COMPUTERS & SECURITY 30 (2011) 273–287

available at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

A secure multi-item e-auction mechanism with bid privacy

Dong-Her Shih [a], David C. Yen [b,*], Chih-Hung Cheng [a], Ming-Hung Shih [c]

[a] Department of Information Management, National Yunlin University of Science and Technology 123, Section 3, University Road, Douliu, Yunlin, Taiwan, ROC

[b] Department of DSC & MIS, Farmer School of Business, Miami University Oxford, OH 45056, USA

[c] Department of Electrical and Computer Engineering, NC State University, Raleigh, NC 27695, USA

ARTICLE INFO

Article history:
Received 17 November 2010
Received in revised form
7 January 2011
Accepted 13 February 2011

Keywords:
Bid privacy
Shared key chain
Multi-item auction
Reverse sealed-bid auction

ABSTRACT

The recent focus within the auction field has been multi-item auctions where bidders are not restricted to buying only one item of the merchandise. It has been of practical importance in Internet auction sites and has been widely executed by them. In this paper, we concentrate on the use of the multi-item auction for task assignment scenarios and propose a novel PUPA auction protocol to solve the problem of bid privacy in multi-item auctions. A verifiable technique of shared key chain is proposed to find the winners without revealing the losing bid and bidder's privacy. It can be shown that our new scheme is robust against cheating bidders.

Crown Copyright © 2011 Published by Elsevier Ltd. All rights reserved.

1. Introduction

E-commerce on the Internet has dramatically increased in the last couple of years. The mechanisms for doing commerce have also received considerable attention by researchers. The auction format is becoming one of the most popular forms of trading on the Internet, as it allows competitive price discovery and fair and efficient allocation of resources. This has sparked renewed interest in the theory of auctions (Board, 2007; Kirkegaard, 2009; Mishra and Garg, 2006; Parkes et al., 2008). And, online auctions have become increasingly prevalent in the corporate procurement practice over a large spectrum of industries. A report produced by the National Auctioneers Association (NAA) provides easy-to-read statistics about the live auction industry's size since 2003. The auction industry holds strong in 2008 with $268.5 billion in sales (National Auctioneers Association, 2008). Most sales in today's electronic markets are to a few large firms, while the number of suppliers is much larger (Jin et al., 2006). E-commerce, especially the online auction, has experienced great development in recent years. The online auction market has already become an important business entity (Kauffman et al., 2009; Li et al., 2006, 2008).

Literature on auction theory is mostly about single-unit auctions. Recently, a new strand of research has emerged analyzing multi-unit auctions, often with applications to treasury auctions (Arupratan, 2001) or others (Zulehner, 2009; Dasu and Tong, 2010). Juda and Parkes (2009) introduced an options-based infrastructure for multiple auctions. They believe that the future research on buyer/supplier behavior and mechanism design for multiple auctions will receive increasing attention, mainly because of the growing need in practice (Jin et al., 2006). Hence, there have been several extensions to the traditional auction paradigm in recent years. The strong theoretical results

* *Corresponding author*. Tel.: +1 513 529 4827; fax: +1 513 529 9689.
E-mail addresses: shihdh@yuntech.edu.tw (D.-H. Shih), yendc@muohio.edu (D.C. Yen), g9423715@yuntech.edu.tw (C.-H. Cheng), dannysmh@gmail.com (M.-H. Shih).

0167-4048/$ – see front matter Crown Copyright © 2011 Published by Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2011.02.004

obtained by isolated single good auctions however, are not necessarily transferable to the more complicated multiple unit situation (Pinker et al., 2010; Teich et al., 2004).

The most commonly studied auction mechanisms are the ascending price English auction, the descending price Dutch auction, and the Vickrey second-price sealed-bid auction. A recent focus of auction research has been multiple-unit auctions, where bidders are not restricted to buying only one unit of the merchandise (Teich et al., 2004). Taking a cue from the literature on single-unit auctions, much of the multi-unit literature has focused on uniform price (Gresik, 2001; Pinker et al., 2010). In the Vickrey auction, it is a dominant strategy for each bidder to bid truthfully on each unit (Engelbrecht-Wiggans and Kahn, 1998; Naldi and D'Acquisto, 2008). A Vickrey-type auction procedure has a good incentive property even in a multi-item setting (Chen and Takeuchi, 2010; Miyake, 1996).

Economist Robert Weber notes: "The second-price (Vickrey) auction naturally generalizes to a uniform-price auction" (Morgan, 2001). In uniform price auctions, each winning bidder pays the issue-clearing price which corresponds to the highest losing bid for each unit (Gresik, 2001) and holds only when individuals are allowed to bid for only one item (Bapna et al., 2001). For instance, consider an auction of three goods and let there be five bidders with the following bids each for one quantity. Sellers' bids and bidding results of uniform price is shown in Table 1. Ordering the bids of all bidders from lowest to highest yields the sequence 15, 15, 20, 30, 30 and the bidder is A, C, B, D, E, respectively. After opening the bid, the A, C, and B will be declared winners as shown in Table 2 and they will all pay $30 (D's bid) assuming that ties are broken randomly. All bidders have it in their interest to bid their true valuations.

In many auction applications, sellers make their bid strategy by tracing other's bids. Therefore, it is desirable 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 (Chung et al., 2008; Fan et al., 2009; Kudo, 1998; Nurmi, 1994; Shih et al., 2006; Shih et al., 2007). Different techniques to protect bid privacy have been proposed for single-item auctions, but only a few works on multi-item auctions can be found in the literature. A multi-item auction uses different pricing and items than a single-item auction, so the development of new algorithm is required for robust bid privacy protection techniques for a multi-item auction. In many contexts, privacy is an important consideration in the auctions. Our intention is to provide an auction protocol for bid privacy and solutions to bid privacy problems as well as to prevent sellers making their bid strategy by tracing other bids.

2. Related works

Privacy is a frequently desired characteristic in auction schemes (Trevathan et al., 2006) and various mechanisms that avoid blind trust in a single auctioneer have been proposed recently (Brandt and Sandholm, 2004; Chung et al., 2008; Fan et al., 2009). In addition to the real-time concerns associated with auctions, there are also privacy concerns. Bidders will bid up to their indifference price, that is, the price at which they value the good being auctioned. A corrupt auctioneer can thus derive detailed information about the bidders' preferences and the value they place on various goods. This is a serious risk and makes consumers naturally reluctant to give out personal information over the web, where they cannot control who has access to the information or for what purposes it can be used (Chung et al., 2008; Fan et al., 2009; Kikuchi et al., 2000).

Table 1 – Sellers' bid of uniform price.

$Seller_i$	A	B	C	D	E
Bid	15	20	15	30	30

Table 2 – open result of uniform price.

$Seller_i$	A	B	C	D	E
Bid ordering	1	3	2	4	5
Winner	ˇ	ˇ	ˇ		
Winner price	30	30	30		

Bid privacy is a frequently desired property in auction schemes. It refers to the confidentiality of losing bids to anybody even after the auction ends. Franklin and Reiter (1996) were among the first researchers to address electronic auction with bid privacy. They covered many problems such as secret sharing, digital cash, and multicasts, as well as their own primitive technique called verifiable signature sharing. They also prevented a single auctioneer agent from altering a bid or throwing an auction to a single bidder successfully. However, a corrupted auctioneer agent can derive detailed information about the bidder's strategy. Kikuchi et al. (2000) attempted to deal with such problems through secret sharing techniques, but Sako (1999) pointed out that several problems remain in their work. The drawback of the convertible undeniable signature and hash chaining technique is that all bidders have to take part in the protocol during opening bids. The privacy issues of the single-item sealed-bid auction protocol are listed in Table 3 for comparison (Shih et al., 2006; Watanabe and Imai, 2000).

As for recent scholars' studies in relation to bid privacy, Jaiswal et al. (2004) makes use of time-release cryptography to provide guaranteed non-disclosure of the bids. And, Juang et al. (2005) propose a secure and fair sealed-bid auction scheme. They use a threshold cryptosystem without the assistance of a mutually entrusted party to guarantee fairness among bidders and the modern cryptographic techniques of fair blind signatures and untraceable e-mail systems to design a real, fair, and secure sealed-bid auction scheme.

The distributed public key crypto technique (Waldspurger et al., 1992) is quite efficient, but it is not fair to all bidders and auctioneer agents. A bidder has to rely on uncertain evidence that more than a threshold of auctioneer agents is honest. A verifiable encryption scheme by Watanabe and Imai (2000) claimed to have achieved strong bid privacy efficiently. A cryptographic tool called encryption key chain was employed in our previously research scheme. But we discovered the encryption key chain having the Achilles heel of the public key generation. The generated public key may not conform to the principle of large prime and only works in the single-item auction, giving this method some problems in

Download English Version:

https://daneshyari.com/en/article/456106

Download Persian Version:

https://daneshyari.com/article/456106

Daneshyari.com