

On the Security of Two Sealed-Bid Auction Schemes

Kin-Woon Yeow, Swee-Huay Heng and Syh-Yuan Tan

Faculty of Information Science and Technology,

Multimedia University, Melaka, Malaysia.

yeowkinwoon@gmail.com, {shheng,sytan}@mmu.edu.my

Abstract—In this paper, we cryptanalyze two sealed-bid auction schemes and show that both schemes are not secure against the known-bid attack. In the first scheme, we show that a dishonest sealer can swap the price of a sealed-bid and yet its validity remains intact; in the second scheme, we show that a dishonest auctioneer can forge a bidder's bid if the bidder was once a winning bidder. We propose a workaround for the former using a designated confirmer signature but not the latter which is fundamentally flawed.

Keyword—sealed-bid, auction, known-bid attack, sealer



Kin-Woon Yeow is a M.Sc. (I.T.) student under the Faculty of Information Science and Technology in Multimedia University, Malaysia. His research interests are applied cryptography and network security.



Swee-Huay Heng received her B.Sc (Hons) and M.Sc degrees from Universiti Putra Malaysia (UPM), and her Doctor of Engineering degree from the Tokyo Institute of Technology, Japan. She currently holds the position of Professor in the Faculty of Information Science and Technology, Multimedia University, Malaysia. Her research interest is in Cryptography and Information Security. She served in numerous technical Program Committees of international security conferences.



Syh-Yuan Tan received his Ph.D. from Universiti Tunku Abdul Rahman in 2015. He is currently attached to the Faculty of Information Science and Technology, Multimedia University, Malaysia as a senior lecturer. His research interests are Cryptography and Network Security, particularly on the provable security techniques.