An Equitably Fair On-line Auction Scheme*

Emmanouil Magkos¹, Mike Burmester¹,², Vassilios Chrissikopoulos¹

¹ Department of Informatics, University of Piraeus, Greece
{emagos, chris}@uni.pi.gr
² Information Security Group, Royal Holloway, University of London, UK
mikeb@dcs.rh.bnc.ac.uk

Abstract. We present a sealed-bid electronic auction scheme that is equitably fair for the bidders and the seller. In this scheme, the interests of both the bidders and the seller are safeguarded: the identity of the non-winning bidders and their bidding behavior are protected (anonymity), and the bidders cannot withdraw their bids without being detected (non-repudiation). The scheme fulfills the requirements of a secure auction scheme and is verifiable. It extends the Stubblebine & Syverson auction scheme that is not equitably fair (it does not prevent bid withdrawals). Our scheme employs a Registrar and an Auctioneer for which no special trust assumptions are made.

1 Introduction

Electronic auctions are increasingly popular among the members of the Internet community. Many auction houses adopt security mechanisms that are fortified by, and result in, the non-anonymity of bidders and/or the non-privacy of their bids. To hold bidders accountable, bids are authenticated and transactions are logged. As a result, buying profiles may be constructed and the personal information of users (e.g., their bidding behavior) may be used in several ways.

In this paper we propose a cryptographically secure scheme for sealed (first or second-price) electronic auctions that is equitably fair [4] for the bidders and “society”. That is, while the identity of the bidders and their bidding behavior are protected, bidders are accountable for their actions (i.e., they cannot withdraw their bids). This protects “society” (the seller or/and the auctioneer) from being abused by irresponsible bidders. Therefore, our system treats the bidder and the seller/auctioneer equitably: bidders cannot withdraw their bids, and the Auctioneer cannot find out the identity of a bidder.

We built a sealed-bid auction protocol, which satisfies all the requirements of a secure auction system and differs from [33] in that, while preserving anonymity and privacy prior to the auctioneer’s commitment, it prevents bidders from withdrawing their bids. We believe that bid-withdrawal, even if the bid has not yet been revealed, may be fair for the bidder but is not equitable [4] towards “society” (e.g., the seller/auctioneer). As argued in [4], if altered circumstances make a bid unprofitable

* Research supported by the Secretariat of Research and Technology of Greece.
or loss making, and a bidder is allowed to withdraw a bid, then “society” is threatened by the individual. Allowing bid withdrawal is as fair as allowing a seller to withdraw the item being auctioned, because altered circumstances make the sale unprofitable.

In our approach, bid-withdrawal can be traced after the auction has ended. For this purpose we make use of Time-Lock Puzzles\(^1\) [29] for non-repudiation. We also make use of Blind Signatures\(^2\) [9] for anonymity, a Cut-and-Choose\(^3\) technique [9] for correctness, and a Certified-Delivery mechanism [5] to prevent denial-of-service attacks. Checks are also made to ensure that only eligible bidders submit valid bids.

**Our Scenario.** We consider sealed auctions where non-winning bidders retain their anonymity, but no bidder can withdraw a bid. There are several applications in which the anonymity of bidders is an important design feature of auctioning. For example, the bidding behavior of non-winning bidders might be of commercial value. Furthermore, by preventing bid withdrawals, bidders cannot dynamically control an auction by withdrawing their bids when altered circumstances make these unprofitable. Our scenario is appropriate for high security level auctions, where correctness and anonymity are important.

### 1.1 Related Work

Franklin and Reiter [17] designed and implemented a distributed service for performing sealed-bid auctions. This makes use of *Threshold Secret Sharing* [31] and *Verifiable Signature Sharing* [18] for protection against faulty auction servers, and off-line *Digital Cash* [7] for non-repudiation. Franklin and Reiter also proposed a modification of their protocol to establish anonymity for loosing bidders, but in this case, a coalition between either two faulty servers from different auctions or a faulty server and the bank, may reveal the identity of loosing bidders. Furthermore, threshold mechanisms are not applicable for auctions run by small organizations where all parties involved may be corrupted [25]. Finally, the use of Digital Cash creates an opportunity cost, especially in the case of large bids.

Harkavy, Tygar and Kikuchi [21] used *Verifiable Secret Sharing* [11] and *Secure Distributed Computations* [2] to perform sealed-bid electronic auctions. Their protocol establishes privacy for all but the winning bidder, even after the end of the bidding period. They also suggested the use of *Identity Escrow* [23] mechanisms to establish non-repudiation while preserving anonymity. Their protocol cannot handle tie-breaking (i.e., when several bidders tie for the highest bid) without sacrificing privacy. In [22], they deal with the tie-breaking problem by adding an extra auction

---

\(^1\) With Time-Lock Puzzles, a message is encrypted so that it cannot be decrypted without running a computer continuously for at least a certain amount of time.

\(^2\) Blind Signatures are the equivalent of signing carbon-paper-lined envelopes. A user seals a slip of a paper inside such an envelope, which is later signed on the outside. When the envelope is opened, the slip will bear the carbon image of the signature.

\(^3\) Cut-and-Choose techniques are used to establish correctness in a blind signature protocol. The signer opens all but one envelope and then signs the remaining envelope.