Received September 19, 2016, accepted October 24, 2016, date of publication November 3, 2016, date of current version July 24, 2017.

Digital Object Identifier 10.1109/ACCESS.2016.2624558

A Verifiable Sealed-Bid Multi-Qualitative-Attribute Based Auction Scheme in the Semi-Honest Model

WENBO SHI[1,2], (Member, IEEE), WEI WEI[3], (Member, IEEE), JIAQI WANG[4], (Member, IEEE), QINGCHUN ZHAO[1], (Member, IEEE), ZHUO LIN[5], (Member, IEEE), AND HUIHUI WANG[6], (Member, IEEE)

[1]School of Computer and Communication Engineering, Northeastern University, Qinhuangdao 066004, China
[2]School of Computer and Software, Nanjing University of Information Science and Technology, Nanjing 210044, China
[3]School of Computer Science and Engineering, Xi'an University of Technology, Xi'an 710048, China
[4]Department of Computer Science and Engineering, Northeastern University, Shenyang 110819, China
[5]School of Mathematics and Information Science and Technology, Hebei Normal University of Science and Technology, Qinhuangdao 066004, China
[6]Department of Engineering, Jacksonville University, Jacksonville, FL 32211, USA

Corresponding author: Wei Wei (taneo@126.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 61472074, Grant 61602099, Grant 11301414, Grant 11226173, and Grant 61472318, in part by the Hebei Province Top Young Talents, in part by the Priority Academic Program Development of Jiangsu Higher Education Institutions, in part by the Jiangsu Collaborative Innovation Center on Atmospheric Environment and Equipment Technology, in part by the West Virginia Higher Education Policy Commission under Grant FRT2W762W, in part by the Beilin District 2012 High-tech Plan, Xi'an, China, under Grant GX1504, in part by the Xi'an Science and Technology Project under Grant CXY1440(6), in part by the Shanxi Scientific Research under Grant 2014k07-11, in part by the Scientific Research Program Funded by Shanxi Provincial Education Department under Grant 2013JK1139, in part by the China Postdoctoral Science Foundation under Grant 2013M542370, in part by the Specialized Research Fund for the Doctoral Program of Higher Education of China under Grant 20136118120010.

ABSTRACT Recently, several privacy–preserving auction schemes are proposed for protecting the bid privacy and securing the auction. In this paper, a sealed-bid auction scheme focusing on multi-attribute is presented. And it mainly concentrates on the security issues of multi-qualitative-attribute auction and utilizes the Pedersen commitment scheme to bind the bid information into commitment for strong bid privacy. In order to accomplish the public verifiable correctness, the buyers and sellers construct the zero-knowledge signatures of knowledge and publish them to the bulletin board. In accordance with the security analysis, major properties, strong bid privacy and public verifiability, are provided under the semi-honest model. According to a comparison of computation, the proposal's computation cost is reasonable.

INDEX TERMS Multi-attribute e-auction, bid privacy, public verifiability, semi-honest model, multi-party computation.

I. INTRODUCTION

The development of the Internet and information technology completely changed the way that people solve the traditional problems [1]–[17]. While, it also brings a variety of security and privacy issues [18]–[23]. A security protocol can ensure the security of the applications by using the cryptographic methods and it can perform a security-related function. In order to solve these practical security problems, many cryptographic protocols including real authentication [24], [25], keyword search in encrypted cloud [26]–[28],verifiable data auditing in Cloud [29] are proposed. These approaches have played a very important role in security protocol design.

With the rapid development of the Internet and the fast economic growth, E-commerce plays an important role in facilitating economic activity and service level. Especially, e-auction has played a very important role in e-commerce times and it has been applied to various fields with assorted environments. Multi-attribute e-auction, which is a primary mechanism, can automate negotiations in electronic commerce and it supports auto-negotiation multiple attributes in the transaction.

Secure multi-party computation, which creates methods for parties to jointly compute a function over their inputs while revealing nothing but the result of the function, is an

2169-3536 © 2016 IEEE. Translations and content mining are permitted for academic research only.
Personal use is also permitted, but republication/redistribution requires IEEE permission.
See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

important subfield of modern cryptography. E-auction is just one application of many examples in the secure multi-party computation.

Follow the development of the market demands, people have more requirements and are no longer satisfied with the price as the only critical measurement to determine who is the winner of an auction. The concept of 'Configurable offer' is proposed by Bichler and Kalagnanam. It not only characterizes the possible configurations of a configurable offer as a set of quantitative and qualitative attributes but also defines the constraints on the association of attribute values and discounts, markups according to some combination of attribute values [30]. Engel and Wellman propose a multi-attribute auction which accommodates Generalized Additive Independent(GAI) preferences and maintains prices on potentially overlapping GAI clusters of attributes and provides an open competition among suppliers over a multi-dimensional domain [31]. Singh and Benyoucef propose a novel fuzzy winner determinate method TOPSIS (Technique for Order Preference by Similarity to Ideal Solution) defining many kinds of utility functions and calculating the ratio of deviation from the positive ideal offer with the deviation from the negative ideal offer [32]. A multi-attribute bid structure is proposed by Ray et al. [33]. Price and non-price attributes are included in their multi-attribute bid. While the bid structure of Ray et al. just describes the dependent relationship between price attribute and corresponding non-price quantity attribute and independent relationship among non-price qualitative attributes. However, [30] and [31] define the dependence of qualitative attributes and the logical constraints of qualitative attributes are not pressed by those bid structures, which have a influence on the quantitative attributes. Some researchers believe that the interdependent relation among attributes may be used for evaluating a solution [34], [35]. To overcome this issue about dependence, they utilize ANP(Analytic Network Process)in place of AHP(Analytic Hierarchy Process) to enhance the ability of processing the interdependent relations among attributes. Moreover, they make full use of the TOPSIS for more evaluation to avoid rank reversal phenomenon and so on [34].

A secure multi-attribute protocol requiring online Trusted Third Party (TTP) is proposed by Srinath et al. [36]. In [36], the bid privacy is weak because of the computation of score function. Furthermore, public verifiability can not be provided in [36]. Srinath et al.'s second protocol utilizes homomorphic properties of Paillier cryptosystem for achieving bid privacy and public verifiability [37], [38]. However, because a bid needs to be revealed to auctioneer during the auction, so the bid privacy is still weak [38].

A scoring function is described as: $S = \sum_{r=1}^{K} w_r \cdot f_r(x_r) - P$ in [36] and [38]. Where, S denotes the total score of the bid evaluation, K denotes the number of non-price attributes, x_r denotes the value of the r^{th} attribute organized by the seller, w_r denotes the weight associated with the attribute, $f_r(\cdot)$ denotes the valuation function corresponding to the attribute, and P denotes the bid price [36]. It indicates that $f_r(\cdot)$ only evaluate independent attribute instead of interdependent attribute relation. So the winner determination model of [36] and [38] is based on the assumption that a multi-attribute bid can be evaluated to value through linear scoring function S. Finally, Homomorphic properties of Paillier cryptosystem is adopted for number comparison under encryption in Srinath et al.' scheme.

Multi-attribute e-auction is still facing many security issues. Security problems should receive more attention and concern. Security requirements, such as anonymity, traceability, unforgeability, are defined by the researchers who focus on the security issues in e-auction [39]–[42]. Even though researchers have already solved some security problems of multi-attribute e-auction which are mentioned above, multi-qualitative-attribute e-auction mechanism introduces several new security issues, such as multi-attribute privacy-preserving winner determination. Based on Shi's scheme [43], a verifiable sealed-bid multi-qualitative-attribute based e-auction protocol is proposed. It adopts the Mayer and Wetzel's scheme and mainly focuses on strong bid privacy and public verifiable correctness under semi-honest model [44]. It utilizes the Pedersen commitment scheme to bind the bid information into commitment for the strong bid privacy. In order to accomplish the public verifiable correctness, the buyers and sellers construct the Zero-knowledge signatures of knowledge and publish them to the bulletin board.

II. PRELIMINARIES

A. SEMI-HONEST MODEL

Following their prescribed actions in the protocol, all parties are supposed to perform computations and message exchanges under the semi-honest model. They may possibly record whatever they perform and try their best to guess as much information as they can during the protocol. Every party could launch arbitrary polynomial-time calculations deviating from the prescribe protocol actions. A standard definition form Goldreich is adopted [45], [46].

Definition 1: Let $S \subseteq \{0, 1\}^*$.Two aggregations (indexed by S),$X \overset{def}{=} \{X_\omega\}_{\omega inS}$ and $Y \overset{def}{=} \{Y_\omega\}_{\omega inS}$ are computationally indistinguishable if there is a negligible function μ for every family of polynomial-size circuits, $\{D_n\}_{n\in N}, N \rightarrow [0, 1]$, so that $|pr[D_n(\omega, X_\omega) = 1] - pr[D_n(\omega, Y_\omega) = 1]| < \mu(|\omega|)$. 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

$$\{S_1(x, f(x, y))\}_{x,y\in\{0,1\}^*} \overset{c}{\equiv} \{view_1^\pi(x, y)\}_{x,y\in\{0,1\}^*},$$
$$\{S_2(x, f(x, y))\}_{x,y\in\{0,1\}^*} \overset{c}{\equiv} \{view_2^\pi(x, y)\}_{x,y\in\{0,1\}^*},$$

where $|x| = |y|$.

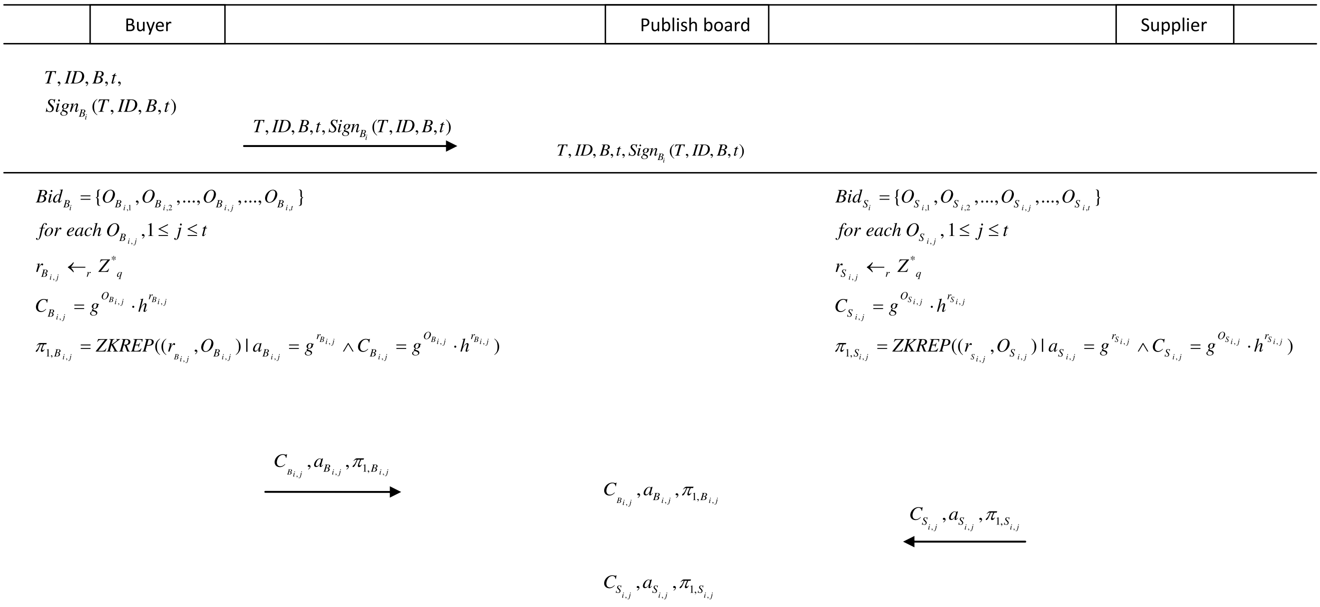

Buyer
Publish board
Supplier
$T, ID, B, t,$
$Sign_{B_i}(T, ID, B, t)$
$T, ID, B, t, Sign_{B_i}(T, ID, B, t)$
$T, ID, B, t, Sign_{B_i}(T, ID, B, t)$
$Bid_{B_i} = \{O_{B_{i,1}}, O_{B_{i,2}}, ..., O_{B_{i,j}}, ..., O_{B_{i,t}}\}$
for each $O_{B_{i,j}}, 1 \le j \le t$
$r_{B_{i,j}} \leftarrow_r Z^*_q$
$C_{B_{i,j}} = g^{O_{B_{i,j}}} \cdot h^{r_{B_{i,j}}}$
$\pi_{1,B_{i,j}} = ZKREP((r_{B_{i,j}}, O_{B_{i,j}}) | a_{B_{i,j}} = g^{r_{B_{i,j}}} \wedge C_{B_{i,j}} = g^{O_{B_{i,j}}} \cdot h^{r_{B_{i,j}}})$
$Bid_{S_i} = \{O_{S_{i,1}}, O_{S_{i,2}}, ..., O_{S_{i,j}}, ..., O_{S_{i,t}}\}$
for each $O_{S_{i,j}}, 1 \le j \le t$
$r_{S_{i,j}} \leftarrow_r Z^*_q$
$C_{S_{i,j}} = g^{O_{S_{i,j}}} \cdot h^{r_{S_{i,j}}}$
$\pi_{1,S_{i,j}} = ZKREP((r_{S_{i,j}}, O_{S_{i,j}}) | a_{S_{i,j}} = g^{r_{S_{i,j}}} \wedge C_{S_{i,j}} = g^{O_{S_{i,j}}} \cdot h^{r_{S_{i,j}}})$
$C_{B_{i,j}}, a_{B_{i,j}}, \pi_{1,B_{i,j}}$
$C_{B_{i,j}}, a_{B_{i,j}}, \pi_{1,B_{i,j}}$
$C_{S_{i,j}}, a_{S_{i,j}}, \pi_{1,S_{i,j}}$
$C_{S_{i,j}}, a_{S_{i,j}}, \pi_{1,S_{i,j}}$

FIGURE 1. **The planning and bidding phase.**

B. ZERO-KNOWLEDGE SIGNATURES OF KNOWLEDGE

Let p, q be large primes such that $q|p - 1$. let Z_q^* be the cyclic subgroup of Z_p^* of order q with independently chosen, random generators g, h. The public parameters are g, h, p, q.

1) SIGNATURE OF KNOWLEDGE OF DISCRETE LOGARITHM

The prover chooses a random $t \in_r Z_q^*$ and computes $c = H(y, g, g^t)$ and $r = t - c \cdot e$. The verifier can check whether $c = H(y, g, g^r g^c)$ given c and r. It is denoted by $ZKDL(e|y = g^e)$ [47].

2) SIGNATURE OF KNOWLEDGE OF EQUALITY OF TWO DISCRETE LOGARITHMS

The prover chooses a random $t \in_r Z_q^*$ and computes $c = H(y_1, y_2, g, h, g^t, h^t)$ and $r = t - c \cdot e$. The verifier can check whether $c = H(y_1, y_2, g, h, g^r y_1^c, h^r y_2^c)$, given c and r. It is denoted by $ZKEDL(e|y_1 = g^e \wedge y_2 = h^e)$ [48].

3) SIGNATURE OF KNOWLEDGE OF REPRESENTATION

The prover chooses a random $t_i \in_r Z_q^*$ for i=1,2 and computes $c = H(y_1, y_2, g, h, g^{t_1}, g^{t_2} \cdot h^{t_1})$ and $r_i = t_i - c \cdot e_i$ for i=1,2. The verifier can check whether $c = H(y_1, y_2, g, h, y_1^c \cdot g^{r_1}, y_2{}^c \cdot g^{r_2} \cdot h^{r_1})$, given c and r_1,r_2. It is denoted by $ZKREP((e_1, e_2)|y_1 = g^{e_1} \wedge y_2 = g^{e_2} \cdot h^{e_1})$ [49].

C. PEDERSEN COMMITMENT SCHEME

An information-theoretically hiding commitment scheme by Pedersen is computationally binding under the discrete logarithm assumption [50]. To commit a $x \in Z_q^*$, the sender generates $r \leftarrow_r Z_q^\star$ and compute $C_x = g^x \cdot h^r$. To open a commitment, the sender reveal x and r, the receiver verifies whether $C_x = g^x \cdot h^r$.

III. PROPOSED SCHEME

As shown in Figure 1 and 2, the proposed scheme is composed of the planning phase,the bidding phase and the winner determination and verification phase.

Assume that there exist M buyers and n sellers in the auction scheme. A bulletin board is established for publishing auction information. A Certification Authority (CA) is adopted in key pre-distribution process. For digital signature, public/private key pairs are arranged in the buyer and seller groups. A buyer B_i can sign message x as $Sign_{B_i}(x)$, where $1 \le i \le M$. A seller S_i's signature of x is denoted as $Sign_{S_i}(x)$, where $1 \le i \le n$. The buyer group publishes the attribute sets $A = \{a_1, \ldots, a_i, \ldots, a_m\}$, where $1 \le i \le m$, m denotes the cardinality of A. There is a corresponding attribute-value set $a_i = (a_{i_1}, \ldots, a_{i_j}, \ldots, a_{i_k})$ for each element in A, a_{i_j} denotes a bit string of length l, j denotes whether a attribute-value $a_{i,j} \in \{0, 1\}^l$, $1 \le j \le k$ is defined or not, k denotes the number of attribute-value. O_j denotes a configurable offer $O_j = (o_1, \ldots, o_i, \ldots, o_{k_1})$, each element o_i is collected from each a_i, where $1 \le i \le k_1$, $1 \le j \le t$, $o_i \in a_i$, k_1 denotes the cardinality of O_j. Assume that each buyer B_i sort his offer set $Bid_{B_i} = \{O_{B_{i,1}}, \ldots, O_{B_{i,j}}, \ldots, O_{B_{i,t}}\}$ according to his preferences as $O_{B_{i,1}} < \ldots < O_{B_{i,j}} < \ldots < O_{B_{i,t}}$.

Let p, q be large primes such that $q|p - 1$. let Z_q^* be the cyclic subgroup of Z_p^* of order q with independently chosen, random generators g, h. The public parameters are g, h, p, q.

A. PLANNING

$T_{deadline}$ denotes the auction deadline, ID denotes the identity of a buy B_i, B denotes the auction attribute sets, where $B \subseteq A$, t denotes the cardinality of a bid, B_i signs T, ID, B, t and publishes $T, ID, B, t, Sign_{B_i}(T, ID, B, t)$ in the bulletin board.

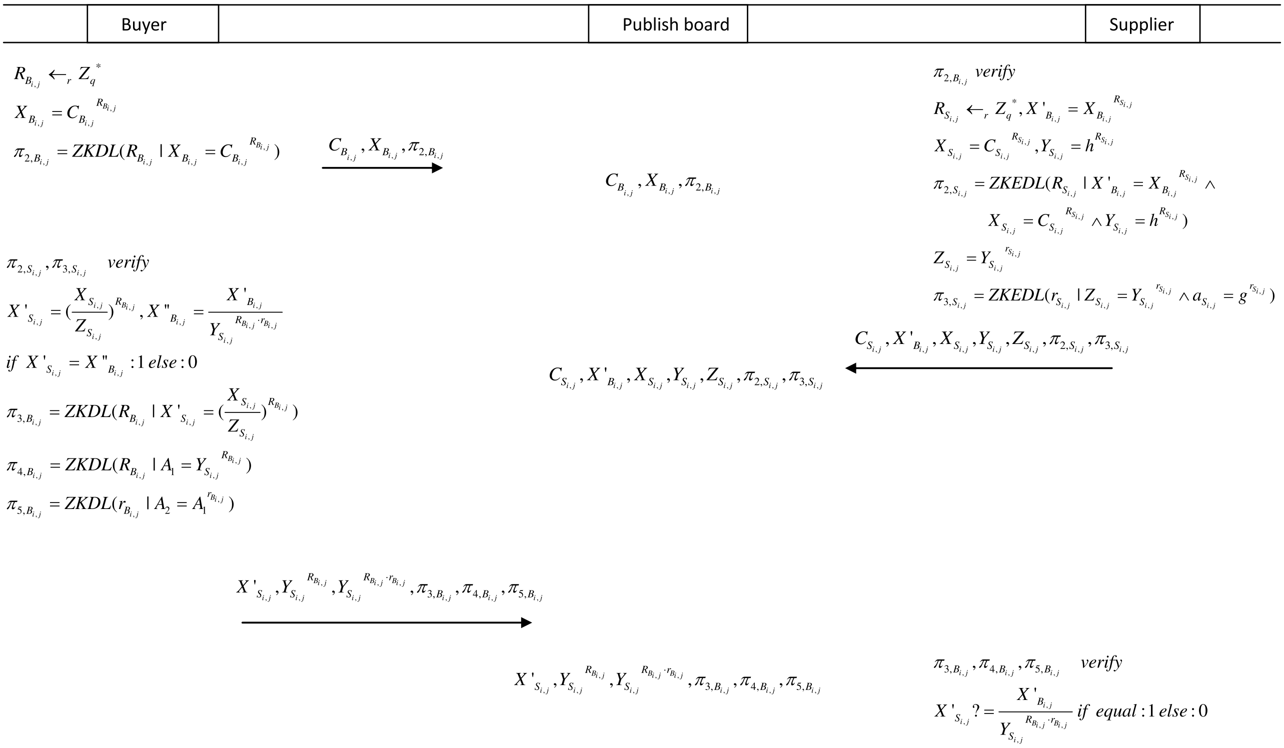

Buyer
Publish board
Supplier
$R_{B_{i,j}} \leftarrow_r Z_q^*$
$X_{B_{i,j}} = C_{B_{i,j}}^{R_{B_{i,j}}}$
$\pi_{2,B_{i,j}} = ZKDL(R_{B_{i,j}} \mid X_{B_{i,j}} = C_{B_{i,j}}^{R_{B_{i,j}}})$
$C_{B_{i,j}}, X_{B_{i,j}}, \pi_{2,B_{i,j}}$
$C_{B_{i,j}}, X_{B_{i,j}}, \pi_{2,B_{i,j}}$
$\pi_{2,B_{i,j}}$ verify
$R_{S_{i,j}} \leftarrow_r Z_q^*, X'_{B_{i,j}} = X_{B_{i,j}}^{R_{S_{i,j}}}$
$X_{S_{i,j}} = C_{S_{i,j}}^{R_{S_{i,j}}}, Y_{S_{i,j}} = h^{R_{S_{i,j}}}$
$\pi_{2,S_{i,j}} = ZKEDL(R_{S_{i,j}} \mid X'_{B_{i,j}} = X_{B_{i,j}}^{R_{S_{i,j}}} \wedge X_{S_{i,j}} = C_{S_{i,j}}^{R_{S_{i,j}}} \wedge Y_{S_{i,j}} = h^{R_{S_{i,j}}})$
$Z_{S_{i,j}} = Y_{S_{i,j}}^{r_{S_{i,j}}}$
$\pi_{3,S_{i,j}} = ZKEDL(r_{S_{i,j}} \mid Z_{S_{i,j}} = Y_{S_{i,j}}^{r_{S_{i,j}}} \wedge a_{S_{i,j}} = g^{r_{S_{i,j}}})$
$C_{S_{i,j}}, X'_{B_{i,j}}, X_{S_{i,j}}, Y_{S_{i,j}}, Z_{S_{i,j}}, \pi_{2,S_{i,j}}, \pi_{3,S_{i,j}}$
$C_{S_{i,j}}, X'_{B_{i,j}}, X_{S_{i,j}}, Y_{S_{i,j}}, Z_{S_{i,j}}, \pi_{2,S_{i,j}}, \pi_{3,S_{i,j}}$
$\pi_{2,S_{i,j}}, \pi_{3,S_{i,j}}$ verify
$X'_{S_{i,j}} = (\frac{X_{S_{i,j}}}{Z_{S_{i,j}}})^{R_{B_{i,j}}}, X''_{B_{i,j}} = \frac{X'_{B_{i,j}}}{Y_{S_{i,j}}^{R_{B_{i,j}} \cdot r_{B_{i,j}}}}$
if $X'_{S_{i,j}} = X''_{B_{i,j}}$:1 else : 0
$\pi_{3,B_{i,j}} = ZKDL(R_{B_{i,j}} \mid X'_{S_{i,j}} = (\frac{X_{S_{i,j}}}{Z_{S_{i,j}}})^{R_{B_{i,j}}})$
$\pi_{4,B_{i,j}} = ZKDL(R_{B_{i,j}} \mid A_1 = Y_{S_{i,j}}^{R_{B_{i,j}}})$
$\pi_{5,B_{i,j}} = ZKDL(r_{B_{i,j}} \mid A_2 = A_1^{r_{B_{i,j}}})$
$X'_{S_{i,j}}, Y_{S_{i,j}}^{R_{B_{i,j}}}, Y_{S_{i,j}}^{R_{B_{i,j}} \cdot r_{B_{i,j}}}, \pi_{3,B_{i,j}}, \pi_{4,B_{i,j}}, \pi_{5,B_{i,j}}$
$X'_{S_{i,j}}, Y_{S_{i,j}}^{R_{B_{i,j}}}, Y_{S_{i,j}}^{R_{B_{i,j}} \cdot r_{B_{i,j}}}, \pi_{3,B_{i,j}}, \pi_{4,B_{i,j}}, \pi_{5,B_{i,j}}$
$\pi_{3,B_{i,j}}, \pi_{4,B_{i,j}}, \pi_{5,B_{i,j}}$ verify
$X'_{S_{i,j}} ? = \frac{X'_{B_{i,j}}}{Y_{S_{i,j}}^{R_{B_{i,j}} \cdot r_{B_{i,j}}}}$ if equal :1 else : 0

FIGURE 2. The winner determination phase.

B. BIDDING

(1) B organizes offer $Bid_{B_i} = \{O_{B_{i,1}}, \ldots, O_{B_{i,j}}, \ldots, O_{B_{i,t}}\}$, where $1 \le i \le M, 1 \le j \le t$. For each $O_{B_{i,j}}$, B generates $r_{B_{i,j}} \leftarrow_r Z_q^\star$, and computes $C_{B_{i,j}} = g^{O_{B_{i,j}}} \cdot h^{r_{B_{i,j}}}$, $\pi_{1,B_{i,j}} = ZKREP((r_{B_{i,j}}, O_{B_{i,j}}) \mid a_{B_{i,j}} = g^{r_{B_{i,j}}} \wedge C_{B_{i,j}} = g^{O_{B_{i,j}}} \cdot h^{r_{B_{i,j}}})$, $Sign_{B_i}(C_{B_{i,j}}, a_{B_{i,j}}, \pi_{1,B_{i,j}})$. Then B publishes $C_{B_{i,j}}, a_{B_{i,j}}, \pi_{1,B_{i,j}}, Sign_{B_i}(C_{B_{i,j}}, a_{B_{i,j}}, \pi_{1,B_{i,j}})$ on bulletin board.

(2) S organizes offer $Bid_{S_i} = \{O_{S_{i,1}}, \ldots, O_{S_{i,j}}, \ldots, O_{S_{i,t}}\}$, where $1 \le i \le n$, $1 \le j \le t$. For each $O_{S_{i,j}}$, S generates $r_{S_{i,j}} \leftarrow_r Z_q^\star$, and computes $C_{S_{i,j}} = g^{O_{S_{i,j}}} \cdot h^{r_{S_{i,j}}}$, $\pi_{1,S_{i,j}} = ZKREP\,((r_{S_{i,j}}, O_{S_{i,j}}) \mid a_{S_{i,j}} = g^{r_{S_{i,j}}} \wedge C_{S_{i,j}} = g^{O_{S_{i,j}}} \cdot h^{r_{S_{i,j}}})$, $Sign_{S_i}(C_{S_{i,j}}, a_{S_{i,j}}, \pi_{1,S_{i,j}})$. Then S publishes $C_{S_{i,j}}, a_{S_{i,j}}, \pi_{1,S_{i,j}}, Sign_{S_i}(C_{S_{i,j}}, a_{S_{i,j}}, \pi_{1,S_{i,j}})$ on bulletin board.

(3) If any $\pi_{1,B_{i,j}}$ does not verify, S_i abort.

(4) If any $\pi_{1,S_{i,j}}$ does not verify, B_i abort.

C. WINNER DETERMINATION AND VERIFICATION

(1) B generates $R_{B_{i,j}} \leftarrow_r Z_q^\star$ and computes $X_{B_{i,j}} = C_{B_{i,j}}^{R_{B_{i,j}}}$, $\pi_{2,B_{i,j}} = ZKDL(R_{B_{i,j}} \mid X_{B_{i,j}} = C_{B_{i,j}}^{R_{B_{i,j}}})$, $Sign_{B_i}(C_{B_{i,j}}, X_{B_{i,j}}, \pi_{2,B_{i,j}})$. Then publishes $C_{B_{i,j}}, X_{B_{i,j}}$, $\pi_{2,B_{i,j}}, Sign_{B_i}(C_{B_{i,j}}, X_{B_{i,j}}, \pi_{2,B_{i,j}})$.

(2) If S verifies the proof $\pi_{2,B_{i,j}}$, then S generates $R_{S_{i,j}} \leftarrow_r Z_q^\star$ and computes $X'_{B_{i,j}} = X_{B_{i,j}}^{R_{S_{i,j}}}$, $X_{S_{i,j}} = C_{S_{i,j}}^{R_{S_{i,j}}}$, $Y_{S_{i,j}} = h^{R_{S_{i,j}}}$, $\pi_{2,S_{i,j}} = ZKEDL(R_{S_{i,j}} \mid X'_{B_{i,j}} = X_{B_{i,j}}^{R_{S_{i,j}}} \wedge X_{S_{i,j}} = C_{S_{i,j}}^{R_{S_{i,j}}} \wedge Y_{S_{i,j}} = h^{R_{S_{i,j}}})$, $Z_{S_{i,j}} = Y_{S_{i,j}}^{r_{S_{i,j}}}$, $\pi_{3,S_{i,j}} = ZKEDL(r_{S_{i,j}} \mid Z_{S_{i,j}} = Y_{S_{i,j}}^{r_{S_{i,j}}} \wedge a_{S_{i,j}} = g^{r_{S_{i,j}}})$, $Sign_{S_i}(C_{S_{i,j}}, X'_{B_{i,j}}, X_{S_{i,j}}, Y_{S_{i,j}}, Z_{S_{i,j}}, \pi_{2,S_{i,j}}, \pi_{3,S_{i,j}})$. Then publishes $C_{S_{i,j}}, X'_{B_{i,j}}, X_{S_{i,j}}, Y_{S_{i,j}}, Z_{S_{i,j}}, \pi_{2,S_{i,j}}, \pi_{3,S_{i,j}}, Sign_{S_i}(C_{S_{i,j}}, X'_{B_{i,j}}, X_{S_{i,j}}, Y_{S_{i,j}}, Z_{S_{i,j}}, \pi_{2,S_{i,j}}, \pi_{3,S_{i,j}})$.

(3) If B verifies the proof $\pi_{2,S_{i,j}}, \pi_{3,S_{i,j}}$, then computes $X'_{S_{i,j}} = (\frac{X_{S_{i,j}}}{Z_{S_{i,j}}})^{R_{B_{i,j}}}$,$X''_{B_{i,j}} = \frac{X'_{B_{i,j}}}{Y_{S_{i,j}}^{R_{B_{i,j}} \cdot r_{B_{i,j}}}}$. If $X'_{S_{i,j}} = X''_{B_{i,j}}$, then $O_{B_{i,j}} = O_{S_{i,j}}$, else $O_{B_{i,j}} \neq O_{S_{i,j}}$. Then computes $\pi_{3,B_{i,j}} = ZKDL(R_{B_{i,j}} \mid X'_{S_{i,j}} = (\frac{X_{S_{i,j}}}{Z_{S_{i,j}}})^{R_{S_{i,j}}})$, $\pi_{4,B_{i,j}} = ZKDL(R_{B_{i,j}} \mid A_1 = Y_{S_{i,j}}^{R_{B_{i,j}}})$, $\pi_{5,B_{i,j}} = ZKDL(r_{B_{i,j}} \mid A_2 = A_1^{r_{B_{i,j}}})$, $Sign_{B_i}(X'_{S_{i,j}}, Y_{S_{i,j}}^{R_{B_{i,j}}}, Y_{S_{i,j}}^{R_{B_{i,j}} \cdot r_{B_{i,j}}}, \pi_{3,B_{i,j}}, \pi_{4,B_{i,j}}, \pi_{5,B_{i,j}})$. Then publishes $X'_{S_{i,j}}$,$Y_{S_{i,j}}^{R_{B_{i,j}}}$, $Y_{S_{i,j}}^{R_{B_{i,j}} \cdot r_{B_{i,j}}}$, $\pi_{3,B_{i,j}}$, $\pi_{4,B_{i,j}}$, $\pi_{5,B_{i,j}}$, $Sign_{B_i}(X'_{S_{i,j}}$,$Y_{S_{i,j}}^{R_{B_{i,j}}}$,$Y_{S_{i,j}}^{R_{B_{i,j}} \cdot r_{B_{i,j}}}$,$\pi_{3,B_{i,j}}$,$\pi_{4,B_{i,j}}$,$\pi_{5,B_{i,j}})$.

(4) If S verifies the proof $\pi_{3,B_{i,j}}, \pi_{4,B_{i,j}}, \pi_{5,B_{i,j}}$, then checks $X'_{S_{i,j}} ? = \frac{X'_{B_{i,j}}}{Y_{S_{i,j}}^{R_{B_{i,j}} \cdot r_{B_{i,j}}}}$. If $X'_{S_{i,j}} = \frac{X'_{B_{i,j}}}{Y_{S_{i,j}}^{R_{B_{i,j}} \cdot r_{B_{i,j}}}}$, then $O_{S_{i,j}} = O_{B_{i,j}}$, else $O_{S_{i,j}} \neq O_{B_{i,j}}$.

According to B_i's preferences $O_{B_{i,1}} < \ldots < O_{B_{i,j}} < \ldots < O_{B_{i,t}}$, gets the biggest index number j of $O_{B_{i,j}}$ for each seller S_i, where $O_{S_{i,j}} = O_{B_{i,j}}$, the seller who possesses the j will be the winner. The winner determination process can be checked and verified by other sellers in the same way.

IV. SECURITY ANALYSIS

Theorem 1: Assume that the buyer B_i organizes $Bid_{B_i} = \{O_{B_{i,1}}, \ldots, O_{B_{i,j}}, \ldots, O_{B_{i,t}}\}$ sorted according to B_i's preferences $O_{B_{i,1}} < \ldots < O_{B_{i,j}} < \ldots < O_{B_{i,t}}$. The seller S_i organizes $Bids_{S_i} = \{O_{S_{i,1}}, \ldots, O_{S_{i,j}}, \ldots, O_{S_{i,t}}\}$. After bidding phase, B_i and S_i commit to their bids, make proofs for their bids, and verify each other's bid.

Proof: After B_i organizes Bid_{B_i}, then B_i generates $r_{B_{i,j}}$ and computes commitment $C_{B_{i,j}} = g^{O_{B_{i,j}}} \cdot h^{r_{B_{i,j}}}$ in which B_i binds and hides $O_{B_{i,j}}$,$a_{B_{i,j}} = g^{r_{B_{i,j}}}$. No one other than B_i is able to compute $C_{B_{i,j}}$ because of the intractable discrete logarithm problem [51].

To prove the knowledge $r_{B_{i,j}}$, $O_{B_{i,j}}$ subject to $a_{B_{i,j}} = g^{r_{B_{i,j}}} \wedge C_{B_{i,j}} = g^{O_{B_{i,j}}} \cdot h^{r_{B_{i,j}}}$, B_i generates t_1, t_2 and computes $c = H(a_{B_{i,j}}, C_{B_{i,j}}, g, h, g^{t_1}, g^{t_2} \cdot h^{t_1})$, $r_1 = t_1 - c \cdot r_{B_{i,j}}$, $r_2 = t_2 - c \cdot O_{B_{i,j}}$. After gets c, r_1, r_2, S_i checks the equation $c? = H(a_{B_{i,j}}, C_{B_{i,j}}, g, h, a^c_{B_{i,j}} \cdot g^{r_1}, C^c_{B_{i,j}} \cdot g^{r_2} \cdot h^{r_1})$. First, it can easily be seen that an honest prover will always succeed in constructing a valid proof since

$$\begin{aligned} a^c_{B_{i,j}} \cdot g^{r_1} &= (g^{r_{B_{i,j}}})^c \cdot g^{t_1 - c \cdot r_{B_{i,j}}} = g^{t_1}, \\ C^c_{B_{i,j}} \cdot g^{r_2} \cdot h^{r_1} &= g^{c \cdot O_{B_{i,j}}} \cdot h^{c \cdot r_{B_{i,j}}} \cdot g^{t_2 - c \cdot O_{B_{i,j}}} \cdot h^{t_1 - c \cdot r_{B_{i,j}}} \\ &= g^{t_2} \cdot h^{t_1}. \end{aligned}$$

Second, assume that a cheating prover who does not know $r_{B_{i,j}}$ and $O_{B_{i,j}}$ is able to compute such proofs. Since the hash function is hard to invert, we can assume that the values $a^c_{B_{i,j}} \cdot g^{r_1}$ and $C^c_{B_{i,j}} \cdot g^{r_2} \cdot h^{r_1}$ are fixed before c is computed. It also seems necessary to prepared to compute a proof for many other possible c when fixing the values $a^c_{B_{i,j}} \cdot g^{r_1}$ and $C^c_{B_{i,j}} \cdot g^{r_2} \cdot h^{r_1}$ for the prover. But it means that the cheating prover could also compute different representations of $a^c_{B_{i,j}} \cdot g^{r_1}$ and $C^c_{B_{i,j}} \cdot g^{r_2} \cdot h^{r_1}$ to the bases g and h, which implies the knowledge of $r_{B_{i,j}}$ and $O_{B_{i,j}}$, the discrete logarithm of $a_{B_{i,j}}$ and $C_{B_{i,j}}$ to the base g and h, it contradicts the assumption that the cheating prover does not know $r_{B_{i,j}}$ and $O_{B_{i,j}}$. That means that no one except B_i is able to make proofs for his bid.

S_i can be proved by the same way.

Theorem 2: In the winner determination phase, B_i compares $O_{B_{i,j}}$ with $O_{S_{i,j}}$ of S_i and verifies whether the bid is $O_{S_{i,j}}$; S_i compares $O_{S_{i,j}}$ with $O_{B_{i,j}}$ of B_i and verifies whether the bid is $O_{B_{i,j}}$.

Proof: B_i generates $R_{B_{i,j}} \leftarrow_r Z^\star_q$ and computes $X_{B_{i,j}} = C^{R_{B_{i,j}}}_{B_{i,j}}$, $\pi_{2,B_{i,j}} = ZKDL(R_{B_{i,j}} \mid X_{B_{i,j}} = C^{R_{B_{i,j}}}_{B_{i,j}})$, $Sign_{B_i}(C_{B_{i,j}}, X_{B_{i,j}}, \pi_{2,B_{i,j}})$. Then publishes $C_{B_{i,j}}, X_{B_{i,j}}, \pi_{2,B_{i,j}}$, $Sign_{B_i}(C_{B_{i,j}}, X_{B_{i,j}}, \pi_{2,B_{i,j}})$ on bulletin board. After S_i verifies $\pi_{2,B_{i,j}}$ and checks whether the bid equals $O_{B_{i,j}}$. Then S_i generates $R_{S_{i,j}} \leftarrow_r Z^\star_q$ and computes $X'_{B_{i,j}} = X^{R_{S_{i,j}}}_{B_{i,j}}$, $X_{S_{i,j}} = C^{R_{S_{i,j}}}_{S_{i,j}}$, $Y_{S_{i,j}} = h^{R_{S_{i,j}}}$, $\pi_{2,S_{i,j}} = ZKEDL(R_{S_{i,j}} \mid X'_{B_{i,j}} = X^{R_{S_{i,j}}}_{B_{i,j}} \wedge X_{S_{i,j}} = C^{R_{S_{i,j}}}_{S_{i,j}} \wedge Y_{S_{i,j}} = h^{R_{S_{i,j}}})$, $Z_{S_{i,j}} = Y^{r_{S_{i,j}}}_{S_{i,j}}$, $\pi_{3,S_{i,j}} = ZKEDL(r_{S_{i,j}} \mid Z_{S_{i,j}} = Y^{r_{S_{i,j}}}_{S_{i,j}} \wedge a_{S_{i,j}} = g^{r_{S_{i,j}}})$,$Sign_{S_i}(C_{S_{i,j}}, X'_{B_{i,j}}, X_{S_{i,j}}, Y_{S_{i,j}}, Z_{S_{i,j}}, \pi_{2,S_{i,j}}, \pi_{3,S_{i,j}})$. Then publishes $C_{S_{i,j}}, X'_{B_{i,j}}, X_{S_{i,j}}, Y_{S_{i,j}}, Z_{S_{i,j}}, \pi_{2,S_{i,j}}, \pi_{3,S_{i,j}}$, $Sign_{S_i}(C_{S_{i,j}}, X'_{B_{i,j}}, X_{S_{i,j}}, Y_{S_{i,j}}, Z_{S_{i,j}}, \pi_{2,S_{i,j}}, \pi_{3,S_{i,j}})$. After B_i verifies the proof $\pi_{2,S_{i,j}}, \pi_{3,S_{i,j}}$ and checks whether the bid equals $O_{S_{i,j}}$.

Theorem 3: In the winner determination phase, if $X'_{S_{i,j}} = X''_{B_{i,j}}$, then $O_{S_{i,j}} = O_{B_{i,j}}$.

Proof:

$$\begin{aligned} X'_{S_{i,j}} &= (\frac{X_{S_{i,j}}}{Z_{S_{i,j}}})^{R_{B_{i,j}}} = (\frac{C^{R_{S_{i,j}}}_{S_{i,j}}}{Y^{r_{S_{i,j}}}_{S_{i,j}}})^{R_{B_{i,j}}} = (\frac{(g^{O_{S_{i,j}}} \cdot h^{r_{S_{i,j}}})^{R_{S_{i,j}}}}{h^{R_{S_{i,j}} r_{S_{i,j}}}})^{R_{B_{i,j}}} \\ &= g^{O_{S_{i,j}} \cdot R_{S_{i,j}} \cdot R_{B_{i,j}}} \\ X''_{B_{i,j}} &= \frac{X'_{B_{i,j}}}{Y^{R_{B_{i,j}} \cdot r_{B_{i,j}}}_{S_{i,j}}} = \frac{X^{R_{S_{i,j}}}_{B_{i,j}}}{(h^{R_{S_{i,j}}})^{R_{B_{i,j}} \cdot r_{B_{i,j}}}} = \frac{C^{R_{B_{i,j}} \cdot R_{S_{i,j}}}_{B_{i,j}}}{(h^{R_{S_{i,j}}})^{R_{B_{i,j}} \cdot r_{B_{i,j}}}} \\ &= \frac{(g^{O_{B_{i,j}}} \cdot h^{r_{B_{i,j}}})^{R_{B_{i,j}} \cdot R_{S_{i,j}}}}{(h^{R_{S_{i,j}}})^{R_{B_{i,j}} \cdot r_{B_{i,j}}}} = g^{O_{B_{i,j}} \cdot R_{S_{i,j}} \cdot R_{B_{i,j}}} \end{aligned}$$

If $X'_{S_{i,j}} = X''_{B_{i,j}}$, then $g^{O_{S_{i,j}} \cdot R_{S_{i,j}} \cdot R_{B_{i,j}}} = g^{O_{B_{i,j}} \cdot R_{S_{i,j}} \cdot R_{B_{i,j}}} \Rightarrow O_{S_{i,j}} = O_{B_{i,j}}$

Theorem 4: Privacy of $O_{B_{i,j}}$ and $O_{S_{i,j}}$ is provided from the bidding phase to the winner determine phase.

Proof: In the bidding phase, $O_{S_{i,j}}$ is bound by $C_{B_{i,j}}$, where $C_{B_{i,j}} = g^{O_{B_{i,j}}} \cdot h^{r_{B_{i,j}}}$. Even though an attacker gets the $r_{B_{i,j}}$, the attacker still needs to face the intractable discrete logarithm problem [51]. In the winner determine phase, $O_{S_{i,j}}$ is still protected by $C_{B_{i,j}}$. Privacy of $O_{B_{i,j}}$ and $O_{S_{i,j}}$ is provided throughout the process.

Theorem 5: After B_i publishes the winner result, each S_i can verify the winner determination result in the winner determine phase.

Proof: Firstly, each B_i verifies the comparison of $O_{B_{i,j}}$ and $O_{S_{i,j}}$ by following theorem 4.2. After B_i publishes $X'_{S_{i,j}}, Y^{R_{B_{i,j}}}_{S_{i,j}}, Y^{R_{B_{i,j}} \cdot r_{B_{i,j}}}_{S_{i,j}}, \pi_{3,B_{i,j}}, \pi_{4,B_{i,j}}, \pi_{5,B_{i,j}}$, $Sign_{B_i}(X'_{S_{i,j}}, Y^{R_{B_{i,j}}}_{S_{i,j}}, Y^{R_{B_{i,j}} \cdot r_{B_{i,j}}}_{S_{i,j}}, \pi_{3,B_{i,j}}, \pi_{4,B_{i,j}}, \pi_{5,B_{i,j}})$. Each S_i verifies the proof $\pi_{3,B_{i,j}}, \pi_{4,B_{i,j}}, \pi_{5,B_{i,j}}$. Then computes $X'_{S_{i,j}}? = \frac{X'_{B_{i,j}}}{Y^{R_{B_{i,j}} \cdot r_{B_{i,j}}}_{S_{i,j}}}$, if the equation is true, the result for comparison between $O_{B_{i,j}}$ and $O_{S_{i,j}}$ is true.

All comparison results between $Bid_{B_i} = \{O_{B_{i,1}}, \ldots, O_{B_{i,j}}, \ldots, O_{B_{i,t}}\}$ and $Bids_{S_i} = \{O_{S_{i,1}}, \ldots, O_{S_{i,j}}, \ldots, O_{S_{i,t}}\}$ are summarized together. According to B_i's preferences $O_{B_{i,1}} < \ldots < O_{B_{i,j}} < \ldots < O_{B_{i,t}}$, gets the biggest index number j of $O_{B_{i,j}}$ for each seller S_i, where $O_{S_{i,j}} = O_{B_{i,j}}$, the seller who possesses the j is the winner.

TABLE 1. The achieved properties.

Properties	[36]	[38]	[43]	Proposal
Trusted third-party	Yes	No	No	No
Strong bid privacy	No	No	Yes	Yes
Bulletin board	No	Yes	Yes	Yes
The number of parties	3	2	2	2
Attribute relation	Independent	Independent	Independent, dependent, interdependent	Independent, dependent, interdependent
Winner determination	Quantitative	Quantitative	Qualitative and quantitative	Qualitative and quantitative
Adversary model	Semi-honest(TTP)	Semi-honest	Semi-honest	Semi-honest

TABLE 2. The numbers of different computation operations.

Phase	[36]	[38]	[43]	Proposal
The initiation phase	1 HF 2 R n+3 PKE 0	1 HF 2 R 1 PKE 1 PKD	1 R 1 PKE 1 PKD	1 R 1 PKE 1 PKD
The bidding phase	0 n PKE n PKD	0 n(T+1)+2T PKE n(T+2)+2T PKD	t+2 HF t+1 PKE 0	6t R 22t ME
The opening phase	0 0 n PKE 0	0 0 2nT PKE n(T+1) PKD	t R 2(t+1) HF t PKE t+1 PKD	
The winner determination phase	0 0 n PKD	0 2nT PKE 0	nt HF 0 0	8t R 34t ME

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

By theorem 4.2-4.5, it shows a bid does not have to be opened for achieving winner determination and public verifiability in the proposed scheme, so the strong bid privacy is provided during an auction.

V. DISCUSSIONS AND EXPERIMENTS

At first, a comparison among related protocols is summarized in Table 1. Because of complicated relation among attributes, the bid expression is important to winner determination process. In [36] and [38], a linear utility function is introduced for multi-attribute bid evaluation. It is assumed that every attribute is independent in each multi-attribute bid using linear utility function. The bid structure of the proposed scheme and Shi's scheme are flexible to support independent, dependent and interdependent attribute relation [43]. Accordingly, [36], [38] only support quantitative attribute winner determination, the proposed scheme and Shi's scheme can support both quantitative and qualitative attribute winner determination. It is assumed that all parties launch computations and message exchange according to protocol specifications in these schemes. However, during or after protocol execution, any party might try his/her best to infer as much additional information as possible. In addition, a TTP support is needed in [43].

Furthermore, a comparison of the computation operations in related protocols is shown in Table 2. Assume that the length of the prime number p is 512, 1024, 1536 bits in modular exponentiation, public key encryption, certification and signature (for RSA), hash function digest is 512 bits (for SHA-1). 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. So compared with a modular multiplication computation in Z_n^*, the computation time

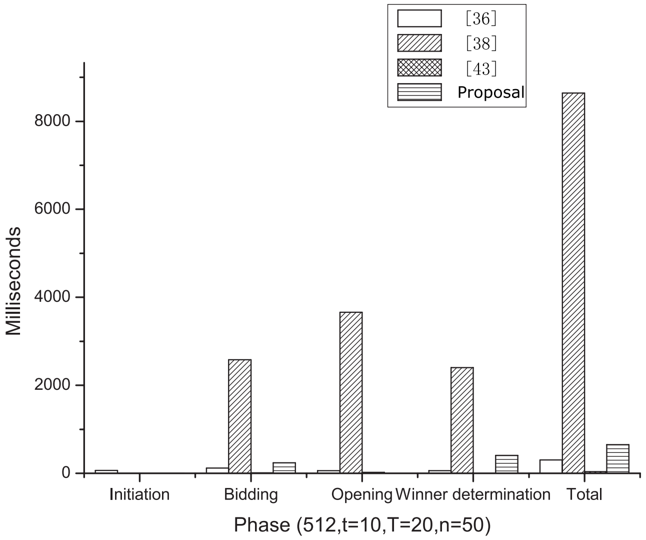


FIGURE 3. Comparison of computation time (key=512bit, t=10, T=20, n=50).

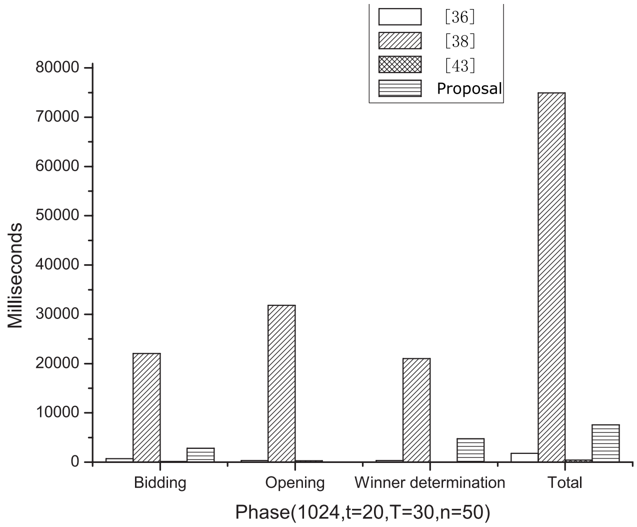


FIGURE 4. Comparison of computation time (key=1024bit, t=20, T=30, n=50).

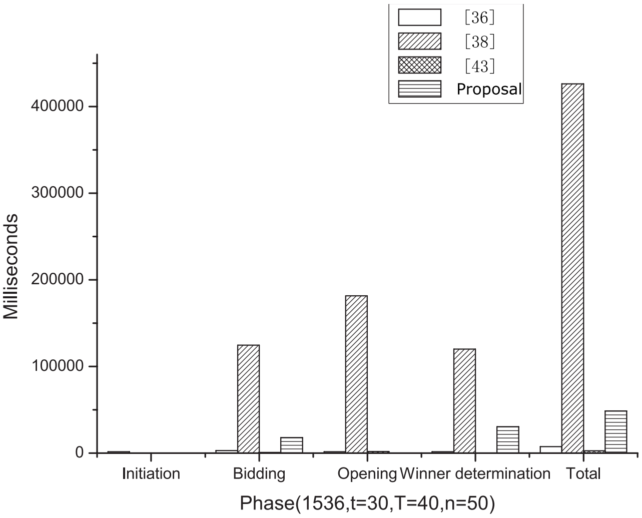


FIGURE 5. Comparison of computation time (key=1536bit, t=30, T=40, n=50).

consumed by hashing operations and random generation can be neglected [52].

At last, a performance simulation is provided. Reference [36], [38], and [43] and proposal are implemented in C using MIRACL library and server configuration: Microsoft Windows XP Professional 2002 Service Pack 3, Intel(R) Core(TM), CPU 2.53 GHz, 1.98 GB of RAM [53]. The average time for computing a single modular exponentiation is 1.2ms for 512-bit,7ms for 1024-bit,and 30ms for 1536-bit. t, T, n denotes the number of bid, attribute and seller separately. For a small-scale system design, assume that $n > T \approx t$. Several experiments have been done and three typical experiments are shown in Figure 3, 4, 5. The comparisons of computation time of the related protocols are shown in Figure 3, 4, 5. Because strong privacy and public verifiability can not be provided in [36], the computation time of [36] is much less than [38]. Due to [43] takes hash function instead of public key system, the computation time of [43] is much less than [38] in the opening and winner determination phase. According to Figure 3, 4, 5, it shows that the computation cost of the proposed scheme is reasonable and less than [38].

VI. CONCLUSIONS

In this paper, it demonstrates a verifiable sealed-bid multi-qualitative-attribute e-auction protocol with semi-honest adversaries. In the proposed scheme, it solves the privacy-preserving multi-qualitative-attribute winner determination problem. In accordance with the security analysis, the strong bid privacy and public verifiability are provided during an auction. Computation simulation of protocols shows the computational cost of the proposed scheme is reasonable.

REFERENCES

[1] C. Fu, "GRAP: Grey risk assessment based on projection in ad hoc networks," *J. Parallel Distrib. Comput.*, vol. 71, no. 9, pp. 1249–1260, 2011.

[2] H. Song and M. Brandt-Pearce, "Model-centric nonlinear equalizer for coherent long-haul fiber-optic communication systems," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2013, pp. 2394–2399.

[3] W. Wei *et al.*, "GI/Geom/1 queue based on communication model for mesh networks," *Int. J. Commun. Syst.*, vol. 27, no. 11, pp. 3013–3029, 2014.

[4] Z. Pan, Y. Zhang, and S. Kwong, "Efficient motion and disparity estimation optimization for low complexity multiview video coding," *IEEE Trans. Broadcast.*, vol. 61, no. 2, pp. 166–176, Jun. 2015.

[5] Y. Qi, "Information potential fields navigation in wireless Ad-Hoc sensor networks," *Sensors*, vol. 11, no. 5, pp. 4794–4807, 2011.

[6] B. Gu, X. Sun, and V. S. Sheng, "Structural minimax probability machine," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 28, no. 7, pp. 1646–1656, Jul. 2016, doi: 10.1109/TNNLS.2016.2544779.

[7] W. Wei, X. L. Yang, and B. Zhou, "Combined energy minimization for image reconstruction from few views," *Math. Problems Eng.*, vol. 2012, Sep. 2012, Art. no. 154630.

[8] J. Shen, H. Tan, J. Wang, J. Wang, and S. Lee, "A novel routing protocol providing good transmission reliability in underwater sensor networks," *J. Internet Technol.*, vol. 16, no. 1, pp. 171–178, 2015.

[9] W. Wei, X.-L. Yang, P.-Y. Shen, and B. Zhou, "Holes detection in anisotropic sensornets: Topological methods," *Int. J. Distrib. Sensor Netw.*, vol. 8, no. 10, p. 135054, 2012.

[10] Y. Zheng, B. Jeon, D. Xu, Q. M. J. Wu, and H. Zhang, "Image segmentation by generalized hierarchical fuzzy C-means algorithm," *J. Intell. Fuzzy Syst.*, vol. 28, no. 2, pp. 961–973, 2015.

[11] W. Wei, Y. Qiang, and J. Zhang, "A bijection between lattice-valued filters and lattice-valued congruences in residuated lattices," *Math. Problems Eng.*, vol. 2013, Jul. 2013, Art. no. 908623.

[12] Z. Xia, X. Wang, X. Sun, Q. Liu, and N. Xiong, "Steganalysis of LSB matching using differences between nonadjacent pixels," *Multimedia Tools Appl.*, vol. 75, no. 4, pp. 1947–1962, Feb. 2016.

[13] W. Wei, H. M. Srivastava, and Y. Zhang, *A Local Fractional Integral Inequality on Fractal Space Analogous to Andersons Inequality Abstract and Applied Analysis*. Cairo, Egypt, Hindawi Publishing Corp., 2014.

[14] S. Xie and Y. Wang, "Construction of tree network with limited delivery latency in homogeneous wireless sensor networks," *Wireless Pers. Commun.*, vol. 78, no. 1, pp. 231–246, 2014.

[15] W. Wei, X. Fan, H. Song, X. Fan, and J. Yang, "Imperfect information dynamic Stackelberg game based resource allocation using hidden Markov for cloud computing," *IEEE Trans. Serv. Comput.*, 2017, doi: 10.1109/TSC.2016.2528246.

[16] B. Chen, H. Shu, G. Coatrieux, G. Chen, X. Sun, and J. L. Coatrieux, "Color image analysis by quaternion-type moments," *J. Math. Imag. Vis.*, vol. 51, no. 1, pp. 124–144, 2015.

[17] X. Wen, L. Shao, Y. Xue, and W. Fang, "A rapid learning algorithm for vehicle classification," *Inf. Sci.*, vol. 295, pp. 395–406, Feb. 2015.

[18] L. Kong, L. He, X.-Y. Liu, Y. Gu, M.-Y. Wu, and X. Liu, ''Privacy-preserving compressive sensing for crowdsensing based trajectory recovery,'' in *Proc. IEEE 35th Int. Conf. Distrib. Comput. Syst. (ICDCS)*, 2015.

[19] R. Ou, F. Cai, Z. Jing, H. Lansheng, and X.-Y. Liu, ''Efficient fair UC-secure two-party computation on committed inputs,'' in *Proc. 12th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun.*, Jul. 2013, pp. 544–551.

[20] J. Li, X. Li, B. Yang, and X. Sun, ''Segmentation-based image copy-move forgery detection scheme,'' *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 3, pp. 507–518, Mar. 2015.

[21] P. Guo, J. Wang, X. H. Geng, C. S. Kim, and J.-U. Kim, ''A variable threshold-value authentication architecture for wireless mesh networks,'' *J. Internet Technol.*, vol. 15, no. 6, pp. 929–936, 2014.

[22] Z. Xia, X. Wang, X. Sun, and B. Wang, ''Steganalysis of least significant bit matching using multi-order differences,'' *Security Commun. Netw.*, vol. 7, no. 8, pp. 1283–1291, Aug. 2014.

[23] T. Ma, ''Social network and tag sources based augmenting collaborative recommender system,'' *IEICE Trans. Inf. Syst.*, vols. E98–D, no. 4, pp. 902–910, Apr. 2015.

[24] D. He, S. Zeadally, N. Kumar, and J.-H. Lee, ''Anonymous authentication for wireless body area networks with provable security,'' *IEEE Syst. J.*, 2016, doi: 10.1109/JSYST.2016.2544805.

[25] D. He, S. Zeadally, N. Kumar, and J.-H. Lee, ''One-to-many authentication for access control in mobile pay-TV systems,'' *Sci. China-Inf. Sci.*, vol. 59, p. 052108, May 2016, doi: 10.1007/s11432-015-5469-5.

[26] Z. Xia, X. Wang, X. Sun, and Q. Wang, ''A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data,'' *IEEE Trans. Parallel Distrib. Syst.*, vol. 27, no. 2, pp. 340–352, Jan. 2016.

[27] Z. Fu, K. Ren, J. Shu, X. Sun, and F. Huang, ''Enabling personalized search over encrypted outsourced data with efficiency improvement,'' *IEEE Trans. Parallel Distrib. Syst.*, vol. 27, no. 9, pp. 2546–2559, Sep. 2016, doi: 10.1109/TPDS.2015.2506573.

[28] Z. Fu, X. Sun, Q. Liu, L. Zhou, and J. Shu, ''Achieving efficient cloud search services: Multi-keyword ranked search over encrypted cloud data supporting parallel computing,'' *IEICE Trans. Commun.*, vol. E98–B, no. 1, pp. 190–200, 2015.

[29] Y. Ren, J. Shen, J. Wang, J. Han, and S. Lee, ''Mutual verifiable provable data auditing in public cloud storage,'' *J. Internet Technol.*, vol. 16, no. 2, pp. 317–323, 2015.

[30] M. Bichler and J. Kalagnanam, ''Configurable offers and winner determination in multi-attribute auctions,'' *Eur. J. Oper. Res.*, vol. 160, no. 2, pp. 380–394, 2005.

[31] Y. Engel and M. P. Wellman, ''Multiattribute auctions based on generalized additive independence,'' *J. Artif. Intell. Res.*, vol. 37, no. 1, pp. 479–525, 2010.

[32] R. K. Singh and L. Benyoucef, ''A fuzzy TOPSIS based approach for e-sourcing,'' *Eng. Appl. Artif. Intell.*, vol. 24, no. 3, pp. 437–448, 2011.

[33] A. K. Ray, M. Jenamani, and P. K. J. Mohapatra, ''An efficient reverse auction mechanism for limited supplier base,'' *Electron. Commerce Res. Appl.*, vol. 10, no. 2, pp. 170–182, 2011.

[34] H.-J. Shyur and H.-S. Shih, ''A hybrid MCDM model for strategic vendor selection,'' *Math. Comput. Model.*, vol. 44, nos. 7-8, pp. 749–761, 2006.

[35] M. N. Kasirian and R. M. Yusuff, ''An integration of a hybrid modified TOPSIS with a PGP model for the supplier selection with interdependent criteria,'' *Int. J. Prod. Res.*, vol. 51, no. 4, pp. 1–18, 2012.

[36] T. R. Srinath, S. Kella, and M. Jenamani, ''A new secure protocol for multi-attribute multi-round e-reverse auction using online trusted third party,'' in *Proc. 2nd Int. Conf. Emerg. Appl. Inf. Technol.*, Feb. 2011, pp. 149–152.

[37] D. C. Parkes, M. O. Rabin, S. M. Shieber, and C. A. Thorpe, ''Practical secrecy-preserving, verifiably correct and trustworthy auctions,'' in *Proc. 8th Int. Conf. Electron. Commerce*, 2006, pp. 70–81.

[38] T. R. Srinath, M. P. Singh, and A. R. Pais, ''Anonymity and verifiability in multi-attribute reverse auction,'' *Int. J. Inf. Technol. Convergence Services*, vol. 1, p. 4, 2011.

[39] M.-J. Li, J. S.-T. Juan, and J. H.-C. Tsai, ''Practical electronic auction scheme with strong anonymity and bidding privacy,'' *Inf. Sci.*, vol. 181, no. 12, pp. 2576–2586, 2011.

[40] K. Omote and A. Miyaji, *A Practical English Auction With One-Time Registration* (Lecture Notes in Computer Science), vol. 2119. Berlin, Germany: Springer, 2001, pp. 221–234.

[41] Y. F. Chung, Y. T. Chen, T. L. Chen, and T. S. Chen, ''An agent-based English auction protocol using Elliptic Curve Cryptosystem for mobile commerce,'' *Expert Syst. Appl.*, vol. 38, no. 4, pp. 9900–9907, 2011.

[42] H. Xiong, Z. Chen, and F. Li, ''Bidder-anonymous English auction protocol based on revocable ring signature,'' *Expert Syst. Appl.*, vol. 39, pp. 7062–7066, Jan. 2012.

[43] S. Wenbo, ''A provable secure sealed-bid multi-attribute auction scheme under semi-honest model,'' *Int. J. Commun. Syst.*, vol. 27, no. 12, pp. 3738–3747, 2014, doi: 10.1002/dac.2571

[44] D. A. Mayer and S. Wetzel, ''Verifiable private equality test: Enabling unbiased 2-party reconciliation on ordered sets in the malicious model,'' in *Proc. 7th ACM Symp. Inf., Comput. Commun. Secur.*, 2012, pp. 46–47.

[45] O. Goldreich, *Foundations of Cryptography* (Basic Applications), vol. 2. Cambridge, U.K.: Cambridge Univ. Press, 2004.

[46] J. Brickell and V. Shmatikov, ''Privacy-Preserving Graph Algorithms in the Semi-Honest Model,'' in *Advances in Cryptology-ASIACRYPT* (Lecture Notes in Computer Science), vol. 3788. Berlin, Germany: Springer, 2005, pp. 236–252.

[47] C. P. Schnorr, ''Efficient signature generation by smart cards,'' *J. Cryptol.*, vol. 4, pp. 161–174, Jan. 1991.

[48] D. Chaum and T. Pedersen, ''Wallet databases with observers,'' in *Advances In Cryptology (Crypto)* (Lecture Notes in Computer Science), vol. 740. Berlin, Germany: Springer, 1993, pp. 89–105.

[49] J. Camenisch and M. Stadler, ''Proof Systems for general statements about discrete logarithms,'' Dept. Comput. Sci., ETH Zurich, Zürich, Switzerland, Tech. Rep. 260, Mar. 1997. [Online]. Available: ftp://ftp.inf.ethz.ch/pub/publications/tech-reports/

[50] T. Pedersen, ''Non-interactive and information-theoretic secure verifiable secret sharing,'' in *Advances in Cryptology (CRYPTO)* (Lecture Notes in Computer Science), vol. 576. Berlin, Germany: Springer, 1992, pp. 129–140.

[51] R. Crandall and C. Pomerance, ''Prime numbers: A computational perspective,'' in *Exponential Factoring Algorithms*, 1st ed. New York, NY, USA: Springer, 2001, pp. 191–226.

[52] C. Paar and J. Pelzl, ''Understanding cryptography,'' in *A Textbook for Students and Practitioners Introduction to Public-Key Cryptography*. Berlin, Germany: Springer, 2009, pp. 149–170.

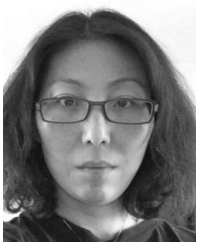
[53] M. Scott. (2003). MIRACL—A multiprecision integer and rational arithmetic C/C++ library. Shamus Software Ltd, Dublin, Ireland. [Online]. Available: http://www.shamus.ie

WENBO SHI received the M.S. and Ph.D. degrees from Inha University, Incheon, South Korea, in 2007 and 2010, respectively. He is currently an Assistant Professor with Northeastern University. His current research interests include cryptography and network security.

WEI WEI received the Ph.D. and M.S. degrees from Xi'an Jiaotong University, in 2011 and 2005, respectively. He is currently an Assistant Professor with the Xi'an University of Technology. His current research interests include wireless networks and wireless sensor networks application, image processing, mobile computing, distributed computing, and pervasive computing.

JIAQI WANG is currently pursuing the Ph.D. degree in computer application technology from Northeastern University, Shenyang, China, in 2015. Her current research interests include network information security and spectrum auction security.

QINGCHUN ZHAO was born in Shandong, China, in 1982. He received the B.S. degree from the University of Jinan, Jinan, China, in 2006, the M.E. degree from the Taiyuan University of Technology, Taiyuan, China, in 2009, and the Ph.D. degree from the Dalian University of Technology, Dalian, China, in 2014. He is currently a Lecturer with the School of Computer and Communication Engineering, Northeastern University, Qinhuangdao, China. His current research interests include optical fiber communications and photonic signal processing.



ZHUO LIN was born in Hebei, China, in 1979. She received the M.E. degree from Yanshan University, China, in 2007. Her research interests mainly focus on virtual reality, simulation of plants and data mining.

HUIHUI WANG (M'13) received the Ph.D. degree in electrical engineering from the University of Virginia, Charlottesville, VA, USA, in 2013. In 2013, she joined the Department of Engineering, Jacksonville University, Jacksonville, FL, USA, where she is currently an Assistant Professor and the Founding Chair of the Department of Engineering. In 2011, she was an Engineering Intern with Qualcomm, Inc. She has authored over 30 articles and holds one U.S. patent. Her current research interests include cyber-physical systems, internet of things, healthcare and medical engineering based on smart materials, robotics, haptics based on smart materials/structures, ionic polymer metallic composites, and MEMS.