A SECURE MULTI-ITEM E-AUCTION MECHANISM WITH BID PRIVACY

Dong-Her Shih, Department of Information Management, National Yunlin University of Science and Technology, 123, Section 3, University Road, Douliu, Yunlin, Taiwan, R.O.C, 886-5-5342601x5340, shihdh@yuntech.edu.tw
Chih-Hung Cheng, Department of Information Management, National Yunlin University of Science and Technology, 123, Section 3, University Road, Douliu, Yunlin, Taiwan, R.O.C, 886-5-5342601x5308, g9423715@yuntech.edu.tw
Jui-Chi Shen, Kaohsiung Hospitality College, 1, Sung-Ho Rd., Shiao-Kang, Kaohsiung, Taiwan, R.O.C, 886-7-8060591, shen@mail.nkhc.edu.tw

ABSTRACT

A novel MRVP auction protocol to solve the bid privacy problems of multi-item reverse Vickrey auction for task assignment scenarios is proposed. A verifiable technique of encryption key chain is used to find the highest bids without revealing the losing bid and unnecessary information. Through analysis, our new scheme is robust against cheating bidders.

INTRODUCTION

On-line auctions have become increasingly prevalent in the corporate procurement practice over a large spectrum of industries. Forrester Research predicts global on-line trade will expand to $12.8 trillion by 2006 [1]. In many auction applications, sellers making their bid strategy by tracing others bid. Therefore, it is desired to keep the lost bids private even at the end of the auction. This requirement is called bid privacy and is discussed in many papers. In many contexts, privacy is an important consideration in the auctions. Our hope is that by providing an auction protocol for bid privacy and solutions to bid privacy problems as well as preventing sellers marking their bid strategy by tracing other bid.

Multi-item Reverse Vickrey auction with Privacy (MRVP) Protocol

In the MRVP protocol, sellers must publish their goods which deal explicitly with multiple issues/attributes on UDDI servers. Whenever a buyer begins an auction that describes the good to be bought and specifies the quantity demanded, the auctioneer agent finds and evaluates by meeting the buyer's minimum requirements regarding the bidder attributes sellers having registered on the UDDI server and sends a request for bidding. Sellers are verified by a third trusted party and respond for secure seal bidding. If there are disputes, a third trusted party is responsible for key resubmission and the bidding is continued. The MRVP protocol, a verifiable encryption sealed-bid multi-attribute and multi-item auction protocol in optimistic approach, consists of initial, bidding and opening phases that are described in details as follows. Figure 1 illustrates our MRVP auction procedure.

Initial Phase

***Step 1*:** Buyer describes the good to be bought, and specifies the quantity demand. Auctioneer agent A

chooses Sellers from registry server or UDDI in web service environment.

***Step* 2:** Bidder S_i is notified and chooses his/her secret share $x_{i,j}$ for price p_j. The corresponding public key share is $y_{i,j} = g^{x_{i,j}} \bmod p$. Additionally, $x_{i,j}$ is encrypted as $\beta_{i,j} = V E_T (x_{i,j})$ by the public key of a third trusted party T. A Naccache-Stern encryption algorithm [2] is used. $\beta_{i,j}$ is recoverable by T and can be verified as a correct encryption of the secret committed in $y_{i,j}$ by zero knowledge proof of equality of logarithms [3]. S_i gives his/her signature and sends $Com1i$ to auctioneer agent A.

***Step* 3:** Auctioneer agent A verifies both the signature of S_i on $y_{i,j}$ and $\beta_{i,j}$, $j = 1, 2, \ldots, w$. If the verification is successful, A sends a certificate $Com2 = (z_{i,1}, z_{i,2}, \ldots, z_{i,j})$ to S_i. Then A chooses his/her own secret shares $x_{A,j}$ and generates the public keys in the chain Y_j. Finally A publishes Y_j, $Com3$, and the registration information of the bidders in BB (Bulletin Board). Key generation is illustrated in Table 1 for the case of 5 bidders and 6 biddable prices.

Bidding Phase

Bidder S_i publishes his/her bid $Com4i$ for $i = 1, 2, \ldots, n$. If he/she is not willing to pay p_j , $V_{i,j} = E_{Yi}(No, x_{i,j+1})$. Otherwise, $V_{i,j} = E_{Yi}(Yes, proof(x_{i,j+1}))$ where $proof(x_{i,j+1})$ is a transcript for zero knowledge proof of knowledge of $x_{i,j+1}$. When price p_k is higher than p_j, $V_{i,k}$ is randomly chosen. Finally, Auctioneer agent A publishes $Com5$ in BB. Bid format is illustrated in Table 2.

Opening Phase

***Step* 1:** Bidder S_i publishes $Com6i = (x_{i,1}, Sig_{Si}(x_{i,1}))$ for $i = 1, 2, \ldots, n$. Auctioneer agent A calculates and publishes $Com7=(X_1)$, the first decryption key for the bids at p_1.

***Step* 2:** If no "*Yes*" bid is found at this price, decryption key (X_2) for p_2 can be constructed and opening procedure continues. Similarly the opening procedure can go on along the encryption key chain until a "*Yes*" bids that are to be within the limit of demand quantity is found as a winning bid. Then, the encryption key chain is broken as shown in p_2 of Table 2.

***Step* 3:** Auctioneer agent A negotiates with winner S_i to decrypt the next price until the highest losing bid price is found. For example, S_2, S_4 and A negotiate to recover X_3 and S_2, S_4, S_5 negotiate to recover X_4 with A , and p_4 is the highest losing bid price by others to be founded in Table 2. Therefore, S_2, S_4, S_5 is the winner and p_4 is the possible contract price.

ANALYSES

The following properties are achieved in our protocol. (1) Fairness: No one can disclose the content of any of the bids until the bidding period closes, including the auctioneer agent. (2)Privacy of losing bid: All bidding prices except the contract price is not revealed to anyone. (3) Public verifiability: It is universally verifiable that the price of successful bids is the highest losing bid among all bids. (4) Non-repudiation: The winners cannot deny they submitted the winning bid. (5) Robustness: No bidder can make the protocol impossible by his malicious act. (6) Soundness: Nobody can impersonate any other bidder to make a bid. (7) Efficiency: In

order to calculate efficiency, the parameters n and w are used to denote the number of bidders and the number of biddable prices, respectively. Integer length of 1024 bits is assumed for all the cryptographic primitives. Table 3 compares computation and communication efficiencies between the proposed scheme and the one by Watanabe and Imai [4].

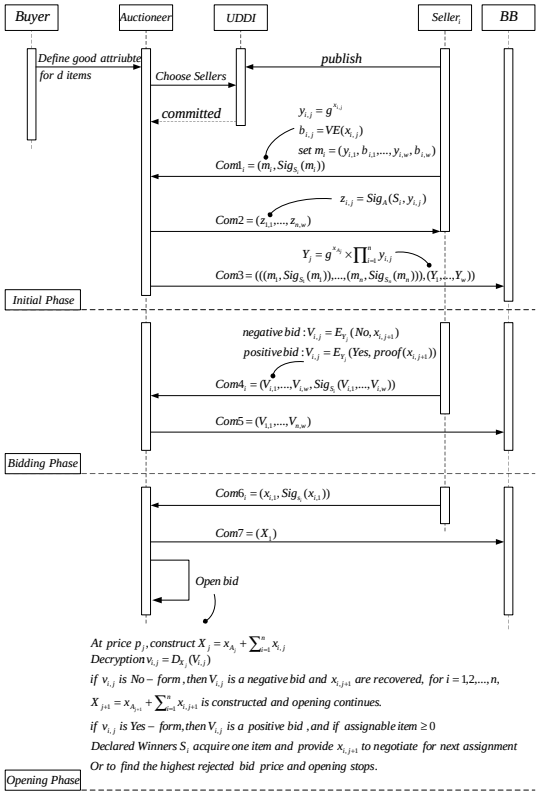

Figure 1: MRVP auction procedures

Table 1 Public Key generations

	A	S_1	S_2	S_3	S_4	S_5	Encryption key
p_1	$y_{A1}=g^{xA1}$	$y_{1,1}=g^{x1,1}$	$y_{2,1}=g^{x2,1}$	$y_{3,1}=g^{x3,1}$	$y_{4,1}=g^{x4,1}$	$y_{5,1}=g^{x5,1}$	$Y_1= y_{A1}* y_{1,1}* y_{2,1}* y_{3,1}* y_{4,1}* y_{5,1}$
p_2	$y_{A2}=g^{xA2}$	$y_{1,2}=g^{x1,2}$	$y_{2,2}=g^{x2,2}$	$y_{3,2}=g^{x3,2}$	$y_{4,2}=g^{x4,2}$	$y_{5,2}=g^{x5,2}$	$Y_2= y_{A2}* y_{1,2}* y_{2,2}* y_{3,2}* y_{4,2}* y_{5,2}$
p_3	$y_{A3}=g^{xA3}$	$y_{1,3}=g^{x1,3}$	$y_{2,3}=g^{x2,3}$	$y_{3,3}=g^{x3,3}$	$y_{4,3}=g^{x4,3}$	$y_{5,3}=g^{x5,3}$	$Y_3= y_{A3}* y_{1,3}* y_{2,3}* y_{3,3}* y_{4,3}* y_{5,3}$
p_4	$y_{A4}=g^{xA4}$	$y_{1,4}=g^{x1,4}$	$y_{2,4}=g^{x2,4}$	$y_{3,4}=g^{x3,4}$	$y_{4,4}=g^{x4,4}$	$y_{5,4}=g^{x5,4}$	$Y_4= y_{A4}* y_{1,4}* y_{2,4}* y_{3,4}* y_{4,4}* y_{5,4}$
p_5	$y_{A5}=g^{xA5}$	$y_{1,5}=g^{x1,5}$	$y_{2,5}=g^{x2,5}$	$y_{3,5}=g^{x3,5}$	$y_{4,5}=g^{x4,5}$	$y_{5,5}=g^{x5,5}$	$Y_5= y_{A5}* y_{1,5}* y_{2,5}* y_{3,5}* y_{4,5}* y_{5,5}$
p_6	$y_{A6}=g^{xA6}$	$y_{1,6}=g^{x1,6}$	$y_{2,6}=g^{x2,6}$	$y_{3,6}=g^{x3,6}$	$y_{4,6}=g^{x4,6}$	$Y_{5,6}=g^{x5,6}$	$Y_6= y_{A6}* y_{1,6}* y_{2,6}* y_{3,6}* y_{4,6}* y_{5,6}$

Table 2 Bids Data and Decryption Key generation

	S_1	S_2	S_3	S_4	S_5	Decryption Key
p_1	$E_{Y1}(x_{1,2})$	$E_{Y1}(x_{2,2})$	$E_{Y1}(x_{3,2})$	$E_{Y1}(x_{4,2})$	$E_{Y1}(x_{5,2})$	$X_1=x_{A1}+x_{1,1}+x_{2,1}+x_{3,1}+x_{4,1}+x_{5,1}$
p_2	$E_{Y2}(x_{1,3})$	$E_{Y2}(proof(x_{2,3}))$	$E_{Y2}(x_{3,3})$	$E_{Y2}(proof(x_{4,3}))$	$E_{Y2}(x_{5,3})$	$X_2=x_{A2}+x_{1,2}+x_{2,2}+x_{3,2}+x_{4,2}+x_{5,2}$
p_3	$E_{Y3}(x_{1,4})$	Random bid in correct format	$E_{Y3}(x_{3,4})$	Random bid in correct format	$E_{Y3}(proof(x_{5,4}))$	S_2, S_4 and A must negotiate to recover X_3
p_4	$E_{Y4}(proof(x_{1,5}))$	Random bid in correct format	$E_{Y4}(x_{3,5})$	Random bid in correct format	Random bid in correct format	S_2, S_4, S_5 and A must negotiate to recover X_4
p_5	Random bid in correct format	Random bid in correct format	$E_{Y5}(proof(x_{3,6}))$	Random bid in correct format	Random bid in correct format	S_1, S_2, S_4, S_5 and A must collude to recover X_5
p_6	Random bid in correct format	Random bid in correct format	Random bid in correct format	Random bid in correct format	Random bid in correct format	All the bidders and A must collude to recover X_6

Table 3 Computation and communication cost (exponentiations) of our protocol

Complexity	Scheme by Watanabe & Imai	Our scheme
Computational cost of a bidder	$8w+1$	$4w+3$
Computational cost of an auctioneer	$5.5\,n\,w + w + 4\,n$	$6\,n\,w + w + 2n$
Bid length	at least 5120 bits	1024 bits
Communication cost of a bidder	at least $1024*(8\,n\,w + w)$ bits	$1024*(8w+2)$ bits

CONCLUSION

We proposed a MRVP auction to solve problems of bid privacy in typical multi-item reverse Vickrey auction. Our MRVP protocol resulted in a practical sealed-bid auction protocol that allows an auctioneer agent to determine the winning bid and the price in a universally verifiable way. More importantly, our scheme is robust against cheating bidders. The advantages of our proposed MRVP protocol are that collusion will be difficult and a losing bidder can have his/her own bid unrevealed.

REFERENCE (References are upon request)