |ID| + |TS| + 2 \times 161) \times I$ bits. The message of $buyer - DC$ is formed by $msg_{buyer_j \to DC} = (C_{buy}||\boldsymbol{\mathcal{R}}||\boldsymbol{\mathcal{W}}||ID_{B_j}||TS)$, each R_k $(k = 1,2,\cdots,l)$ includes two ciphertexts of Paillier Cryptosystem, and W_k includes one. Thus its total size is $(2048 \times (3l + 1) + |ID| + |TS| + 2 \times 161) \times J$ bits. In $DC - FC$ phase, there are J messages of $msg_{DC \to FC} = (C||\boldsymbol{\mathcal{R}}||ID_{DC}||ID_{B_j}||TS)$ and $(weight_i||ID_{DC}||ID_{B_j}||TS)$, the total size is $(2048 \times (2l + 2) + 4 \times |ID| + 2 \times |TS| + 2 \times 161) \times J$ bits.

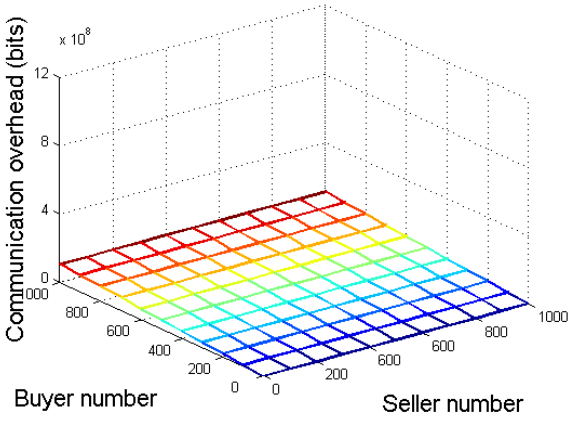

Fig. 7. Communication overhead of EMRQ

In comparison, in SESA, $EB - to - AS$ phase needs IJ messages of 963 bits, therefore the size is $963 \times IJ$ bits; $DER - to - AS$ needs to delivery a trapdoor of 160 bits and the corresponding signature of 161×2 bits, the total size is $(160 + 2 \times 161) \times I$ bits; in $AS - to - RS$ phase, for each DER, there are N ciphertexts C_j of 160 bits and signatures of 161×2 bits, hence the total size is $(160 + 2 \times 161) \times IN$ bits.

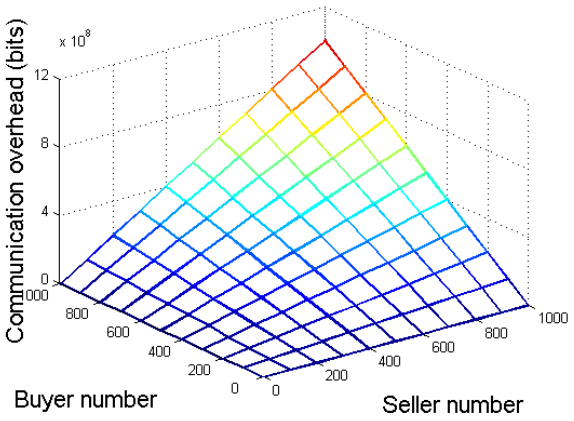

Fig. 8. Communication overhead of SESA

We set $|ID| + |TS|$ as 50 bits, then the comparison of total communication overhead for SESA and EMRQ are $482I + 963IJ + 482IN$ bits and $2420I + 109388J$ bits, respectively. As shown in Fig. 7 and Fig. 8, EMRQ is more efficient than SESA.

7. RELATED WORKS

The traditional auction market has been widely studied and many famous auction web sites have been applied to practice (e.g., Yahoo!, eBay, etc.) [14,15]. Recently, online auction becomes more popular, many people prefer to shop on the internet. Song et al. [16] estimate the behaviors of the rivals and present the bid. Chang et al. [17] present anonymous auction protocol with freewheeling bids.

In power market, auction technology has been extensively studied and various auction models are presented [2,14,18, 20]. Nguyen et al. [2] propose a demand respond exchange scheme, which thinks of demand respond as a kind of virtual goods. Li et al. [14] propose a auction scheme with privacy, which can also achieve anonymity bidding. Bompard et al. [18] propose supply function models in power market, which support supply-side strategic bidding. Liaw et al. [19] propose an electronic online bidding auction protocol, which can achieve the corresponding security and efficiency. Based on game theory, Kanga et al. [20] define oligopolistic strategy to efficient auction in power market.

Auction market in smart grid has attracted a lot of attention due to the remarkable economic benefits in electricity trading[21,22]. The corresponding issues have been extensively studied and various auction market schemes have been proposed to protect its security [3,8,23]. Wen et al. [3] propose a searchable encryption scheme (SESA) for auctions between energy generators and retailers. In SESA, each buyer makes a different tag message for every seller's energy he wants to bid. In this case, the computation and communication overheads are heavy. And Wen et al. [8] also propose a novel privacy-preserving range query (PaRQ) scheme over encrypted metering data, which protects the privacy of financial auditing in smart grid. Lu et al. [24] adopt a super increasing-sequence to aggregate all types of electricity data. In such a scheme, the intermediate can achieve privacy preservation and efficiency, without decrypting the received messages. Therefore, it is feasible to introduce this method into searchable encryption auction market.

In addition, querying encrypted data has been extensively studied because of its wide range of applications. The first work can refer to Song et al. [25], which embeds a symmetric key setting to search on encrypted data, and its improvements and advanced security definitions are given in Goh [26], Chang et al. [27], and Curtmola et al. [28]. Recently, many searchable encryption schemes [29-33] have also been proposed to query outsourced data without disclosing any private information to unauthenticated entities. A relevance score scheme is presented by Wang et al. [29], which uses relevance score to achieve ranked query of keyword. And Li et al. [30] propose a fuzzy keyword search scheme which is purposed to solve minor typos and format inconsistencies in keyword search. Cao et al. [31] propose a widely used searchable encryption scheme, which can return the ranked results of search according to the number of matching keywords. Then, a multi-keyword top-k scheme is proposed by Yu et al. [32], such scheme returns ranked results and achieves high security with fully homomorphic encryption. Sun et al. [33] consider the multidimensional tree technique and the relevance scores of keywords, this scheme supports multi-keyword search and it can achieve efficient query. In our scheme, with a super increasing-sequence, we achieve the efficient multi-keyword range query of the encrypted auction.

8. CONCLUSION

In this paper, we have proposed an efficient multi-keyword range query (EMRQ) scheme for the auction market in smart grid. It can achieve range query, ranked search and

personalized search simultaneously. Security analysis demonstrates that EMRQ can achieve confidentiality of keywords, authentication, data integrity and query privacy. Performance evaluation shows that the proposed scheme significantly improves computation and communication efficiency compared with the SESA scheme in [3].

References

[1] Y. Yang, H. Li, M. Wen, H. Luo, and R. Lu, "Achieving ranked range query in smart grid auction market," in *Proc. of ICC*, pp. 951-956, 2014. Article (CrossRef Link)

[2] H. Li, X. Lin, H. Yang, X. Liang, R. Lu, and X. Shen, "Eppdr: an efficient privacy-preserving demand response scheme with adaptive key evolution in smart grid," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no.8, pp. 2053-2064, 2014. Article (CrossRef Link)

[3] M. Wen, R. Lu, J. Lei, H. Li, X. Liang, and X. Shen, "Sesa:an efficient searchable encryption scheme for auction in emerging smart grid marketing," *Security and Communication Networks*, vol. 7, no. 1, pp. 234-244, 2014. Article (CrossRef Link)

[4] H. Liang, B. Choi, W. Zhuang, and X. Shen, "Towards optimal energy store-carry-and-deliver for phevs via v2g system," in *Proc. of INFOCOM*, pp. 1674-1682, 2012. Article (CrossRef Link)

[5] H. Liang, B. Choi, A. Abdrabou, W. Zhuang, and X. Shen, "Decentralized economic dispatch in microgrids via heterogeneous wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 6, pp. 1061-1074, 2012. Article (CrossRef Link)

[6] H. Li, X. Liang, R. Lu, X. Lin, and X. Shen, "Edr: an efficient demand response scheme for achieving forward secrecy in smart grid," in *Proc. of GLOBECOM*, pp. 929-934, 2012. Article (CrossRef Link)

[7] H. Li, R. Lu, L. Zhou, B. Yang, and X. Shen, "An efficient merkle tree based authentication scheme for smart grid," *IEEE Systems Journal*, vol. 8, no. 2, pp. 655-663, 2014. Article (CrossRef Link)

[8] M.Wen, R. Lu, K. Zhang, J. Lei, X. Liang, and X. Shen, "PaRQ: a privacy- preserving range Query scheme over encrypted metering data for smart grid," *IEEE Transactions on Emerging Topics in Computing*, vol. 1, no.1, pp. 178-191, 2013. Article (CrossRef Link)

[9] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Proc. of EUROCRYPT*, pp. 223-238, 1999. Article (CrossRef Link)

[10] N. Ferguson, R. Schroeppel, and D. Whiting, "A simple algebraic representation of rijndael," in *Proc. of Selected Areas in Cryptography*, pp. 103-111, 2001. Article (CrossRef Link)

[11] B. Libert and J. Quisquater, "The exact security of an identity based signature and its applications," *Cryptology ePrint Archive*, http://eprint.iacr.org/2004/102.

[12] D. Boneh and M. K. Franklin, "Identity-based encryption from the weil pairing," in *Proc. of CRYPTO*, pp. 213-229, 2001. Article (CrossRef Link)

[13] "Multiprecision integer and rational arithmetic c/c++library," http://www.certivox.com/miracl/.

[14] M. Li, S. Justie, H. Jennifer, "Practical electronic auction scheme with strong anonymity and bidding privacy," *Information Science*, vol. 181, no. 12, pp. 2576-2586, 2011. Article (CrossRef Link)

[15] S. Chakraborty, M. Weiss, and M. Simoes, "Distributed intelligent energy management system for a single-phase high-frequency ac microgrid," *IEEE Transactions on Industrial Electronics*, vol. 54, no. 1, pp. 97-109, 2007. Article (CrossRef Link)

[16] Y. Song, Y. Ni, F. Wen, "An improvement of generation firm's bidding strategies based on conjectural variation regulation via dynamic learning," In *Proc. of the CSEE*, pp. 23-27, 2003. http://en.cnki.com.cn/Article_en/CJFDTOTAL-ZGDC200312004.htm

[17] Y. Chang, C. Chang, "Enhanced anonymous auction protocols with freewheeling bids," In *Proc. of 20th International Conference on Advanced Information Networking and Application (AINA06)*, pp. 353-358, 2006. Article (CrossRef Link)

[18] E. Bompard, W. Lu, R. Napoli, "Network constraint impacts on the competitive electrically markets under supply-side strategic bidding," *IEEE Transactions on Power System*, vol. 21, no. 1, pp. 160-170, 2006. Article (CrossRef Link)

[19] H. T. Liaw, W. S. Juang, C. K. Lin, "An electronic online bidding auction protocol with both security and efficiency," *Applied Mathematics and Computation*, vol. 174, no. 2, pp. 1487-1497, 2006. Article (CrossRef Link)
[20] D. J. Kanga, B. H. Kimb, D. Hur, "Supplier bidding strategy based on non-cooperative game theory concepts in single auction power pools," *Electric Power Systems Research*, vol. 77, no. 5, pp. 630-636, 2007. Article (CrossRef Link)
[21] R. Jiang, R. Lu, J. Luo, C. Lai, and X. Shen, "Efficient self-healing group key management with dynamic revocation and collusion resistance for SCADA in smart grid," *Security and Communication Networks*, 2014. Article (CrossRef Link).
[22] R. Jiang, R. Lu, Y. Wang, J. Luo, C. Shen, and X. Shen, "Energy-theft detection issues for advanced metering infrastructure in smart grid," *TSINGHUA SCIENCE AND TECHNOLOGY*, Vol. 19, No. 2, pp. 105-120, 2014. Article (CrossRef Link)
[23] D. Liu, H. Li, Y. Yang, and H. Yang, "Achieving multi-authority access control with efficient attribute revocation in smart grid," in *Proc. of ICC*, pp. 634-639, 2014. Article (CrossRef Link)
[24] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, "Eppa: an efficient and privacy preserving aggregation scheme for secure smart grid communications," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 9, pp. 1621-1631, 2012. Article (CrossRef Link)
[25] D. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in *Proc. of IEEE Symp. Security and Privacy*, pp. 44-55, 2000. Article (CrossRef Link)
[26] E. J. Goh, "Secure Indexes," *Cryptology ePrint Archive*, http://eprint.iacr.org/2003/216. 2003.
[27] Y. C. Chang and M. Mitzenmacher, "Privacy preserving keyword searches on remote encrypted data," in *Proc. of Third Int'l Conf. Applied Cryptography and Network Security*, pp. 442-455, 2005. Article (CrossRef Link)
[28] R. Curtmola, J.A. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," in *Proc. of 13th ACM Conf. Computer and Comm. Security (CCS '06)*, pp. 79-88, 2006. Article (CrossRef Link)
[29] C. Wang, N. Cao, K. Ren, and W. Lou, "Enabling secure and efficient ranked keyword search over outsourced cloud data," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 8, pp. 1467-1479, 2012. Article (CrossRef Link)
[30] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy keyword search over encrypted data in cloud computing," in *Proc. of INFOCOM*, pp. 1-5, 2010. Article (CrossRef Link)
[31] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 1, pp. 222-233, 2014. Article (CrossRef Link)
[32] J. Yu, P. Lu, Y. Zhu, G. Xue, and M. Li, "Towards secure multi-keyword top-k retrieval over encrypted cloud data," *IEEE Transactions on Dependable and Secure Computing*, vol. 10, no. 4, pp. 239-250, 2013. Article (CrossRef Link)
[33] W. Sun, B. Wang, N. Cao, M. Li, W. Lou, Y. T. Hou, and H. Li, "Verifiable privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking," *IEEE Transactions on Parallel and Distributed Systems*, 2013. Article (CrossRef Link)

Hongwei Li received his M.S. degree in Computer Application from Southwest Jiaotong University (SWJTU) and Ph.D. degree in Computer Software and Theory from University of Electronic Science and Technology of China (UESTC) in 2004 and 2008 respectively. From 2011 to 2012, he worked as a Postdoctoral Fellow at University of Waterloo, Canada. Currently, he is an associate professor at the School of Computer Science and Engineering, UESTC, China. His research interests include cryptography, and the secure smart grid. Dr. Li serves as the Associate Editor of Peer-to-Peer Networking and Applications, the Guest Editor for Peer to Peer Networking and Applications Special Issue on Security and Privacy of P2P Networks in Emerging Smart City. He also serves on the technical program committees for many international conferences such as IEEE INFOCOM, IEEE ICC, IEEE GLOBECOM, IEEE WCNC, etc. He is a member of IEEE, a member of China Computer Federation and a member of China Association for Cryptologic Research.

Yi Yang received his B.S. degree in Network Engineering from Tianjin University of Science and Technology (TUST) in 2012. Currently, he is a master student at the School of Computer Science and Engineering, University of Electronic Science and Technology of China (UESTC), China. He serves as the reviewer of Peer-to-Peer Networking and Application, IEEE INFOCOM, IEEE ICC, IEEE GLOBECOM, IEEE ICCC, etc. His research interests include cryptography, and the secure smart grid.

Mi Wen received her M.S. degree in Computer Software and Theory from Universi ty of Electronic Science and Technology of China (UESTC) and Ph.D. degree in com puter system structure from Shanghai Jiaotong University of China (SJTU) in 2004 a nd 2008, respectively. From 2012 to 2013, she worked as a Visting Scholar at Univer sity of Waterloo, Canada. Currently, she is an associate professor at the College of C omputer Science and Technology, Shanghai University of Electric Power, China. Her research interests include applied cryptography, and the security in smart grid. Dr. W en serves as the Associate Editor of Peer-to-Peer Networking and Application. She al so serves on the technical program committees for many international conferences su ch as IEEE INFOCOM, IEEE ICC, IEEE GLOBECOM, IEEE ICCC, etc. She is a me mber of IEEE, a member of China Computer Federation and a member of China Ass ociation for Cryptologic Research.

Hongwei Luo received his B.S. and M.S. degrees from Beijing University of Posts and Telecommunications (BUPT), in 1998 and 2003, respectively. Now, He is a PhD candidate in BUPT, majoring in information security. From 1998 to 2003, he served as an engineer in China Telecom. He is a senior engineer and the deputy director of Department of Information Security, Telecommunication Terminal Technology Labs, China Academy of Telecom Research (CATR). He was a visiting scholar in University of Waterloo from 2011 to 2012. From 2005 till now, He has been acting as the rapporteur of ITU-T Q.5/17, countering spam by technical means and has published 3 ITU-T recommendations. From 2014, he has also been selected as the chairman of China Communications Standards Association (CCSA) WG3/TC11, Terminal Workgroup. He has published more than 20 national standards, 2 patents, 2 conference papers and more than 50 magazine articles. His research interests include wireless communications, routing and switching, information security and performance evaluation.

Rongxing Lu received the Ph.D degree in computer science from Shanghai Jiao Tong University, Shanghai, China in 2006 and the Ph.D. degree (awarded Canada Governor General Gold Medal) in electrical and computer engineering from the University of Waterloo, Waterloo, Ontario, Canada, in 2012. Since May 2013, he has been with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore, as an Assistant Professor. His research interests include computer, network and communication security, applied cryptography, security and privacy analysis for vehicular network, eHealthcare system, and smart grid communications. He won the IEEE Communications Society (ComSoc) Asia Pacific (AP) Outstanding Young Researcher Award in 2013.