Abstract: An Untraceable, Anonymity and Secure Sealed-bid Auction Schemes using Threshold Cryptosystem without A Third Party

Wei-Chen Wu[1], Horng-Twu Liaw[2], and Chih-Ta Yen[3]
[1]*Computer Center, Hsin Sheng College of Medical Care and Management, Taoyuan County, Taiwan, R.O.C.*
[2]*Department of Information Management, Shih Hsin University, Taipei, Taiwan, R.O.C.*
[3]*Department of Information Management, National Taiwan University of Science and Technology, Taipei, Taiwan, R.O.C.*
[1]*wwu@hsc.edu.tw,* [2]*htliaw@cc.shu.edu.tw*

Abstract

This paper proposes untraceable and secure sealed-bid auction schemes which adopt threshold cryptosystem without a third party. In the previous proposed sealed-bid auction schemes, an auctioneer is responsible for opening bids. However, malicious auctioneers can conspire with malicious bidders by revealing all bidding prices before the bid opening stage for bidding optimal bidding price to win the auction. To prevent against this, we decide to eliminate auctioneer from opening phase and involve plural clerks to choose secret keys, and then clerks distribute public keys to each other. On the bid opening phase, the clerks can cooperate with each other to open the bids without an auctioneer by using Pedersen's protocol and Lagrange interpolating polynomial. Hence, an auctioneer is only responsible for verifying user's identification and checking whether bids are valid or not. Furthermore, for enhancing security in our schemes, we utilize a hardware framework entitled "Untraceable Decryptor" to make all bids pass through it when the bids are transferred to clerks.