Optimization of Electronic First-Bid Sealed-Bid Auction Based on Homomorphic Secret Sharing

Kun Peng, Colin Boyd, and Ed Dawson

Information Security Institute,
Queensland University of Technology
{k.peng, c.boyd, e.dawson}@qut.edu.au
http://www.isrc.qut.edu.au

Abstract. Although secret sharing techniques have been applied to implement secure electronic sealed-bid auction for a long time, problems and attacks still exist in secret-sharing-based electronic sealed-bid auction schemes. In this paper, a new secret-sharing-based first-bid e-auction scheme is designed to achieve satisfactory properties and efficiency. Correctness and fairness of the new auction are based on hard computation problems and do not depend on any trust. Complete bid privacy based on a threshold trust is achieved in the new scheme. Attacks to existing secret-sharing-based sealed-bid e-auction schemes are prevented.

1 Introduction

The first secure electronic sealed-bid auction scheme [3] is based on threshold secret sharing. Since then, more secret-sharing-based sealed-bid e-auction schemes [4,6,5,10] have been proposed. Most of them [4,6,10] are supposed to support first-bid sealed-bid e-auction. However as will be shown many security problems exist in these auction schemes and they are vulnerable to various attacks. The newest and most advanced of them, [10], pointed out lack of secret sharing verification and vulnerability to three attacks in the previous secret-sharing-based sealed-bid e-auctions. However, the countermeasures in [10] cannot completely prevent these three attacks. In this paper, drawbacks of the previous secret-sharing-based sealed-bid e-auction schemes are listed and analysed. Then a new secret-sharing-based sealed-bid auction scheme is proposed, which can implement secure and efficient first-bid sealed-bid e-auction. Several attacks in the existing secret-sharing-based sealed-bid e-auction schemes are prevented in the new scheme.

2 Requirements and Related Work

Auction is a useful tool to distribute resources. The principle of auction is to sell goods at the highest possible price. Sealed-bid auction usually contains four phases: preparation phase, bidding phase, bid opening phase and winner determination phase.

E. Dawson and S. Vaudenay (Eds.): Mycrypt 2005, LNCS 3715, pp. 84–98, 2005.

1. In the preparation phase, the auction system is set up and the auction rule is published.
2. In the bidding phase, every bidder submits a sealed bid through a communication network.
3. In the bid opening phase, the bids are opened to determine the winning price.
4. In the winner determination phase, the winner is identified.

The following properties are often desired in sealed-bid auction.

1. **Correctness**: The auction result is determined strictly according to the auction rule. For example, if first bid auction is run, the bidder with the highest bid wins and pays the highest bid.
2. **Bid confidentiality**: Each bid remains confidential to anyone other than the bidder himself before the bid opening phase starts.
3. **Fairness**: No bidder can take advantage of other bidders (e.g. recover other bids and choose or change his own bids according to other bids).
4. **Unchangeability**: Any bidder, especially the winner, cannot change or deny his bid after it is submitted.
5. **Public verifiability**: Correctness of the auction (including validity of the bids, correctness of bid opening and correctness of winner identification) must be publicly verifiable.
6. **Bid Privacy**: Confidentiality of the losing bids must be still retained after the auction finishes. Strictly speaking, no information about any losing bid is revealed except what can be deduced from the auction result.
7. **Robustness**: The auction can still run properly in abnormal situations like existence of invalid bid.

The commonly used auction rules in sealed-bid auctions include first bid auction and Vickrey auction. In a first bid auction, the bidder with the highest bid wins and pays the highest bid. In a Vickrey auction, the bidder with the highest bid wins and pays the second highest bid. Another popular rule, the i^{th} bid auction [5] is a multiple-item version of first bid auction or Vickrey auction.

In a secure auction scheme, secrecy of the bid is very important. Usually, bid confidentiality must be achieved without any trust on the auctioneers, as loss of confidentiality is fatal to fairness of the auction. If a bidder can collude with some auctioneers to know other bids before submitting his own bid, he can win at a price as low as possible in a first bid auction, which violates the principle and fairness of auction. On the other hand, bid privacy can be based on some trust, like a threshold trust on the auctioneers as breach of a bidder's personal privacy is not so serious and is tolerable in some cases. Implementation of bid privacy is rule-dependent. Although Vickery auction is preferred in many applications, it is difficult to achieve bid privacy in Vickrey auction. As the winner's bid and the identity of the bidder submitting the winning bid must be kept secret as required in bid privacy, there is no practical method to achieve bid privacy in Vickrey auction. As bid privacy is required in this paper, we focus on first-bid auction.