A Privacy-preserving Distributed Multi-attribute Reverse Auction Scheme with Public verification using Threshold Paillier cryptosystem

Jiaqi Wang[1], Wenbo Shi[2]*, and Xin Su[3]
[1]Northeastern University, Shenyang 110819,
849598571@qq.com
[2]Northeastern University at Qinhuangdao, Qinhuangdao 066004,
swb319@hotmail.com
[3]College of IOT Engineering, Hohai University Changzhou, 213022,
leosu8622@163.com

Abstract

With the rapid updating of Internet technology, electronic auction network environment is more complex, so the electronic auction security requirements are getting higher and higher. In addition, the study of multi-attribute auction research on security is still very lacking. In this paper, a secure multi-attribute reverse auction scheme is proposed. It uses the paillier threshold homomorphic cryptosystem and multiple servers to prevent conspiracy attack between buyer and auction servers. Moreover, the techniques of oblivious transfer and anonymization are also used to achieve the bidder privacy and anonymity. Finally, the scheme achieves the public verification of auction process and auction results and the security analysis is given.

Keywords: auction, threshold paillier cryptosystem, oblivious transfer, public verification

1 Introduction

The rapid development of the Internet brings people a lot of information resources, which makes peoples' lives more convenient. In the business world, Internet-based e-commerce has become one of the main drivers of economic development. Electronic Auction as an important part of e-commerce and the traditional auction will be transplanted to the Internet[32, 29]. Enterprises or the government through the construction of e-procurement platform, publishing the information about purchased items, then online negotiations and so on to achieve online ordering and payment and finally sending the goods to the buyers according to the logistics distribution line, which completing the entire transaction. Electronic auctions are generally not subject to time and space constraints[30, 4, 6]. Therefore, the transaction is more flexible and convenient and the cost of services is lower, which means that auction items can be more abundant. It is precisely because of these characteristics of electronic auctions, to promote electronic auction has become a huge potential for development of the market, with a very considerable economic prospects[28, 27, 5].

Because at the beginning of the Internet design, people only considers the convenience and openness, which can make the security of the Internet is very fragile, vulnerable to hacker or hacker attacks and invasion.There may be non-standard use of the system and the risk of malicious damage, making the user or the system sensitive information leaked. Therefore, the electronic auction based on Internet

Research Briefs on Information & Communication Technology Evolution (ReBICTE), Vol. 3, Article No. 6 (October 15, 2017)
*Corresponding author: Northeastern University at Qinhuangdao, Qinhuangdao City, Hebei Province,China, Tel: +8613722553385

technology to consumers to bring convenient, fast, cheap and efficient way of trading, but also to the user a lot of security threats, which is electronic auction and even e-commerce research areas to face a huge challenge [31, 1, 14, 10, 19].

The secure electronic auction system is a set of network security protocols and systems for application layer. Among them, various types of auction models are presented in the form of electronic protocols[18, 17, 15, 22]. The main function is that in the distrusted network environment, the system can not only follow the auction model of the auction / sale rules for commodity auctions, but also ensure the user data privacy, data integrity, the fairness of the auction, the auction results of public verification. In addition, we must take the possible internal and external fraud and collusion and other issues into account to ensure that their respective economic interests, privacy information, etc. do not violated[3, 16]. In summary, the security of electronic auction model has become a hot topic in electronic auction research.

So far, the research on auction security for single attribute is very rich, however, research on security for multi-attribute auction is very lacking. With the need for multi-attribute auction security in recent years, the study of secure multi-attribute auction has been paid more and more attention by people. Suzuki et al. 's work [25] is the first paper on the study of multi-attribute security auctions, which incorporates trusted third parties and achieves the confidentiality and public verification of tenders, but the computation method of winner does not consider the weight factor and the bidder can not arbitrarily bid. In addition, the attribute value can not be freely selected. Shi proposed a semi-honest model of qualitative attributes of the sealed bidding multi-attribute auction model [23]. The main concern is the different tender structure under the confidential winners decision-making problem. Srinath et al. proposed two MREA protocols with single and multiple rounds of bidding, using a linear weighting function to determine the auction winner, and using the pseudonym generation algorithm to achieve the anonymity of the bidders [24, 12]. However, both protocols are needed to open the tenders in the computation process. Therefore, there has a weak bid privacy and the public verifiability do not provided.

In this paper, we consider the security problems above to propose a privacy-preserving distributed multi-attribute reverse auction scheme with public verification using Threshold Paillier cryptosystem.Our contributions as follows: (1) our proposed scheme can achieve the bid privacy and anonymity by using the oblivious transfer and anonymization. (2) paillier threshold homomorphic cryptosystem and multiple servers are used to prevent the conspiracy attack between buyer and auctioneer server. (3) proposed scheme achieves the public verifiability of auction process and auction results and security analysis is given. The remainder of this paper is organized as follows: in section 2, we recall some preliminary knowledge including distributed multi - attribute reverse auction model, oblivious transfer, paillier cyptosystem and threshold paillier cryptosystem. We proposed our scheme in section 3 and in section 4, security analysis is given. Finally, we conclude this paper in section 5.

2 Preliminaries

2.1 Distributed multi - attribute reverse auction model

In the distributed multi - attribute reverse auction model, there is a buyer, n distributed servers and a number of bidders. The figure 1 is shown below. Each bidder provides a length of n attribute vector as the bottom of the target: $B_i = \{b_i, \{\alpha_j | 1 \leq j \leq n\}\} (b_i, \alpha_j \in \mathrm{Z}_N)$, b_i is denoted as the price attribute that any bidder provides. $\{\alpha_j\}$ is a non-price attribute vector of length j. The traditional linear addition letter is used as the utility function of the winner decision in the auction model [12]: $Score_i(b_i, AT_i) = -b_i + \sum_{j=1}^{n-1} \omega_j \alpha_j$, which is defined as a non-price attribute set. The price attribute is also given the same weight: $Score_i(AT_i) = \sum_{j=1}^{n} \omega_j \alpha_j$, which denoted as a collection of attributes that contain price attributes. AT_i represents the set of bid attributes provided by the ith bidders. $\{\omega_i\}$ is defined as the

weight of each attribute. After all the auction servers have finished the operation of all the bidders, the buyer can determine the winning bidder by the following formula: $\arg\max_i(Score(b_i, AT_i))$.

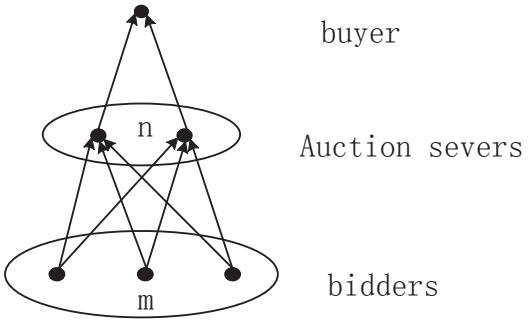


Figure 1: The auction model

2.2 Oblivious transfer

Oblivious transfer is a data transmission protocol that protects the privacy of both parties and enable both sides to send messages in a vague way . Rabin et al designed the earliest the oblivious transfer protocol and achieved the oblivious transfer function of "two chooses one" [21]. Moreover, Tzeng [26] designed the OT_1^n oblivious transfer protocol of "n chooses one" which is a very useful cryptography tool and the protocol is shown in the table 1, where q is a large prime and G_q is a cyclic group of order q. (g,h) is two generators of G_q. Z_q is a finite additive group of q elements and (g,h) can be reused if $\log_g h$ is not revealed.

Table 1: 1-out-of-n oblivious transfer protocol

Protocol 1-out-of-n oblivious transfer (OT_1^n)
parameters input: (g,h,G_q):
Sender Alice's input:$s_1, s_2 \ldots s_n \in G_q$**:**
Receiver Bob's choice: $\varepsilon \in [1,n]$**:**
Receiver Bob can access a specified elements from $\{s_i\}$ and can not get other elements. While sender Alice can not know ε;
(1) Receiver Bob sends ε, $y = g^r h^\varepsilon, r \in_R Z_q$;
(2) Sender Alice replies: $c_j = (g^{t_j}, s_j(y/h^j)^{t_j}), t_j \in_R Z_q, 1 \le j \le n$;
(3)After Bob receiving $\{c_j\}$, $c_\varepsilon = (d,f)$, **sender computes**$s_\varepsilon = f/d^r$;

2.3 Paillier cryptosystem

The Paillier cryptosystem is a homomorphic cryptosystem with additive homology [20]. The scheme consists of the following parts:

Key generation: assume $n = pq$ is RSA- modulus, in other words, p,q are strong primes. Select $\lambda = lcm(p-1, q-1)$ and random integer g to satisfied $\gcd(L(g^\lambda \bmod n^2), n) = 1$ and the $L(\mu) = \frac{\mu-1}{n}$.The public key is (n,g) and the private key is λ.

Encryption: Set the plaintext $m \in Z_n$ to be encrypted and select $r \in_R Z_n^*$ to get the ciphertext $c = g^m r^n \bmod n^2$.

Decryption: plaintext $m = \frac{L(c^{\lambda} \bmod \mathrm{n}^2)}{L(g^{\lambda} \bmod \mathrm{n}^2)} \bmod \mathrm{n}$.

The security of the Paillier cryptosystem depends on the Decisional Composite Residuosity Assumption (DCRA), that is, there is no algorithm in the polynomial time to distinguish whether a modulus is the remaining n of the modulus n^2.

The Paillier cryptosystem satisfies the addition of homomorphism and there are two properties:

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

(2) $D(E(m_1)^k \bmod n^2) = km \bmod n$

2.4 Threshold paillier cryptosystem

When one party knows the secret key to decrypt any ciphertext and violates the privacy of the participant, in order to prevent this possible fraud, threshold paillier cryptosystem is used in our proposed scheme [2, 7, 13]. The threshold Paillier cryptography is the idea of using the threshold password for the Paillier public key cryptography, and there are many application examples in multi-parity security calculations. The four parts of the threshold password system are as follows [9]: key generation algorithm, encryption algorithm, decryption algorithm and combination algorithm. The threshold Paillier password system is introduced and the specific details will be described in detail in the next section. Assume the scheme has a secret publisher D and n participants U_i.

Key generation algorithm: D generates public and private keys (PK, SK) according to the key generation algorithm. Each protocol participant U_i can get a part of the private key sk_i After the algorithm is finished, exit the protocol.

Encryption algorithm: any private key holder can use the public key PK to encrypt the plaintext M and outputs the ciphertext c.

Decryption algorithm: all participants use the partial private key sk_i to "decrypt" c and get a "decrypt" result c_i with the generation of an operational correctness proof $proof_i$.

Combination algorithm: assume that at least $c_1, ..., c_t proof_i$ are verified to be correct $(t \leq n)$ and the ciphertext can restore the plaintext by the langrange interpolation.

3 The proposed scheme

3.1 Initialization phase

In the initialization phase, buyer needs to publish the requirements of goods and corresponding non-price attribute weight set $\{\omega_i\}_{i\in[1,l]}$. Set $\{\alpha_j\}_{1\leq j\leq l}$ to an attribute vector of length l, which represents supply program of bidders including the price, weight and other attributes. Moreover, the trusted third party is set as a threshold paillier homomorphic scheme for key generation and distribution, which denoted as D. D starts the threshold Paillier encryption initialization:

(1) D generates $n = pq$ and satisfies $\gcd(n, \phi(n)) = 1$, which p and q are strong primes. In addition, $p = 2p' + 1$, $q = 2q' + 1$, p' and q' are large primes. Set $m = p'q'$ and randomly generated $\beta \in_R \mathrm{Z}_n^*$ to get the private key $Sk = \beta m$ which can broadcast in all auction servers according to Shamir secret sharing. $f(X) = \sum_{i=0}^{t} a_i X^i$ is computed and $a_0 = \beta m$, $a_i \in [0, nm-1]$. Sub key is sent to the l auction severs $\{P_l\}$ according to the corresponding number and P_i gets the sub key denoted as $s_i = f(i) \bmod \mathrm{nm}$. After distribution, Sk is destroyed.

(2) Select $(a, b) \in Z_n^* \times Z_n^*$ Randomly and let $g = (1+n)^a b^n \bmod \mathrm{n}^2$. The public key Pk is consist (g, n, θ), where $\theta = L(g^{m\beta}) = am\beta \bmod \mathrm{n}$ and be sent to the all bidders through the broadcast channel by D.

(3) Let $VK = v$ is the square number of the composition of the circulation group of $Z_{n^2}^*$ and $\overline{v} = v^{\Delta} \bmod \ \mathrm{n}^2$. The key $VK_i = \overline{v}^{s_i} = v^{s_i} \bmod \ \mathrm{n}^2$ is Verified, where $= l!$. Then public $VK, VK_i (1 \leq i \leq l)$ according to the broadcast channel.

Moreover, Anonymity technology is also used to vague the true identities UID of the bidders [11] and we can get an anonymous identity $PID = E_{Pk}(UID||Pad)||Pk||n$. Pad is a random padding bit and buyer specified the location to fill a certain length. The security and uniqueness of PID is elaborated and discussed in [11]. The PID will be sent in the broadcast channel.

3.2 Bidding phase

After bidders receiving the public key, they use the paillier encryption to encrypt the price attribute and all non-price attributes: $E_{Pk}(-b_i) = -g^{b_i} r_1^n \bmod \ \mathrm{n}^2$, $e_j = E_{Pk}(\alpha_j) = g^{\alpha_j} r_2^n \bmod \ \mathrm{n}^2$, where $r_1, r_2 \in_R \mathrm{Z}_n^*$.

OT_1^n protocol is used to transfer the encrypted attribute value. In addition, $P_{i\in[1,l]}$ is denoted as a auctioneer sever. P_i selects a subscript k randomly and sends the $y = g^r h^k$ to the anonymous bidders, where $r \in_R \mathrm{Z}_n$. Then, an anonymous bidder replies a response set $\{c_1, c_2 ... c_l\}$, where $c_{j\in[1,l]} = (g^{t_j}, e_j(y/h^j)^{t_j})$, $t_j \in_R \mathrm{Z}_n$; P_i selects k corresponding the element $c_k = (d, f)$ in $\{c_1, c_2 ... c_l\}$ and computes: $e_k = f/d^r = e_k(y/h^k)^{t_j}/(g^{t_j})^r = e_k(g^r h^k/h^k)^{t_j}/(g^{t_j})^r$. Finally, bidders send the $E_{Pk}(-b_i)$, $\{e_j\}_{j\in[1,l-1]}$ to the auctioneer server $\{P_l\}_{l\in[1,l-1]}$.

When each $P_{k\in[1,l-1]}$ receives the encrypted attribute value $e_{j\in[1,l-1]}$ sent from bidders, P_k begins to use the threshold Paillier encryption of homomorphic properties to compute the weighted attribute values.

For plaintext $m_1 \in \mathrm{Z}_n, r_1 \in_R \mathrm{Z}_n^*$, threshold Paillier satisfies the formula: $D(E(m_1, r_1)^{\lambda} \bmod \ \mathrm{n}^2) = \lambda m_1 \bmod \ \mathrm{n}$.

P_k can get the weighted attribute values $\omega_j \alpha_j$ in the ciphertext: $E_{Pk}(AT_{ij}) = e_j^{\omega_j}$.

When finish the computation, all $\{P_k\}$ will send the $E_{Pk}(AT_{ij})$ to the P_l and compute the final weight accroding to the formula $Score_i(b_i, AT_i) = -b_i + \sum_{j=1}^{n-1} \omega_j \alpha_j$:

$$E_{Pk}(Score(AT_i)) = \prod_{j=1}^{l-1} AT_{ij} = \prod_{j=1}^{l-1} e_j^{\omega_j}$$

$$E_{Pk}(Score_i(b_i, AT_i)) = E_{Pk}(AT_i) * E_{Pk}(-b_i)$$

Then, P_l sends the $E_{Pk}(Score_i(b_i, AT_i))$ to the rest of the auction server in the broadcast channel.

3.3 Winner determination phase

When $\{P_i\}_{i\in[1,l]}$ gets the $E_{Pk}(Score_i(b_i, AT_i))$ in the broadcast channel, P_i uses the s_i to partially decrypt. Set $E_{Pk}(Score_i(b_i, AT_i))$ as c. P_i computes $c_i = c^{2\Delta s_i} \bmod \ \mathrm{n}^2$ and generates the correctness proof $proof_i$ which is discussed in detail in the next section. P_i sends the $(c_i, proof_i)$ to the buyer and result publisher.

At this phase, assume that the buyer is honest and has received no less than valid c_i of t, which can recover the plaintext according to the combinational algorithm. The buyer can not recover the $Score_i(b_i, AT_i)$ if buyer receives the effective part of the decryption less than t. Otherwise, recover the weight and plaintext by the following formula:

$$Score_i(b_i, AT_i) = L(\prod_{j\in S} c_j^{2\mu_{0,j}^S} \bmod \ \mathrm{n}^2) \times \frac{1}{4(l!)^2 \theta} \bmod \ \mathrm{n}$$

where $\mu_{0,j}^S = \Delta \times \prod_{j'\in S\setminus\{j\}} \frac{j'}{j'-j} \in \mathrm{Z}$. After computing the bids, buyer can choose the most satisfactory supply options and then the auction ends. Figure 2 describes the flow of the protocol.

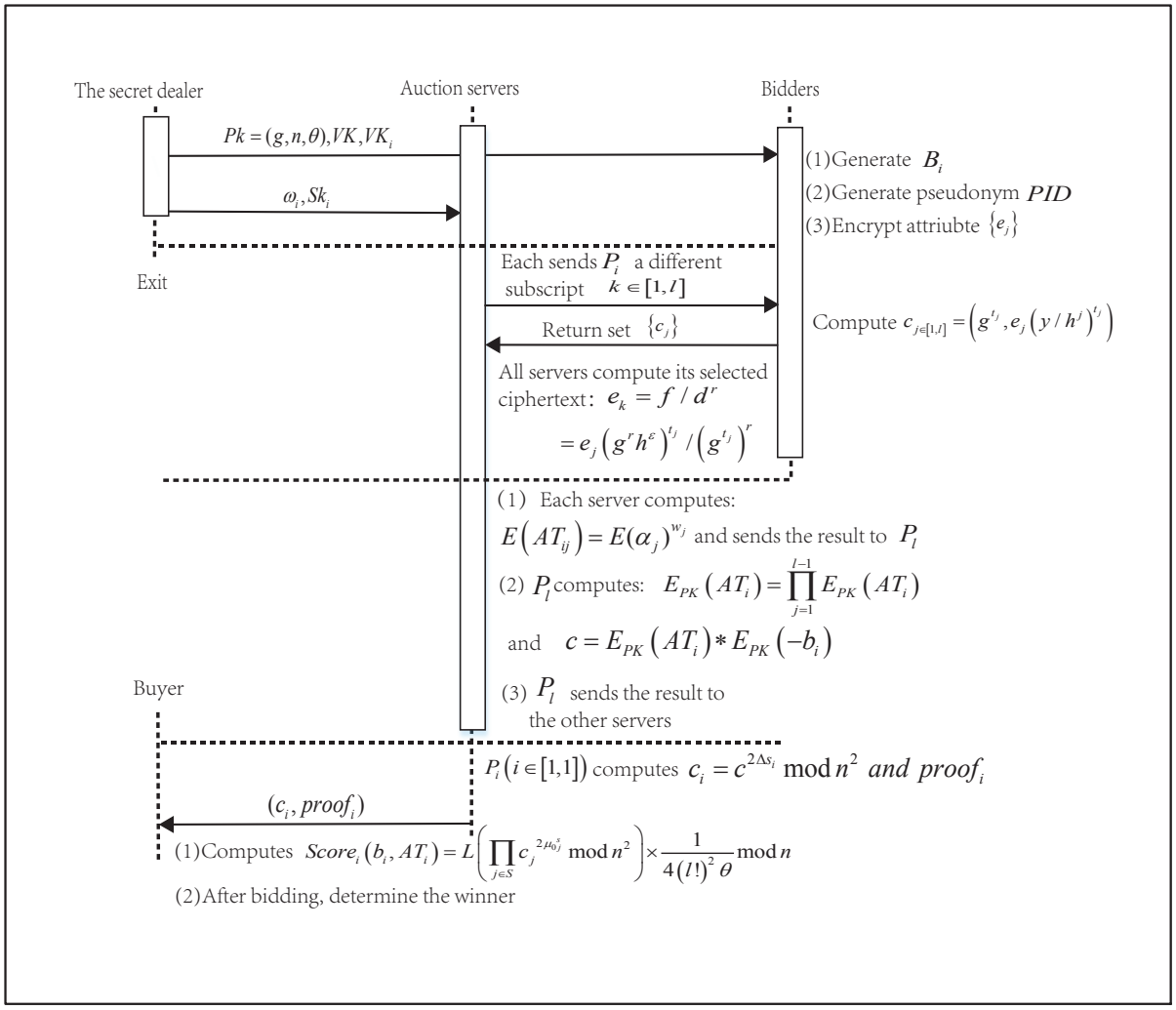


Figure 2: The flow chart of protocol

4 Security analysis

4.1 Public verification analysis and proof

Public verifiability is a very important research in electronic auction and secure multi-party computation. It is an effective method of protecting the privacy of participants in a distributed environment. [9] proposed zero-knowledge interaction protocols for the threshold paillier encryption scheme. According to the validity of multi-attribute encryption values and the correctness of partial decryption private key sharing in multi-attribute electronic auctions, protect the secret do not reveal in this paper, a zero-knowledge proof process based on this two protocols for two honest participants is constructed. There are two ciphertext validity issues that need to be publicly verified:

(1) To prove the weight of the auction server encryption and $E_{Pk}(Score_i(b_i,AT_i))$ decryption when using the correct part of the private key s_i without exposing the true value of s_i.

(2) To prove that the auction server P_i receives the encrypted attribute ciphertext e_j must come from the corresponding set of plaintext attributes $\{\alpha_j\}$ without revealing the actual value of e_j.

4.1.1 Interactive proof of correctness for partial decryption private key sharing

In our proposed scheme, auction server $\{P_i\}_{i\in[1,l-1]}$ needs to prove to some trusted third party that when ciphertext c generates partial decryption c_i, auction server $\{P_i\}_{i\in[1,l-1]}$ uses the correct partial private key s_j without revealing the true information of s_j.

According to our proposed scheme, the public inputs:

(1) Two large prime product n, where $p = 2p' + 1, q = 2q' + 1$;

(2) $|n| = k$ ($|n|$ represents the length of a bit string when n is a binary), $\xi = p'q'$;

(3) $VK = \overline{v} = v^{\Delta} \bmod n^2, VK_i = \overline{v}^{s_i} = v^{\Delta s_i} \bmod n^2$;

(4) $\overline{c} = c^{4\Delta} \bmod n^2, c_i^2 = \overline{c}^{s_i} = c^{4\Delta s_i} \bmod n^2$.

The prover P inputs input secretly $s_i \in \mathrm{Z}_{n\xi}$, and prove to the verifier V that it knows that $s_i \in \mathrm{Z}_{n\xi}$ satisfies the following equation:

$$VK_i = (\overline{v})^{s_i} = (v^{\Delta})^{s_i} \bmod n^2,$$

$\overline{c}^{s_i} = (c^{4\Delta} \bmod n^2)^{s_i} \bmod n^2$ or $\log_{\overline{c}}(c_i^2) = \log_{\overline{v}}(VK_i)$.

(1) P generates a random number $w \in_R \mathrm{Z}_n$ and computes $(x, y) \to (\overline{c}^w, \overline{v}^w)$. Then sends (x, y) to the verifier V;

(2) V selects $e \in_R \mathrm{Z}_{n\xi}$ and sends e to P;

(3) P computes $r = w + s_i e$ and r sends to V;

(4) V verifies $\overline{c}^r \stackrel{?}{=} x(c_i^2)^e$ and $\overline{v}^r \stackrel{?}{=} y(VK_i)^e$;

The flow figure 3 is shown below.

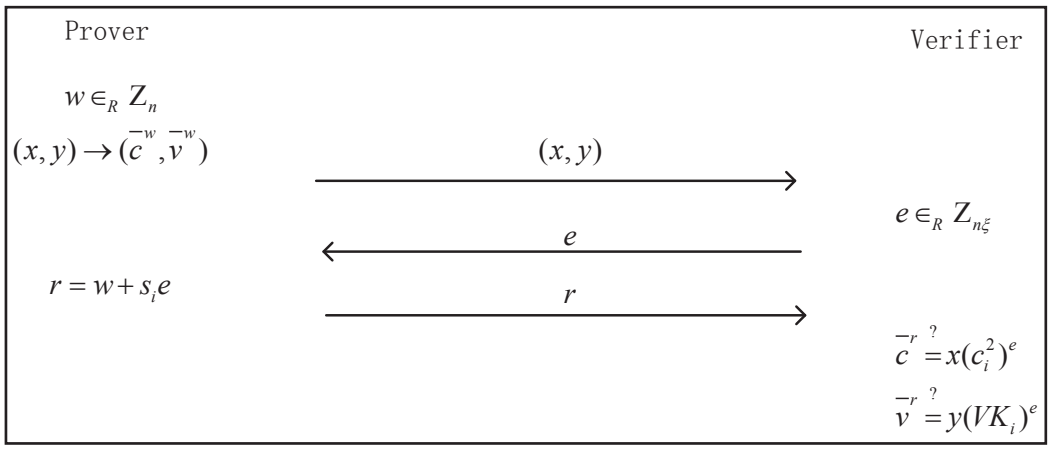


Figure 3: The flow chart for the interactive proof of partial decryption's correctness

4.1.2 Non-interactive proof of correctness for partial decryption private key sharing

Because of the communication cost of the protocol for interactive zero-knowledge proof is high, it is necessary to convert the interactive zero-knowledge proof protocol into non-interactive zero-knowledge proof. Fiat-Shamir proposed a "heuristic approach" [8] that uses a hash function to convert the zero-knowledge proof protocol of a honest verifier into a digital signature scheme. In addition, it uses the $(Commit, Challenge, Response)$ to represent a copy of the integrity of a honest verifier.

Set H as a hash function with an output length of L and $n = pq$, where $p = 2p' + 1, q = 2q' + 1$, the bit length of n is n and denoted as $\overline{c} = c^{4\Delta} \bmod \mathrm{n}^2, \overline{c}^{s_i} = c^{4\Delta s_i} \bmod \mathrm{n}^2$. The non-interactive method is as follows :

Prover computes the commitment $(a,b) \leftarrow (\overline{v}^{s_i} \bmod \mathrm{n}^2, \overline{c}^{s_i} \bmod \mathrm{n}^2)$ and uses the hash function to compute the challenge $e = H(a,b,\overline{v},\overline{c},\overline{v}^w,\overline{c}^w)$, where $w \in \{0,1,...,2^{2k+2L}-1\}$; then compute the response $r = es_i + w,\ r \in \{0,1,...,2^{2k+2L}-1\}$. The proof for correctness of private key sharing is $proof_i = (e,r)$;

Verifier verifies that whether the equation $e \stackrel{?}{=} H(a,b,\overline{v},\overline{c},\overline{v}^r a^{-e},\overline{c}^r b^{-e})$ is valid or not to prove if is valid.

4.1.3 Interactive proof of validity for attribute ciphertext

Our proposed scheme verifies that auction server $P_{i\in[1,l]}$ can prove that the received ciphertext attribute $e_{j\in[1,l-1]}$ is valid for any honest bidders. Let $P_{i\in[1,l]}$ receives the attribute ciphertext as e_j and corresponding attribute plaintext as α_j. The proof of the remaining attributes is similar.

According to our proposed scheme, the public inputs:

(1)Two large prime product n,

where $p = 2p' + 1, q = 2q' + 1$; $S = \{\alpha_1, \alpha_2, \alpha_3\}$, $e_j/g_{,}^{\alpha_1} e_j/g_{,}^{\alpha_2} e_j/g^{\alpha_3}$;

(2)$e_j = g^{m_j} r^n \bmod \mathrm{n}^2$, where $r \in_R \mathrm{Z}_n^*$ and The subscript j is kept secret.

Verifier P randomly selects $x, b_1, b_2 \in_R \mathrm{Z}_n$, and computes $u_1 = g^{b_1} \bmod \mathrm{n}^2$, $u_2 = g^{b_2} \bmod \mathrm{n}^2$; after selecting $w_1, w_2 \in \mathrm{Z}_n$, P computes the commitment:

$$v_1 = u_1^n (g^{\alpha_1}/e_j)^{w_1} \bmod n^2, v_2 = u_2^n (g^{\alpha_2}/e_j)^{w_2} \bmod n^2, v_3 = g^{xn} \bmod n^2$$

Then P sends the $\{v_1, v_2, v_3\}$ to V and generates a response $w \in_R \mathrm{Z}_n$ randomly. P computes $w_3 = w - (w_1 + w_2) \bmod n$ and $u_3^n = g^{nx} r^{nw_3} g^{w_3(\alpha_3' - \alpha_3)} \bmod n^2$, where α_3' is the actual cihpertext of ciphertext e_3 generated by P. If $\alpha_3' \in S$, P is an honest verifier. Otherwise, $\alpha_3' \notin S$, is dishonest and $\alpha_3' \neq \alpha_3$. P sends $\{u_1^n, u_2^n, u_3^n, w_1, w_2, w_3\}$ to V and verifies the validity of the encrypted attribute by determining whether the following equation is true or not.

$$u_1^n \stackrel{?}{=} v_1 (e_j/g^{\alpha_1})^{w_1} \bmod n^2, u_2^n \stackrel{?}{=} v_2 (e_j/g^{\alpha_2})^{w_2} \bmod n^2$$

$$u_3^n \stackrel{?}{=} v_3 (e_j/g^{\alpha_3})^{w_3} \bmod n^2, e \stackrel{?}{=} e_1 + e_2 + e_3 \bmod n$$

The flow figure 4 is shown below.

4.1.4 Non-interactive proof of validity for attribute ciphertext

P randomly selects $\{x_1, x_2\} \in_R H, \{w_1, w_2\}, x \in_R \mathrm{Z}_N$ and computes P and V inputs together: $y_1 = x_1^n (g^{\alpha_1}/e_j)^{w_1} \bmod n^2$, $y_2 = x_2^n (g^{\alpha_2}/e_j)^{w_2} \bmod n^2$ and $y_3 = g^{rn} \bmod n^2$. a challenge is generated:

$$e = H(y_1, y_2, y_3, e_j/g^{\alpha_1}, e_j/g^{\alpha_2}, e_j/g^{\alpha_3})$$

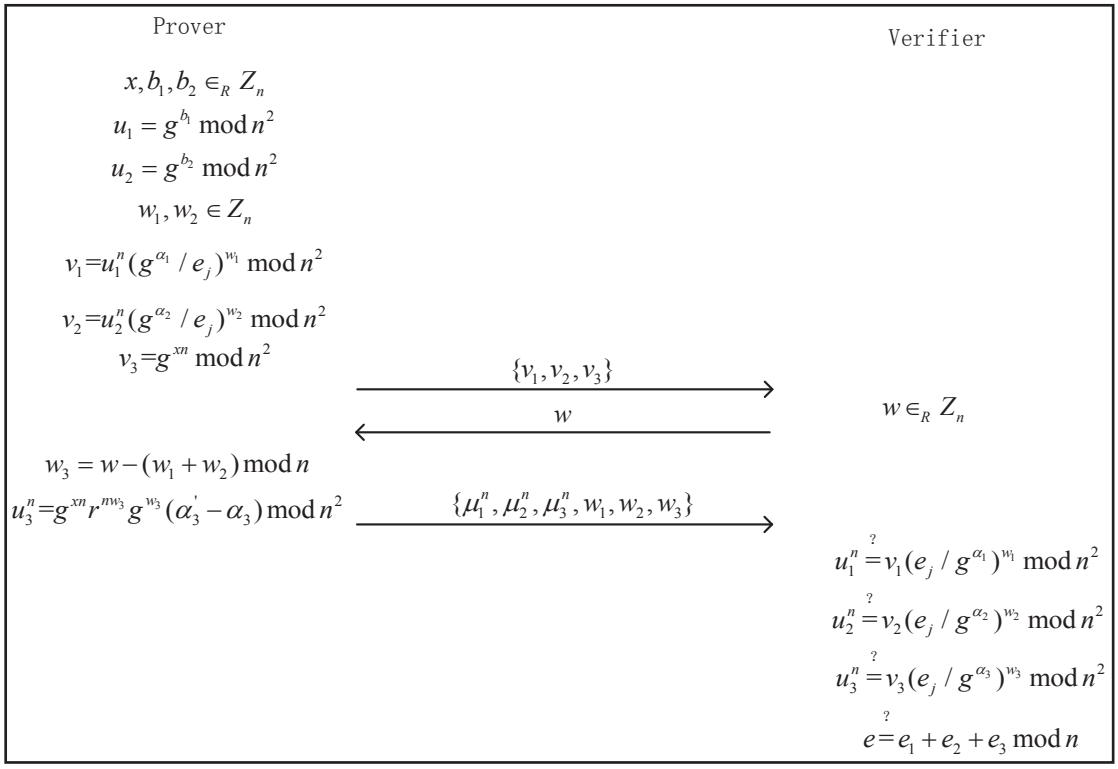


Figure 4: The flow chart of the interactive proof of ciphertext 's validity

And computes the response $w_3 = e - (w_1 + w_2) \bmod n$ to generate $x_3^n = g^{nx} r^{nw_3} g^{w_3(\alpha_3' - \alpha_3)} \bmod n$. V verifies the validity of the encrypted attribute by determining whether the following equation is true or not.

$$e \stackrel{?}{=} H(y_1, y_2, y_3, e_j/g^{\alpha_1}, e_j/g^{\alpha_2}, e_j/g^{\alpha_3})$$

$$y_1^n \stackrel{?}{=} x_1 (e_j/g^{\alpha_1})^{w_1} \bmod n^2, \quad y_2^n \stackrel{?}{=} x_2 (e_j/g^{\alpha_2})^{w_2} \bmod n^2$$

$$y_3^n \stackrel{?}{=} x_3 (e_j/g^{\alpha_3})^{w_3} \bmod n^2, \quad e \stackrel{?}{=} w_1 + w_2 + w_3 \bmod n$$

4.2 Other security

(1) Anonymity : at the phase of the initialization, each buyer has an temporary identity pseudonym to participate in the auction and buyers achieve the anonymity according to the private key.

(2) Fairness: paillier threshold encryption is used in our proposed scheme. Therefore, there is no collusion between buyers and auction servers. In addition, there is no conspiracy attack between seller and any other two sides neither because of using the technique of oblivious transfer and identity anonymity.

(3)Public verifiability: zero proof of knowledge is used by buyer to verify the commitment of auction servers, which can achieve the public verifiability of decryption operation.

5 Conclusion

In this paper, a privacy-preserving distributed multi-attribute reverse auction scheme with Public verification using Threshold Paillier cryptosystem is proposed. It uses the paillier threshold homomorphic

cryptosystem and multiple servers to prevent conspiracy attack between buyer and auction servers. The techniques of oblivious transfer and anonymization in our scheme can achieve the bidder privacy and anonymity. Finally, the scheme achieves the public verification of auction process and auction results and the security analysis is given to demonstrate that our scheme has a strong security and can prevent the conspiracy attack of each two party.

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).

References

[1] A. Aly and M. V. Vyve. Practically efficient secure single-commodity multi-market auctions. In *Proc. of the International Conference on Financial Cryptography and Data Security (FC'16), Christ Church, Barbados*, pages 110–129. Springer-Verlag, February 2016.

[2] O. Baudron, P. A. Fouque, D. Pointcheval, J. Stern, and G. Poupard. Practical multi-candidate election system. In *Proc. of the 20th ACM Annual Symposium on Principles on Distributed Computing (PODC'01), Newport, Rhode Island, USA*, pages 274–283. ACM, August 2001.

[3] A. Bektaş, M. S. Kiraz, and O. Uzunkol. A secure and efficient protocol for electronic treasury auctions. In *Proc. of the 1st International Conference on Cryptography and Information Security in the Balkans (BalkanCryptSec'14), Istanbul, Turkey, LNCS*, volume 9024, pages 123–140. Springer-Verlag, October 2014.

[4] G. Cao. Secure and efficient electronic auction scheme with strong anonymity. *Journal of Networks*, 9(8):2189–2194, August 2014.

[5] G. Cao and J. Chen. Practical electronic auction scheme based on untrusted third-party. In *Proc. of the 5th International Conference on Computational and Information Sciences (ICCIS'13), Shiyang, China*, pages 493–496. IEEE, June 2013.

[6] C. C. Chang, T. F. Cheng, and W. Y. Chen. A novel electronic english auction system with a secure on-shelf mechanism. *IEEE Transactions on Information Forensics & Security*, 8(4):657–668, April 2013.

[7] D. Chaum and T. P. Pedersen. Wallet databases with observers. In *Proc. of the 12th Annual International Cryptology Conference (Crypto'92), Santa Barbara, California, USA, LNCS*, volume 740, pages 89–105. Springer-Verlag, August 1992.

[8] R. Cramer, I. Damgård, and J. B. Nielsen. Multiparty computation from threshold homomorphic encryption. In *Proc. of the International Conference on the Theory and Application of Cryptographic Techniques (EUROCRYPT'01), Innsbruck, Austria, LNCS*, volume 2045, pages 280–299. Springer-Verlag, May 2001.

[9] I. Damgå rd and M. Jurik. A generalisation, a simplication and some applications of paillier's probabilistic public-key system. In *Proc. of the 4th International Workshop on Practice and Theory in Public Key Cryptography (PKC'01), Jeju Island, South Korea*, volume 7, pages 119–136, February 2001.

[10] R. K. Das, S. K. Nayak, S. K. Bhoi, S. K. Choudhury, B. Majhi, and S. Mohanty. Bsea: A blind sealed-bid e-auction scheme for e-commerce applications. *Computers*, 5(4), December 2016.

[11] M. K. Franklin and M. K. Reiter. The design and implementation of a secure auction service. *IEEE Transactions on Software Engineering*, 22(5):302–312, May 1996.

[12] T. R. S. S. K. M. Jenamani. A new secure protocol for multi-attribute multi-round e-reverse auction using online trusted third party. In *Proc. of the 2nd International Conference on Emerging Applications of Information Technology (EAIT'11), Kolkata, India*, pages 149–152. IEEE, February 2011.

[13] M. Jurik and J. B. Nielsen. A generalization of paillier's public-key system with applications to electronic voting. *International Journal of Information Security*, 9(6):371–385, December 2010.

[14] J. S. Lee, K. J. Wei, Y. C. Chen, and Y. H. Sun. Provable secure brand-new multi-auction mechanism with dynamic identity. *Ksii Transactions on Internet & Information Systems*, 10(12), December 2016.

[15] W. Li, M. Larson, C. Hu, R. Li, X. Cheng, and R. Bie. Secure multi-unit sealed first-price auction mechanisms. *Security & Communication Networks*, 9(16):3833–3843, November 2016.

[16] W. Li, S. Wang, and X. Cheng. Truthful multi-attribute auction with discriminatory pricing in cognitive radio networks. In *Proc. of the 1st ACM Workshop on Cognitive radio architectures for broadband (CRAB'13), Miami, Florida, USA*, pages 21–30. ACM, October 2013.

[17] X. Liu and D. Wang. Bidding evaluation behavior analysis of grouped multi-attribute reverse auction based on qualitative simulation. *Journal of Northeastern University*, 33(3):314–317+322, 2012.

[18] B.-C. M., C. F., and G. L. et al. 3.28 qualitative and multi-attribute learning from diverse data collections. *Functoriality in Geometric Data*, 17(3):314–317+322, 2017.

[19] T. Mitsunaga, Y. Manabe, and T. Okamoto. A secure m + 1st price auction protocol based on bit slice circuits. volume 99, pages 1591–1599, 2016.

[20] P. Paillier. Public-key cryptosystems based on composite degree residuosity classes. In *Proc. of the International Conference on Theory and Application of Cryptographic Techniques (EUROCRYPT'99), Prague, Czech Republic, LNCS*, volume 1592, pages 223–238. Springer-Verlag, May 1999.

[21] M. O. Rabin. How to exchange secrets with oblivious transfer. Technical report, Harvard University, October 2005.

[22] S. Sadaoui and S. K. Shil. A multi-attribute auction mechanism based on conditional constraints and conditional qualitative preferences. *Journal of theoretical and applied electronic commerce research*, 11(1):1–25, January 2016.

[23] W. Shi. A sealed-bid multi-attribute auction protocol with strong bid privacy and bidder privacy. *Security & Communication Networks*, 6(10):1281–1289, October 2013.

[24] T. R. Srinath, M. P. Singh, and A. R. Pais. Anonymity and verifiability in multi-attribute reverse auction. *International Journal of Information Technology Convergence and Services (IJITCS)*, 1(4), August 2011.

[25] K. Suzuki and M. Yokoo. Secure multi-attribute procurement auction. *Proc. of the 6th International Workshop on Information Security Applications (WISA'05), Jeju Island, South Korea, LNCS*, 3786:306–317, August 2005.

[26] W. G. Tzeng. Efficient 1-out-of-n oblivious transfer schemes with universally usable parameters. *IEEE Transactions on Computers*, 53(2):232–240, 2004.

[27] A. Wahaballa, Z. Qin, H. Xiong, Z. Qin, and M. Ramadan. A taxonomy of secure electronic english auction protocols. *International Journal of Computers & Applications*, 37(1):28–36, May 2015.

[28] W. X, Z. X, and e. a. GAO M. An efficient sealed-bid electronic auction scheme. *Journal of Qingdao University (Natural Science Edition)*, (1):64–69, 2015.

[29] K.-W. Yeow, S.-H. Heng, and S.-Y. Tan. From sealed-bid electronic auction to electronic cheque. In *Proc. of the International Conference on Information Science and Applications (ICISA'17), Macau, China*, pages 366–376. Springer-Verlag, March 2017.

[30] K.-W. Yeow, S.-H. Heng, and S.-Y. Tan. Known bid attack on an electronic sealed-bid auction scheme. In *Proc. of the International Conference on Information Science and Applications (ICISA'17), Macau, China*, pages 306–314. Springer-Verlag, March 2017.

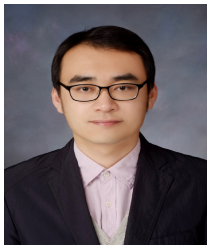
[31] K.-W. Yeow, S.-H. Heng, and S.-Y. Tan. On the security of two sealed-bid auction schemes. In *Proc. of the 19th International Conference on Advanced Communication Technology (ICACT'17), Bongpyeong, South Korea*, pages 58–63. IEEE, February 2017.

[32] H. Zhong, S. Li, T. F. Cheng, and C. C. Chang. An efficient electronic english auction system with a secure on-shelf mechanism and privacy preserving. *Journal of Electrical and Computer Engineering*, 2016:1–14, March 2016.

Author Biography

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.

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.



Xin Su received B.E. degree in Computer Engineering from kunming University of Science and Technology, China, in 2008. He received his M.E. in computer engineering from Chosun University,Korea,in 2010.In 2015, he received his Ph.D. degree in the Program in IT & Media Convergence Studies, Inha University,Korea. He is currently with the College of Internet of Things Engineering,Hohai University,China. his research interests include 3GPP LTE(-A) systems, MIMO beamforming, non-orthogonal multiple access(NOMA),antenna pattem and polarization-based MIMO systems, wireless backhaul solutions,and mobile ad-hoc networks.