NON-INTERACTIVE BID REVERSE AUCTION SCHEME WITH STRONG PRIVACY

Dong-Her Shih, Shin-Yi Huang, Department of Information Management, National Yunlin University of Science and Technology, 123, Section 3, University Road, Touliu, Yunlin, Taiwan, R.O.C.
David C. Yen, Department of DSC & MIS, Miami University, Oxford, Ohio, USA

ABSTRACT

In recent years auctions have become more and more important as useful mechanisms for resource allocation, task assignment and last but not least electronic commerce. This paper specifies a new scheme that is needed to ensure the accurate and secret execution of the reverse Vickrey auctions.

INTRODUCTION

The Vickrey auction [1] has received particular attention within the multi-agent community and has been applied in a variety of contexts like e-commerce and computer networks. This paper concentrates on the use of the reverse Vickrey auction for task assignment scenarios. In the reverse auction, a buyer displays their desired goods and along with a desired price, and sellers competitively decrease their price until a sale is made. Bidders that did not win an auction do not necessarily get to know who placed the lowest bid. The only information that is revealed to all bidders is the selling price. It is desired to keep the losing bids private even at the end of the auction. This requirement is called bid privacy. Franklin and Reiter were among the first to address electronic auction wit bid privacy [2]. They combined cryptographic primitives such as secret sharing, digital cash and multicasts, and introduced their own "verifiable signature sharing". In this paper, we propose the RVP auction protocol. The RVP auction is a novel protocol in which the buyer nominates sellers and the nominated sellers compete on price with strong privacy. The idea of key chain [3] is inherited, so that bid privacy for a losing bidder is achieved.

REVERSE VICKREY AUCTION PRIVACY (RVP) MECHANISM

In the reverse auction, multiple sellers compete on goods and the evaluation value shown by the buyer. Since buyers can solicit nominations via Internet. Therefore, we adopted the designated auction mechanism [4] to the Internet auction. There is an active auctioneer in our RVP scheme. The auctioneer is responsible for constructing the public keys in the chain. To weaken the trust on the bidders, a share for each decryption key is provided by the auctioneer. Moreover, veritable encryption is employed so that an off-line third party can interfere if a bidder is dishonest when constructing the key chain. In this case the third party can recover the concealed correct share to help construct the next decryption key.

Our RVP protocol is as follows and Figure 1 illustrates the auction procedure.

1. **Initial phase**

– Buyer chooses Sellers from registry server or UDDI in web service.

– Bidder S_i chooses his secret share $x_{i,j}$ for price p_j . The corresponding public key share is $y_{i,j} = g^{x_{i,j}}$. Additionally $x_{i,j}$ is encrypted as $\beta_{i,j} = VE\ (x_{i,j})$ by a third party T 's public key. $\beta_{i,j}$ is recoverable by T and can be verified as a secret committed in $y_{i,j}$ by zero knowledge proof of equality of logarithms [5]. S_i signs, and sends $Com1i =(m_{i1},\dots,m_{iw}, Sig_{Si}(S_i, m_{i1},\dots, m_{iw}))$ to auctioneer A.

– A verifies S_i's signature on $y_{i,j}$ and $\beta_{i,j}$ for $j = 1, 2, \dots, w$ and the correctness of encryption. If the verification is successful, A sends a certificate $certi = (z_{i,1}, z_{i,2}, \dots , z_{i,j})$ to Si where $z_{i,j} = Sig_A(S_i, y_{i,j}\ )$. Then A chooses his own secret shares $x_{A,j}$ and generates the public keys in the chain Y_j . Finally A publishes Y_j , $Com2i$ and the registration information of the bidders. Key generation is illustrated in Table 1 for the case of 3 bidders and 6 biddable prices, so that $n = 3$ and $w = 6$.

2. Bidding phase

– Si publishes his bid $V_{i,j} = E_{Yj}\ (I_{i,j}, y_{i,j}, z_{i,j})$ for $j = 1, 2, \dots, w$. If he is not willing to pay p_j, $I_{i,j} = (No, x_{i,j+1})$. If he is willing to pay p_j , $I_{i,j} = (Yes, proof\ (x_{i,j+1}\ ))$ where $proof(x_{i,j+1})$ is a transcript for zero knowledge proof of knowledge of $x_{i,j+1}$. $I_{i,j}$ can be checked against $y_{i,j}$ and $z_{i,j}$ to show that S_i provides a valid $x_{i,j+1}$ (in a "Yes" bid) or knows its value (in a "No" bid). Bid format is illustrated in Table 2. In the table only $x_{i,j}$, the basic element of bid $V_{i,j}$, is presented.

3. Opening phase

–S_i publishes $Com3i = (x_{i,1}, Sig_{Si}(S_i,x_{i,1}))$ for $i = 1, 2, \dots, n$.

– A calculates and publishes X_1, the decryption key for the bids at p_1.

– If no "Yes" bid is found at this price, decryption key for p_2 can be constructed and opening continues. Similarly the opening can go on along the key chain until a "Yes" bid is found as winning bid and key chain is broken. The second lowest price bid is found by collusive operation of the winner and the auctioneer. Not until the second lowest bid is found, the opening is stopped since the opening must continues with second lowest bidder's collusion which is irrational.

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. (2)Privacy of losing bid: All bidding prices except the contract price is not revealed to anyone. (3)Universal verifiability: It is universally verifiable that the price of the successful bid is lowest among all bids. (4)Correctness: The winning bid is indeed the lowest bid and contracting bid is the second price. (5)Non-repudiation: The winners cannot deny they submitted the winning bid. (6)Robustness: No bidder can make the protocol impossible by his malicious act. Namely, even after detecting the cheater, the auctioneer can continue the protocol without bidding again from scratch. (7)Soundness: Nobody can impersonate any other bidder to make a bid.

CONCLUSIONS AND FUTURE WORK

We proposed the RVP auction to solve bid privacy problems in typical reverse auctions. The advantages of the RVP auction are collusion is difficult and losing bidder can have his own bid unrevealed. Our future work includes extending the RVP auction protocol to cases where group buying exists and to cases where the double-auction mechanism is used in web service environments.

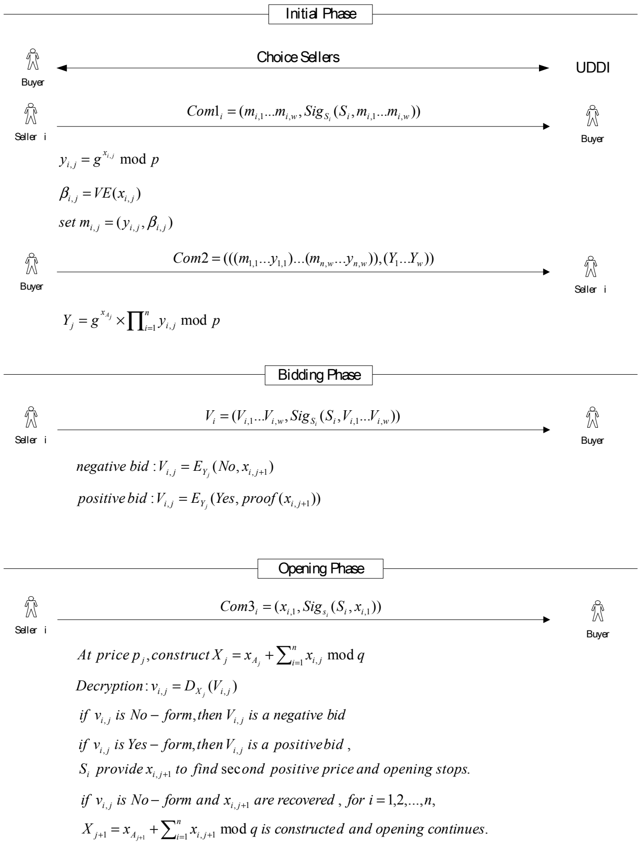
Initial Phase
Buyer
Choice Sellers
UDDI
Seller i
$Com1_i = (m_{i,1}...m_{i,w}, Sig_{S_i}(S_i, m_{i,1}...m_{i,w}))$
Buyer
$y_{i,j} = g^{x_{i,j}} \bmod p$
$\beta_{i,j} = VE(x_{i,j})$
$set\ m_{i,j} = (y_{i,j}, \beta_{i,j})$
Buyer
$Com2 = (((m_{1,1}...y_{1,1})...(m_{n,w}...y_{n,w})),(Y_1...Y_w))$
Seller i
$Y_j = g^{x_{A_j}} \times \prod_{i=1}^{n} y_{i,j} \bmod p$
Bidding Phase
Seller i
$V_i = (V_{i,1}...V_{i,w}, Sig_{S_i}(S_i, V_{i,1}...V_{i,w}))$
Buyer
$negative\ bid: V_{i,j} = E_{Y_j}(No, x_{i,j+1})$
$positive\ bid: V_{i,j} = E_{Y_j}(Yes, proof(x_{i,j+1}))$
Opening Phase
Seller i
$Com3_i = (x_{i,1}, Sig_{s_i}(S_i, x_{i,1}))$
Buyer
$At\ price\ p_j, construct\ X_j = x_{A_j} + \sum_{i=1}^{n} x_{i,j} \bmod q$
$Decryption: v_{i,j} = D_{X_j}(V_{i,j})$
$if\ v_{i,j}\ is\ No-form, then\ V_{i,j}\ is\ a\ negative\ bid$
$if\ v_{i,j}\ is\ Yes-form, then\ V_{i,j}\ is\ a\ positive bid,$
$S_i\ provide\ x_{i,j+1}\ to\ find\ second\ positive\ price\ and\ opening\ stops.$
$if\ v_{i,j}\ is\ No-form\ and\ x_{i,j+1}\ are\ recovered, for\ i=1,2,...,n,$
$X_{j+1} = x_{A_{j+1}} + \sum_{i=1}^{n} x_{i,j+1} \bmod q\ is\ constructed\ and\ opening\ continues.$

Figure 1 RVP auction procedures

Table 1

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

Table 2

	S_1	S_2	S_3	Decryption Key
p_1	$E_{Y1}(x_{1,2})$	$E_{Y1}(x_{2,2})$	$E_{Y1}(x_{3,2})$	$X_1=x_{A1}+x_{1,1}+x_{2,1}+x_{3,1}$
p_2	$E_{Y2}(x_{1,3})$	$E_{Y2}(proof(x_{2,3}))$	$E_{Y2}(x_{3,3})$	$X_2=x_{A2}+x_{1,2}+x_{2,2}+x_{3,2}$
p_3	$E_{Y3}(x_{1,4})$	$E_{Y3}(x_{2,4})$	$E_{Y3}(x_{3,4})$	S_2 and A must collude to recover X_3
p_4	$E_{Y4}(proof(x_{1,5)})$	$E_{Y4}(x_{2,5})$	$E_{Y4}(x_{3,5})$	S_2 and A must collude to recover X_4
p_5	$E_{Y5}(x_{1,6})$	$E_{Y5}(x_{2,6})$	$E_{Y5}(proof(x_{3,6}))$	S_1,S_2 and A must collude to recover X_5
p_6	$E_{Y6}(x_{1,1})$	$E_{Y6}(x_{2,1})$	$E_{Y6}(x_{3,1})$	S_1,S_2,S_3 and A must collude to recover X_6

REFERENCE

[1] Vickrey, W., Counter speculation, auctions, and competitive sealed tenders, Journal of Finance, 1961, 16(1), pp8-37.

[2] Franklin, M.K. & Reiter, M.K., The design and implementation of a secure auction service, IEEE Trans. on Software Engineering, 1996, 22(5), pp302-312.

[3] Watanabe, Y. & Imai, H., Reducing the round complexity of a sealed-bid auction protocol with an off-line ttp, In STOC 2000, 2000, pp 80-86.

[4] Baba, Y., Financial Review, Policy Research Institute of the Ministry of Finance Japan, 2000, No.53.

[5] Chaum, D. & Pedersen, T.P., Wallet databases with observers. Advances in Cryptology - Crypto '92, Lecture Notes in Computer Science, 1992, Volume 740, pp 89-105.