Intelligent Automation And Soft Computing, 2019

Vol.25,no.1,171–181

A novel privacy-preserving multi-attribute reverse auction scheme with bidder anonymity using multi-server homomorphic computation

Wenbo Shi[1], Jiaqi Wang[2], Jinxiu Zhu[3], YuPeng Wang[4], Dongmin Choi[5]

[1]School of Computer and Communication Engineering, Northeastern University at Qinhuangdao, Qinhuangdao, China
[2]Department of Computer Science and Engineering, Northeastern University, Shenyang, China
[3]Research Institute of Ocean and Offshore Engineering, Hohai University, Nantong, 226300, China
[4]College of Electronical and IT Engineering, Shenyang Aerospace University, Shenyang, 110136, China
[5]Division of Undeclared Majors, Chosun University, Gwangju 61452, South Korea

ABSTRACT
With the further development of Internet, the decision-making ability of the smart service is getting stronger and stronger, and the electronic auction is paid attention to as one of the ways of decision system. In this paper, a secure multi-attribute reverse auction protocol without the trusted third party is proposed. It uses the Paillier public key cryptosystem with homomorphism and combines with oblivious transfer and anonymization techniques. A single auction server easily collides with a bidder, in order to solve this problem, a single auction server is replaced with multiple auction servers. The proposed scheme uses multiple auction servers to calculate the attributes under encryption protection and obtains the linear additive score function value finally. Since the attribute is calculated under the protection of encryption, the proposed scheme achieves privacy-preserving winner determination with bid privacy. Furthermore, the proposed scheme uses oblivious transfer and anonymization techniques to achieve bidder anonymity. In accordance with the security analysis, major properties, bidder anonymity and somewhat reducing collusion possibilities, are provided under the semi-honest model. According to a comparison of computation, the proposal's computation cost is reasonable.

KEY WORDS: Reverse multi-attribute auction • Privacy-preserving • Homomorphic encryption • Oblivious transfer.

1 INTRODUCTION

WITH the advent of networked smart devices and distributed information systems, the demand for new smart services is expected to increase as these services are now becoming an important part of our life. Networked smart devices and distributed information systems completely changed the people's traditional way of life[1-10]. Meanwhile, a variety of security and privacy issues associated with smart services and systems[11-21]. A security protocol can ensure the security of the smart service by using the cryptographic methods and it can perform a security-related function. In order to solve security and privacy issues associated with smart services and systems, many cryptographic protocols including real authentication[22-25], keyword search in encrypted cloud[26-29], verifiable data auditing in Cloud[30] are proposed. These approaches have played a very important role in security protocol design for smart services.

As an important part of economic activities, Auctions attract more and more people and entities rely on the auction to efficiently complete the sale of goods or services. The auction provides the buyer and the seller with the benefit maximization. Electronic auction as a new form of Internet auction, with low cost, convenience, fairness and other characteristics. But the electronic auction also faces some obstacles, such as information security issues.

In sealed auctions, the participants bid is not disclosed to others [31]. On the other hand, auction protocols can be classified into two types: one-sided auction and two-sided auction[32]. Only one seller or buyer can receive the multiple buyers or sellers bids in

CONTACT Wenbo Shi swb319@hotmail.com

one sided auction protocol. After a long period of research and practice, one-sided sealed-bid auction protocol research has achieved a lot [33-37]. Recently, most researchers begin to use cryptography to ensure the security of auction, such as zero-knowledge proof [33-37] and secure multi-party computation[35]. Those techniques provide better bid privacy and winner public verifiability.

Currently, most researchers focus on single-attribute auction model. With the development of market demands, price, as the only determinant of the auction winner, has not met the needs. In comparison with single-attribute model auction, buyers and sellers can reap greater benefits in multi-attribute model auction[38].

Nowadays, multi-attribute model auction become more and more important in our fields of e-auction and it is a hot spot of the research in auction theory. The research of the multi-attribute needs to consider the security issue of online auction that researchers defined. Thus, various problems we should to deal with and consider how to solve them [33, 39-41]. The security requirements of OMOTE et al. [33, 39-41] and summarized as follows: anonymity, traceability, no framing, unforgeability, Non-repudiation, fairness, public verifiability, unlinkability among different rounds of an auction. Some details are not repeat here. To satisfy the requirements of people in auction, some research of multi-attribute can be summed as four parts. We need to considerate the computational complexity of winner determination [42, 43], procurement cost reduction of buyer[43-46], cost function of seller[42,43,46,47], configuration of bids[48] and number of winners[48]. According to the consideration of the configuration of bids for example, Bichlerand Kalagnanam propose the concept of Configurable offer focus on a configurable offer as a function of price on multi-attributes (quantitative and qualitative)[48]. In addition, some protocols of multi-attributes auction may also need online Trusted Third Party (TTP) which is proposed by Srinathet al.[49] However, the protocol in[49] has a weak bid privacy and the public verifiability cannot be provided.

In this paper, we consider the security problems above and proposed privacy-preserving multi-attribute reverse auction scheme with bidder anonymity using multi-server Homomorphic Computation. Our contributions as follows: Firstly, the proposed scheme uses a public key cryptosystem with homomorphism to protect the attributes of the bidding scheme and achieves privacy-preserving bid calculation. Through the comparison of performance, security and homomorphism among RSA, EIgamal and Paiilier, Paillier public key cryptosystem was selected finally[50]. Secondly, a single auction server easily collides with a bidder, in order to solve this problem, a single auction server is replaced with multiple auction servers. The proposed scheme uses multiple auction servers to calculate the attributes under encryption protection and obtains the linear additive score function value finally. Finally, the proposed scheme uses oblivious transfer and anonymization techniques to achieve bidder anonymity. The remainder of this paper is organized as follows. In Section 2, we recall some preliminary knowledge including the semi-honest model, Paillier cryptosystem and oblivious transfer. The proposed scheme is shown in Section 3. In Section 4, security analysis of our scheme is given. Next, the performance evaluation compared with other schemes is provided in Sections 5. Finally, Section 6 concludes this paper.

2 PRELIMINARIES

2.1 Semi-honestmodel

IN the semi-honest model, all parties are assumed to perform computations and send messages according to their prescribed actions in the protocol. They may record all information from the protocol execution and try to infer as much information as possible in the process of the protocol, but the intermediate results in the process of the protocol cannot be modified [51,52].

Definition 1: Let $S \subseteq \{0,1\}^*$ .Two aggregations (indexed by S), $X \overset{def}{=} \{X_w\}_{winS}$ and $Y \overset{def}{=} \{Y_w\}_{winS}$ are computationally indistinguishable if there is a negligible function μ for every family of polynomial-size circuits, $\{D_n\}_{n\in N}$, $N \to [0,1]$, so that $\left|pr[D_n(w,X_w)=1]-pr[D_n(w,Y_w)=1]\right| < \mu(|w|)$. In such a case, it expressed as $X \overset{c}{\equiv} Y$.

Definition 2: protocol π securely computes deterministic functionality f with static semi-honest adversaries if there are probabilistic polynomial-time simulators S_1 and S_2 such that

$$\{S_1(x, f(x,y))\}_{x,y\in\{0,1\}^*} \overset{c}{\equiv} \{view_1^{\pi}(x,y)\}_{x,y\in\{0,1\}^*},$$

$$\{S_1(x, f(x,y))\}_{x,y\in\{0,1\}^*} \overset{c}{\equiv} \{view_2^{\pi}(x,y)\}_{x,y\in\{0,1\}^*},$$

$$where |x| = |y|.$$

2.2 Paillier's cryptosystem [53]

Key generation: let p , q be two large primes and $n = pq$, p and q satisfy $\gcd(pq,(p-1)(q-1)) = 1$. Compute $\lambda = lcm(p-1,q-1)$ and select random integer g where $g \in Z_{n^2}^*$. Ensure n divides the order of g by checking the existence of the following modular multiplicative inverse: $\mu = \left(L\left(g^{\lambda} \bmod n^2\right)\right)^{-1} \bmod n$, where function

L is defined as L(μ) = μ−1 . Get private (decryption) key (λ,μ) and public (encryption) key (n,g) .

Encryption: a message m is encrypted as $c=g^m r^n \bmod n^2$, where $m\in Z_n$, where r is taken at random and $r\in Z_n^*$.

Decryption: the message m is obtained by computing $m=L\left(c^\lambda \bmod n^2\right)$ from ciphertext $c\in Z_{n^2}^*$.

Paillier cryptosystem can achieve two homomorphic properties as follows:

(1) $D\left(E(m_1,r_1)\cdot E(m_2,r_2)\bmod n^2\right)=m_1+m_2 \bmod n$

(2) $D\left(E\left(m_1,r_1\right)^k \bmod n^2\right)=km_1 \bmod n$

$D()$ denotes decryption function, $E()$ denotes encryption function, where m_1 , $m_2\in Z_n$, r_1 , $r_2\in Z_n^*$.

2.3 Oblivious Transfer

Oblivious Transfer (OT) [54] is a very useful cryptography tool to transfer secrets between two parties, a sender and a receiver. Sender transfers n secrets to a receiver, but has no idea of which piece (if any) has been transferred. In the other hand, the receiver can access one of the secrets from the sender, without getting any information about the remaining $n-1$ secrets.

Table 1 shows the pseudo-code of 1-out-of-n oblivious transfer protocol OT_1^n proposed in[55], where q' is a large prime, g and h are two generators of $G_{q'}$, which is a cyclic group of order q' , and $Z_{q'}$ is a finite additive group of q' elements. As long as $\log_g h$ is not revealed, g and h can be used repeatedly.

Table 1. 1-out-of-n oblivious transfer ((OT_n^1))

Initialization:
Parameters: $(g,h,G_{q'})$
Sender's Input: $s_1,s_2,...,s_n\in G_{q'}$;
Receiver's choice: $\varepsilon,\varepsilon\left[1,n\right]$
1. The sender sends $\varepsilon, y=g^r h^\varepsilon, r\in_R Z_{q'}$;
2. The receiver sends $c_j=\left(g^{t_j} s_j\left(y/h^j\right)^{t_j}\right)$, $t_j\in_R Z_{q'}, 1\le j\le n$;
3. After receiving $c_\varepsilon=(d,f)$, sender computes $s_\varepsilon=f/d^r$;

3 THE PROPOSED SCHEME

3.1 Initialization phase

AT the protocol initialization phase, buyers publish the requirements of their goods that they want to purchase and the set of corresponding non-price weight attributes $\{w_i\}_{i\in[1,l]}$. Then buyers generate key pairs (Pk,Sk) and broadcast Pk in the broadcast channel. Private key Sk is kept secretly by the buyer.

In addition, bidders provide the supply program which in fact is an attribute vector of a length of L including such as price, weight and other attribute values denoted as a collection $\{\alpha_j\}_{1\le j\le l}$.

Anonymization technology proposed in [56] is used in this protocol to process the bidders of the true identities UID Register and get an anonymous identity PID which is well-processed.

$$PID=E_{PK}(UID\,||\,pad\,||\,Pk) \tag{1}$$

pad is a random padding bit which is used for filling the location that buyer specified to a certain length. The details of proof for security and uniqueness of PID can be found in[56]. It is unnecessary to go into details here. Bidders will send the PID through the broadcast channel.

At last, bidders use the public key that is published by buyer to encrypt the attribute vector $\{\alpha_j\}_{1\le j\le l}$ using the Paillier encryption:

$$e_j=E_{Pk}(\alpha_j)=g^{\alpha_j} r_j^n \bmod n^2, r_j\in Z_n^* \tag{2}$$

After encryption, bidders modify the status in the broadcast channel and set the flag as to be sent.

3.2 Bidding phase

When the auctioneer servers detect the flag of bidders to become to be sent, l servers use the OT_n^1 protocol (section 2.3) in a random order and begin to select the encrypted attributes. For auctioneer servers $P_{i\in[1,l]}$:

(1) P_i selects a subscript k randomly and sends the $y=g^r h^k$ to the anonymous bidders, where $r\in Z_n$;

(2) Anonymous bidders return a response collection $\{c_1,c_2,...,c_l\}$, where $c_{j\in[1,l]}=\left(g^{t_j},e_j\left(y/h^j\right)^{t_j}\right), t_j\in Z_n$;

(3) P_i selects k corresponding the element $c_k=(d,f)$ in $\{c_1,c_2,...,c_l\}$ and compute:

$$e_k = f / d^r = e_k\left(y / h^k\right)^{t_j} / \left(g^{t_j}\right)^r$$
$$= e_k\left(g^r h^k / h^k\right)^{t_j} / \left(g^{t_j}\right)^r \quad (3)$$

Assume l servers P_k all receive the ciphertext of attribute $e_{j\in[1,l]}$ correctly and formula $D\left(E\left(m_1, r_1\right)^k\right.$, $\left.\left(\bmod n^2\right) = km_1 \bmod n\right.$ is used, the second property of paillier cryptosystem, to compute the weight of the attribute $w_j * \alpha_j$ under the status of ciphertext:

$$E_{Pk}\left(AT_{ij}\right) = E_{Pk}\left(\alpha_j\right)^{w_j} = e_j^{w_j} \quad (4)$$

After computation, sent the $E_{Pk}\left(AT_{ij}\right)$ to the server P_l. When P_l receive the other number of $l-1$ of weight attribute of cipher text, P_l begin to compute:

$$E_{Pk}\left(Score\left(AT_i\right)\right) = \prod_{j=1}^{l} E_{Pk}\left(AT_{ij}\right) \quad (5)$$

$Score()$ is a linear additive score function. And then get the computation $E_{Pk}\left(Score\left(AT_i\right)\right)$ to sent the buyer and when finish computation of the ith of bid document, auctioneer servers continue to monitor the remaining bid status of bidders.

3.3 Winner determination phase

When the bid time that buyer set is deadline, buyer can use the private key Sk to decrypt the bid results that have received and bidders' identities. According to the formula $\arg\max_i\left(score\left(b_i, AT_i\right)\right)$, buyer can either choose one or more optional bidders as winners or launch the next round of bidding according to their scores. Figure 1 describes the procedure of protocol of one bidder.

4 SECURITY ANALYSIS.

IN this section, the security analysis of the proposed scheme will be described in details.

4.1 The security of Paillier cryptosystem

In this protocol, the process of computation of the bid document is based on Paillier cryptosystem. Therefore, the confidentiality of bid document also depends on the security of Paillier cryptosystem. In this section, we analyses the security of the Paillier cryptosystem.

Assumption 1: (Decisional Composite Residuosity Assumption) assume $n = pq$ is a RSA module and there is no polynomial-time algorithm can judge that whether the integer z is the n order remainder of module n^2 or not. In other words, it is hard to verify that whether y exists or not that satisfy the formula $z \equiv y^n \bmod n^2$, which is denoted as $DCRA$ (Decisional Composite Residuosity Assumption).

Definition 3: set $w \in Z_{n^2}^*$, g is a non-zero integer multiple of element which the middle order is n of $Z_{n^2}^*$. There exists unique $m \in Z_n$, $r \in Z\ Z_n^*$ and that can make $w = g^m r^n \bmod n^2$. we call m is w based on g of n -order residue class denoted as $\|w\|_g$ and take the problem of $\|w\|_g$ computation as the n -order residual class problem denoted as $Class[n, g]$ [50]; proof the that for given $w \in Z_{n^2}^*$,the complexity of $Class[n, g]$ is independent of g .Therefore, we can only consider the n from the complexity of computation and this problem can be simplified as $Class[n]$.

If factorize n, we can get the $Class[n]$ .So far, how to factorize the long length module n of RSA is still an open problem in cryptography. Therefore, the following assumptions can be made:

Assumption 2: (Computational Composite Residuosity Assumption) in the algorithm of probability polynomial time, it is difficult to compute the composite order residual class problem. In other words, Class[n] problem is intractable and denoted as CCRA (Computational Composite Residuosity Assumption).

Under premise of Assumption 2, Paillier cryptosystem is unidirectional; under premise of Assumption 1, Paillier cryptosystem is semantically secure. Paillier cryptosystem provides the semantic security against non-responsive selective plaintext attack (IND-CPA1). In assumption of IND-CPA, crypto- graphic system indistinguishability is defined experimentally as follows: for an attacker A (Adversary) and the holder B (Challenger) of encryption algorithm. A and B play a game (Game-Based Security Definition):

(1) B based on a security parameter k generates a key pair (Pk, Sk), then public the Pk and save the Sk.

(2) A sends two equal length and distinct plaintexts m_0, m_1 to B;

(3) B chooses a bit $b \in \{0,1\}$ randomly and sends the ciphertext $c_b = E_{Pk}\left(m_b\right)$ to A;

(4) A can make any computation or operation to c_b and finally output a result (guess) b'.

Paillier encryption is indistinguishable under IND-CPA, because for any probability polynomial within the time of the attacker A may guess the advantage of

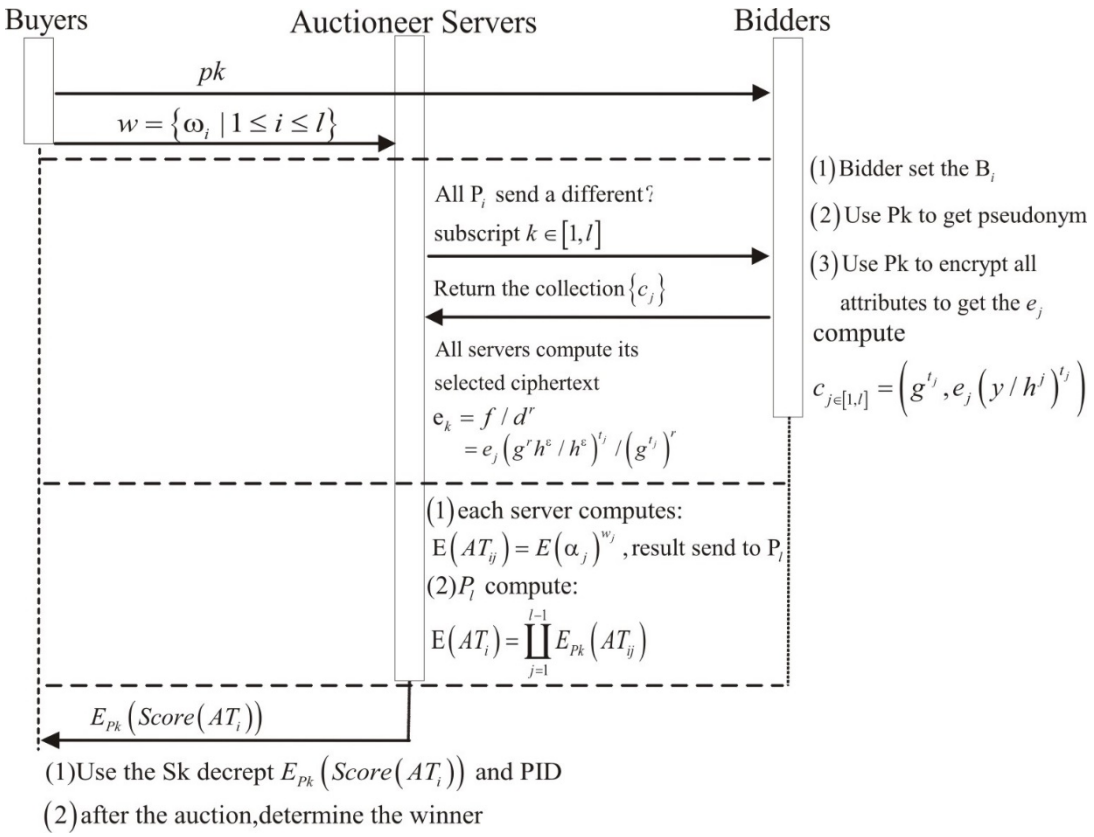

Figure 1. **The proposed scheme procedure**

the right answer of b' (win the game) which can ignore. The formula is:

$$Adv_A(E)=\left|\Pr\left[c\leftarrow E(k,m_0)\right]-\Pr\left[c\leftarrow E(k,m_0)\right]\right|=\epsilon$$

where the ϵmay ignore. Although A knows m_0, m_1, and Pk, according to the probability characteristic of Paillier encryption m_b is just one of many legal ciphertext. Therefore, A cannot get a greater advantage in this game.

Response and non-response chosen plaintext attack (IND-CPA1, IND-CPA2) may also use the similar experiment definition of IND-CPA and Paillier encryption that may resist IND-CPA1 has already proved. However, It is an open discussion in academia to resist IND-CPA2 and chosen ciphertext attack.

4.2 Other security

(1) The identity of winner anonymity: at the phase of seller information preparation, each seller takes part in this auction as a temporary identity pseudonym and buyers perform the anonymity of identities through the private key.

(2) Fairness: The techniques of oblivious transfer and identity anonymity are used in this protocol. Therefore, in the transmission process of encrypted attribute between auctioneer servers and seller, their identities are unrecognizable and in this situation there is no conspiracy attack. The key pair is generated separately by each buyer, which exists the possibility of collusion between buyers and auctioneer servers. Therefore, this protocol cannot fully guarantee the fairness of results of auction.

(3) Avoid the dependency of the private channel: the information transmitted in this protocol is encrypted information and can be arbitrarily transmitted in the broadcast channel. Therefore, for the assumption of private channel can be avoided.

Except several securities above, this protocol do not provide the other requirements of security such as non-repudiation, public verifiability in the security auction protocol. Knowledge signature, digital signature and other cryptographic techniques can be added in to improve this protocol. This is a main task in the future research.

5 PERFORMANCE EVALUATION AND DISCUSSION

5.1 Computation complexity analysis

IN this protocol, assume the binary bit length of n is k denoted as $k=\lceil \log_2 n \rceil+1$ and all the participants are semi-honest. At the bidder information preparation phase, $g^m \bmod n^2$ of module exponential operation is needed to compute and the plaintext m and n^2 of bit length are $2k$, k respectively. The module n^2 multiplication of integers of two k bit length requiring the time complexity is $O(k^2)$ compute the modular exponentiation $g^m \bmod n^2$ at most to call k times. So the time complexity of computing the $g^m \bmod n^2$ is $O(k^3)$ and similarly, the time complexity of computing the $r^m \bmod n^2$ is also $O(k^3)$. At the bidder information preparation phase, the time complexity that the encrypted attribute $E_{Pk}(m,r)=g^m r^n \bmod n^2$ needs is $O(k^3)$. The process needs to be repeated l times and at this phase, the time complexity is $O(lk^3)$. At the encrypted attribute transmission phase, the l times equations is needed to compute the response collection c of oblivious transfer. At the computation of attribute ciphertext phase, the l times power function multiplication is needed to be done to compute the weighted attribute ciphertext and then the l times homomorphic addition is also needed to be done to compute the result of the weighed sum. Finally, buyer needs to decrypted the for all n sellers of the result of the weighted sum and the time complexity of decryption is $O(k^3)$ .In conclusion, if all the participants in the auction are semi-honest, the time complexity of the single round auction protocol is $O(lk^3)$. For the auction with d bidders, the time complexity of the whole protocol is $O(dlk^3)$.

5.2 Communication complexity

As before, assume all the participants are semi-honest and ignore the communication traffic that transmission pseudonym generates. At the initial phase, buyer needs to send the public key to the n sellers. At the encrypted trans- mission phase, l elements are needed as the response collection c of oblivious transfer. At the attribute ciphertext computation phase, $l-1$ severs need to transfer their weighted ciphertext to a specific auction sever. Finally, the weighted sum of l is sent to buyer. Assume all the participants are semi-honest and at most transfer n times. Therefore, the communication traffic of the protocol is $2n+2l-1$ and the communication complexity is $O(n+l)$.

5.3 Properties

Firstly, a comparison among related protocols is summarized in Table 2. We discuss properties concluding the trusted third party, Strong bid privacy, Bulletin board, the number of parties, attribute relation, winner determination, adversary model, bidder anonymity of these protocols. We can easily conclude that the adversary model of all protocols are semi-honest and protocols need no the trusted third party except[49]. According to the complicated relation among attributes, the bid expression is important in the process of the winner determination. The Table 2 has shown that [58,59] are flexible to support independent, and dependent and interdependent attribute relation. In addition, because of the linear utility function is introduced for multi-attribute bid evaluation and it is assumed that each attribute is independent in each multi-attribute bid using linear utility function[49],[57]. are only to support the independent attribute relation. According to the score function we used in this paper and structure of the winner determination, our proposal scheme also support the independent attribute relation only. Therefore, the proposed schemes of [58,59] can support both quantitative and qualitative attribute winner determination[49],[57]. and our proposal scheme only support quantitative attribute winner determination. However, only[49] and our proposal scheme provide the property of bid anonymity to protect the privacy of bidders identities at the bidding phase but do not[57-59].

5.4 Experiments

We detailly discuss the computation operation in this subsection and the computation operation of protocols is shown in Table 3. We make a simple description that the *PKE* denoted as the Public Key Encryption and *PKD* denoted as the Public Key Decryption. We define the length of the prime number p is 512, 1024, 1536 bits in modular exponentiation which set as *ME* and set the *R* as the operation of generating a random number. t , T means the number of offer and the number of attribute respectively. Hash function digest is 512bits (for $SHA-1$) denoted as *HF* . n means the number of supplier. Because computation operation of RSA can be summarized as a modular exponentiation operation, and the computation operation of a modular exponentiation is about $O(|L|)$ times that of a modular multiplication, where $|L|$ denotes the bit length of L . In addition, So compared with a modular multiplication computation in Z_n^* , the computation

time consumed by hashing operations and random generation can be neglected. At the initiation phase, $1HF$ is needed in[49,57] and $1R$ should be done in[58,59]. However[49,57] and our proposal scheme need $2R$. Finally, all protocols should do $1PKE$ and $1PKD$ except[49] which only need to compute $n+3PKE$. At bidding phase, $nPKE$, $nPKD$ are need to be compute only in[49] and $n(T+1)+2T$, $PKEn(T+1)PKE$ in[57]. The computation of operation should be done in[58] are $t+2HF$, $t+1PKE$ and $6tR$, $22tME$ in[59]. According to our proposed scheme we only compute the nP and $nPKE$ only. At the opening phase,[58] needs to compute more operations that are tR, $2(t+1)HF$, $tPKE$, $t+1PKD$ respectively. While in [49] we only need to compute the $nPKE$. $2nTPKE$ and $n(T+1)PKE$ should be done in [57]. Our proposal scheme and do not need computation operation in this process[59]. At the winner determination phase, The protocols of computation operation $nPKD$, $2nTPKE$, $ntHF$ should be done only in[49,57,58] respectively and [59],our proposal scheme should do two more operation. $8tR$, $34tME$ are needed to compute in and $ntME$, $nPKD$ in our proposal scheme[59].

Finally, a performance simulation is shown as follows. [49,57-59] and our proposed scheme are implemented in *C* using *MIRACL* library and server configuration: Microsoft Win7 Professional 2009 Service Pack 1, Intel(R) Core(TM) i5, CPU 2.53 GHz, 1.86 GB of RAM [60]. The average time for computing a single modular exponentiation is 1.5ms for 512-bit,6ms for 1024- bit, and 28ms for 1536-bit. For a small-scale system design, assume that n > T > t. Many experiments have been done and three typical experiments are shown in Figure 2,3,4.

Table 2. Discussion of achieved properties

Protocols	[49]	[57]	[58]	[59]	Proposal
Trusted third party	Yes	No	No	No	No
Strong bid privacy	No	No	Yes	Yes	Yes
Bulletin board	No	Yes	Yes	Yes	No
The number of parties	3	2	2	2	3
Attribute relation	Independent	Independent	Independent Dependent Interdependent	Independent Dependent Interdependent	Independent
Winner determination	Quantitative	Quantitative	Qualitative and quantitative	Qualitative and quantitative	Quantitative
Adversary model	Semi-honest	Semi-honest	Semi-honest	Semi-honest	Semi-honest
Bidder anonymity	Yes	No	No	No	Yes

Table 3. The numbers of different computation operations

Phase	[49]	[57]	[58]	[59]	Proposal
The initiation phase	1 HF 2 R n+3 PKE0	1 HF 2 R 1PKE 1PKD	1R 1PKE 1PKD	1R 1PKE 1PKD	2R 1PKE 1PKD
The bidding phase	0 nPKEnPKD	0 n(T+1)+2TPKEn(T+2)+2TPKD	t+2HF t+1 PKE0	6tR 22tME	nPKE
The opening phase	0 0 n PKE0	0 0 2nTPKEn(T+1)PKD	tR 2(t+1)HFt PKEt+1PKD		
The winnerdetermination phase	0 0 nPKD	0 2nTPKE 0	ntHF 0 0	8tR 34tMEnPKD	ntME

PKE: Public Key Encryption; PKD: Public Key Decryption; HF: Hash Function; ME: Modular Exponentiation; R: generate a random number; t: number of offer; T: number of attribute; n: number of supplier

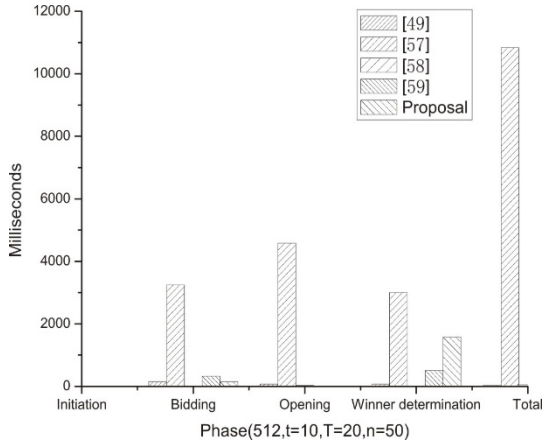

Figure 2. Comparison of computation time(key=512bit,t=10, T=20,n=50)

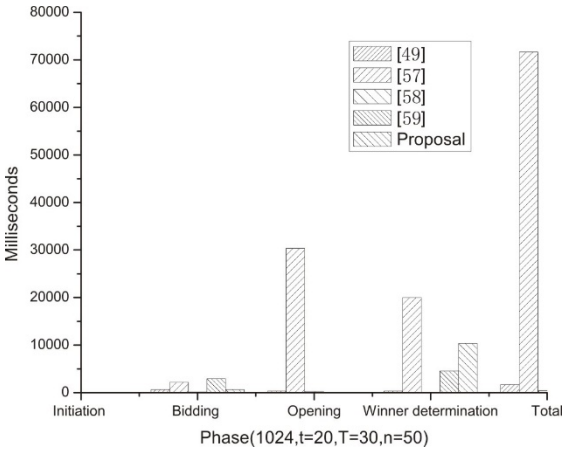

Figure 3. Comparison of computation time(key=1024bit,t=20, T=30,n=50)

6 CONCLUSIONS

IN this paper, A novel privacy-preserving multi-attribute reverse auction scheme with bidder anonymity using multi-server homomorphic computation is pro- posed for future smart services. The proposed scheme uses multiple auction servers instead of a single auction server to alleviate collusion between a bidder and an auction server, and calculate the attributes under encryption protection and obtain the linear additive score function value finally. The proposed scheme achieves privacy-preserving winner determination with bid privacy by oblivious transfer and anonymization techniques. According to the security analysis, we can conclude that our proposed scheme can strongly preserve the information privacy of every participant. In addition, performance evaluation shows that the proposed scheme has a reasonable computation overhead.

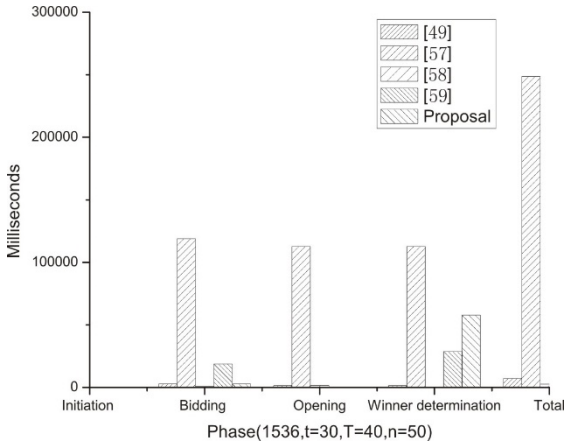

Figure 4. Comparison of computation time(key=1536bit,t=30, T=40,n=50)

7 ACKNOWLEDGEMENT

THE authors thank the editors and the anonymous reviewers for their valuable comments. This research was supported by National Natural Science Foundation of China (Grant No.61472074, U1708262), the Scientific Research Project of Liaoning Provincial Education Department of China under Grant L2014067, Nantong Science and technology projects (Fund No.2016800303).

8 REFERENCES

H. Ai and L. Tong liang, (2017). A smart home system based on embedded technology and face recognition technology, *Intelligent automation & soft computing*. 23, 3, 405-418.

M. Amjed and Z. Tanveer, (2017). Multi-Layer Network Architecture for Supporting Multiple Applications in Wireless Sensor Networks, *Journal of wireless mobile networks, ubiquitous computing, and dependable applications*. 8(3), 36-56.

M. J. Bellosta, S. Kornman, and D. Vanderpooten, (2011). Preference-based English reverse auctions, *Artificial intelligence*. 175(8), 1449-1467.

M. Bichler, (2000). An experimental analysis of multi-attribute auctions, *Decision support systems*. 29(3), 249-268.

M. Bichler and J. Kalagnanam, (2005). Bidding languages and winner determination in multiattribute auctions and winner determination in multi- attribute auctions, *European journal of operational research*. 160(2), 380-394.

B. Bordel, R. Alcarria, and M. A. Manso, et al, (2017). Building enhanced environmental traceability solutions: From Thing-to-Thing communications to Generalized Cyber-Physical Systems, *Journal of Internet Services and information security.* 7(3), 17-33.

J. Brickell and V. Shmatikov, (2005). Privacy-Preserving Graph Algorithms in the Semi-Honest Model, *Asiacrypt lncs*. 3788, 236-252.

L. I. D. Castro and D. H. Karney, (2012). Equilibria existence and characterization in auctions: achievements and open questions, J*ournal of economic surveys*. 26(5):911-932.

Y. F. Chung, Y. T. Chen, and T. L. Chen, et al, (2011). An agent-based English auction protocol using Elliptic Curve Cryptosystem for mobile commerce, *Expert systems with applications*. 38, 9900-9907.

D. Choi and I. Chung, (2016). Recent Emerging Security Threats and Countermeasure Concepts in Mobile User Authentication, *CoNvergence PRActice*. 4(1), 10-17.

Y. W. Chow, W. Susilo, and J. Phillips, et al, (2017). Video Games and Virtual Reality as Persuasive Technologies for Health Care: An Overview, *Journal of wireless mobile networks, ubiquitous computing, and dependable applications*. 8(3), 18-35.

H. E. Debiao, N. Kumar, and H. Shen, et al, (2015). One-to-many authentication for access control in mobile pay-TV systems, *Science China*. 59(5), 1-14.

C. Fontaine and F. Galand, (2009). A survey of homomorphic encryption for non- specialists, *EURASIP journal on information security*. 1(1), 41-50.

Z. Fu, K. Ren, and J. Shu, et al, (2015). Enabling Personalized Search over Encrypted Outsourced Data with Efficiency Improvement, *IEEE transactions on parallel and distributed systems*. 27(9), 2546-2559.

Z. Fu, X. Sun, and Q. Liu, et al, (2015). Achieving Efficient Cloud Search Services: Multi-keyword Ranked Search over Encrypted Cloud Data Supporting Parallel Computing, *IEICE transactions on communications.* 98(1), 190-200.

M. Ganesh, M. Naresh, and C. Arvind, (2017). MRI Brain Image Segmentation Using Enhanced Adaptive Fuzzy K-Means Algorithm, *Intelligent automation & soft computing*. 23(2), 325-330.

C. Gao, Z. A. Yao, and D. Xie, (2011). Electronic sealed-bid auctions with incoercibility, *Electrical power systems and computers*, 99, 47-54.

Goldreich, (2004). *Foundations of cryptography: volume ii (basic applications)*. Cambridge University Press.

C. Gritti, W. Susilo, and Thomas Plantard, et al. (2016). Certificate-Based Encryption with Keyword Search: Enabling Secure Authorization in Electronic Health Record, *Journal of internet services and information security*. 6(4), 1-34.

P. Guo, J. Wang, and X. H. Geng, (2014). A Variable Threshold-value Authentication Architecture for Wireless Mesh Networks, *Journal of internet technology*. 15(6), 929-936.

D. He, S. Zeadally, and N. Kumar, et al, (2016). Anonymous authentication for wireless body area networks with provable security, *IEEE systems journal*. (99), 1-12.

M. Hinkelmann, A. Jakoby, and N. Moebius, et al, (2011). A cryptographically T- private auction system, *Concurrency and computation: practice & experienc*e. 23(12), 1399-1413.

T. Ishida, Y. Shinotsuka, and M. Iyobe, et al, (2016). Development of a Zoo Walk Navigation System using the Positional Measurement Technology and the Wireless Communication Technology, *Journal of internet services and information security*. 6(4), 65-84.

Q. Jiang, J. Ma, and F. Wei, (2016). On the Security of a Privacy-Aware Authentication Scheme for Distributed Mobile Cloud Computing Services, *IEEE systems journal*. (99), 1-4.

S. Kameshwaran, Y. Narahari, C. H. Rosa, et al, (2007). Multiattribute electronic procurement using goal programming, *European journal of operational research*. 179(2), 518-536.

G. Karakaya and M. Koksalan, (2011). An interactive approach for multi-attribute auctions, *Decision support systems*. 51(2), 299-306.

J. Li, X. Li, and B, Yang, et al, (2015). Segmentation-based Image Copy- move Forgery Detection Scheme, *IEEE Transactions on information forensics and security*. 10(3), 507-518.

M. J. Li, S. T. Juan, and H. C. Tsai, (2011). Practical electronic auction scheme with strong anonymi-ty and bidding privacy, *Information sciences*. 181(12), 2576-2586.

X. Li, J. Niu, and M. Karuppiah, et al, (2016). Secure and Efficient Two-Factor User Authentication Scheme with User Anonymity for Net-work Based E-Health Care Applications, *Journal of medical systems.* 40(12), 268.

C. C. Lin, S. C. Chen, and Y. M. Chu, (2011). Automatic price negotiation on the web: an agent-based web application using fuzzy expert system, *Expert systems with applications*. 38(5), 5090-5100.

T. Ma, J. Zhou, and M. Tang, (2015). Social network and tag sources based augmenting collaborative recommender system. *IEICE transactions on information and systems*, 98(4), 902-910.

M. Nojoumian and D. R. Stinson, (2010). Unconditionally secure first-price auction protocols using a multicomponent commitment scheme, *Proceedings of ICICS2010, Barcelona, SPAIN*. 266-280.

P. Paillier, (1999). Public-key cryptosystems based on composite degree residuosity classes, *Proceedings of the 17th International Conference on Theory and Application of Cryptographic Technique, Prague, Czech Republic*. 223-238.

B. Palmer, K. Bubendorfer, and I. Welch, (2010). A protocol for verification of an auction without

revealing bid values, *Procedia computer science*. 1(1), 2649-2658.

B. Palmer, K. Bubendorfer, and I. Welch, et al (2001). A practical English auction with one-time registration, *Lecture Notes in Computer Science. Springer: Heidelberg,* 2119, 221-234.

G. Perrone, P. Roma, and G. L. Nigro, (2010). Designing multi-attribute auctions for engineering services procurement in new product development in the automotive context, *International journal of production economics*. 124(1), 20-31.

M. O. Rabin, (2005). How to exchange secrets with oblivious transfer, *IACR cryptology eprint archive*. 187.

K. Ray, M. Jenamani, and P. K. J. Mohapatra, (2011). An efficient reverse auction mechanism for limited supplier base, *Electronic Commerce research and applications*. 10(2),170- 182.

Y. Ren, J. Shen, and J. Wang, et al, (2015). Mutual Verifiable Provable Data Auditing in Public Cloud Storage, *Journal of internet technology*. 16(2), 317-323.

R. Sanchez-Iborra, J. Snchez-Gmez, and J. Santa, et al, (2017). Integrating LP-WAN Communications within the Vehicular Ecosystem, *Journal of internet services and information security.* 7(4), 45-56.

P. Schartner and M. Schaffer, (2005). Unique User-Generated Digital Pseudonyms. *Computer network security, springer berlin Heidelberg.* 194-205.

M. Scott, (2007). MIRACL: Multiprecision integer and rational arithmetic c/c++ library, 1988C2007. Homepage at http://www. shamus. ie/.

S. S. Seulgi, J. Choi, and T. Kwon, (2016). A Study on Detectionand Detour Methods against Packet Dropping Attacks in IPv6based IoT, *IT CoNvergence PRActice*. 4(3), 20-27.

J. Shen, H. Tan, and J. Wang, et al, (2015). A Novel Routing Protocol Providing Good Transmission Reliability in Underwater Sensor Networks, *Journal of internet technology*. 16(1), 171-178.

J. Shen, H. Tan, and S. Moh, et al, (2015). Enhanced Secure Sensor Association and Key Management in Wireless Body Area Networks, *Journal of Communications and networks*. 17(5), 453-462.

W. Shi, (2014). A Provable Secure Sealed - Bid Multi-Attribute Auction Scheme Under Semi-Honest Model, *John Wiley and Sons LTD*. 27 (12), 3738-3747.

W. Shi, W. Wei, and J. Wang, et al, (2016). A verifiable sealed-bid multi-qualitative- attribute based auction scheme in the semi-honest model, *IEEE access*. (99): 1-1.

T. R. Srinath, (2011). Samrat Kella, Mamata Jenamani, A New Secure Protocol for Multiat- tribute Multi-round E-reverse Auction Using Online Trusted Third Party, *Second International Conference on Emerging applications of information technology.* 149- 152.

T. R. Srinath, M. P. Singh, and A. R. Pais, (2011). Anonymity and verifiability in multi-attribute reverse auction, *International Journal of information technology convergence and services*. 1(4).

S. Strecker, (2010). Information revelation in multiattribute English auctions: a laboratory study, *Decision support systems*. 49(3), 272-280.

X. Su, H. F. Yu, and W. Kim, C. et al, (2016). Interference cancellation for non-orthogonal multiple access used in future wireless mobile networks, *EURASIP journal on wireless communications and networking*. 231, doi: 10. 1186/s13638-016- 0732-z.

X. Su, C. Liang, and D. Choi, et al, (2016). Power allocation schemes for femto-to-macro downlink interference reduction for smart devices in ambient intelligence, *Mobile information systems*. 1-10.

W. G. Tzeng, (2004). Efficient 1-out-of-n oblivious transfer schemes with universally usable parameters, *IEEE transactions on computers*. 53(2), 232-240.

D. Wang and P. Wang, (2016). On the implications of Zipfs law in passwords, *European Symposium on Research in computer security. Springer International Publishing*. 111-131.

F. S. Wei, J. F. Ma, and Q. Jiang, et al, (2016). Cryptanalysis and improvement of an enhanced two-factor user authentication scheme in wireless sensor networks, *Information technology and control*. 45(1), 62-70.

X. Wen, L. Shao, and Y. Xue et al, (2015). A rapid learning algorithm for vehicle classification, *Information sciences*. 295(1), 395-406.

Z. Xia, X. Wang, and X. Sun, et al, (2014). Steg analysis of least significant bit matching using multi-order differences, *Security and communication networks*. 7(8), 1283-1291.

Z. Xia, X. Wang, and X. Sun, et al, (2015). A Secure and Dynamic Multi-keyword Ranked Search Scheme over Encrypted Cloud Data, *IEEE transactions on parallel and distributed systems*. 27(2), 340-352.

S. Xin, W. Yang, and D. Choi, et al, (2017). Channel allocation and powercontrol schemes for cross-tier 3GPP LTE networks to support multimedia applications, *Multimedia tools and applications*. 1-17.

H. Xiong, Z. Chen, and F. Li, (2012). Bidder-anonymous English auction protocol based on revocable ring signature, *Expert Systems with applications.* 39, 7062-7066.

10 NOTES ON CONTRIBUTORS

Wenbo Shi received the M.S. degree from the Inha University, Incheon, South Korea, in 2007 and the Ph.D. degree from the Inha University, Incheon, South Korea, in 2010. Currently he is an assistant Professor at Northeastern University. His research interests include cryptography, network security.

Jiaqi Wang is currently working toward the Ph.D. degree with the Computer Application Technology from Northeastern University, Shenyang, China, in 2015. Her current research interests include network information security and spectrum auction security.

Jinxiu Zhu born in September 1972, is now an associate professor ,received the B.S. degree in electrical engineering from the Nanjing University of Science and Technology, Nanjing, China, in 1994, and the M.S. in communication and information system and Ph.D. degrees in Electric Power System and Automation from the Hohai University, Nanjing, China, in 2003 and 2008, respectively. She is currently a associate professor at the College of Internet of Things Engineering, Hohai University, China. Her current research interests include image/video processing.

YuPeng Wang received B.E. degree in Communication Engineering from Northeastern University, China, in 2004. He received his master and doctoral degrees in the major of information and telecommunication engineering from Inha University, Korea in 2006 and 2010, respectively. Currently, he is with the College of Electronic and Information Engineering, Shenyang Aerospace University, China. His research interests include Mobile Networks, Ad Hoc Networks, Smart Antennas, and Radio Resource Management.

Dongmin Choi received his B.E. degree from the Kyunghee University in 2003 and M.S. and Ph.D. degrees in computer Science from Chosun University in 2007 and 2011, respectively. Since 2014, he has been a Professor in College of General Education, Chosun University, Gwangju, Korea. His research interests are in information security, sensor network systems, mobile ad-hoc systems, smart grid home network systems, mobile sensor applications, and internet ethics.