# Chapter 7.8
# Analyzing the Privacy of a Vickrey Auction Mechanism

**Ismael Rodríguez**
*Universidad Complutense de Madrid, Spain*

**Natalia López**
*Universidad Complutense de Madrid, Spain*

## ABSTRACT

This article studies the properties of a distributed mechanism to perform the Vickrey auction. This mechanism, which was originally presented in López, Núñez, Rodríguez, and Rubio (2004), has the main characteristic that most of the information concerning the bids is kept private for both bidders and the auctioneer without the necessity of any trusted third party. In particular, after the auction is finished, only the value of the second-highest bid and the identity of the highest bidder are publicly revealed. However, in that paper, several questions about the applicability of the protocol were left unanswered. In particular, no implementation was provided. Besides, the analysis of the collusion risk was too brief. In this paper, we address these issues in a deeper way. Let us note that, as it is stated in Brandt and Sandholm (2004), it is impossible to create a completely private mechanism to perform the Vickrey auction. In particular, we identify a gap between the proposed protocol and the complete privacy: If any n-2 bidders and the winning bidder collude, the privacy is lost. Besides, some privacy properties can be broken by chance if some specific situations appear, though the probability of this threat decreases as the number of bidders increases. In addition, we present and analyze a simple implementation of the protocol, and we consider its practical applicability.

## INTRODUCTION

Auctions are very effective ways to allocate resources. There exist several auction mechanisms, with the Vickrey auction (Vickrey, 1961) being one of the mechanisms that has attracted more interest from the computer science researchers. This is a sealed bid where the bidder who submits the highest bid gets the item, but he/she pays the amount submitted in the second highest bid. As it is well known, the Vickrey auction has several good properties. In particular, it removes any incentive for bidders to bid *strategically*. This is so because the dominant strategy of each agent consists in submitting a bid for his or her reserve price, that is, the maximum price that the agent would pay for the auctioned item. Thus, the Vickrey auction is a *direct-revelation* mechanism since, in order to maximize their utility, agents have to say the truth.

In a Vickrey auction, the difference between the first and second prices is the *price* paid by the auctioneer to guarantee that all the agents tell the truth. However, as the *revenue equivalence theorem* (RET) claims (Myerson, 1981), this auction produces the same revenue for the auctioneer as other standard auctions (English, Dutch, first-price-sealed auction), though it is worth pointing out that in general, the auctioneer does not maximize the profit with respect to a more *flexible* scheme.[1] Actually, note that if the auctioneer found out in advance the reserve price of the highest bid, he/she would prefer to sell the item with a fixed price as *take-it-or-leave-it*. Besides, the Vickrey auction is usually assumed to be a *private-value* auction, that is, reserve prices are locally and independently fixed by each agent. This property disallows an agent to get more interested in an item because other agents have higher bids.

Privacy issues may be a handicap in Vickrey auctions. If the auctioneer has access to all the bids, then he/she can use this information in subsequent auctions of similar items (by using a *take-it-or-leave-it* strategy). Thus, it is not desirable for the agents that the auctioneer knows their reserve prices. Moreover, if the bidders know all the bids, they can also adapt their subsequent bids.[2] This would imply that the auction is not with private value anymore, so that reserve prices are not used afterwards (Sandholm & Lesser, 1995).

Thus, a desirable characteristic to be included in Vickrey auctions consists in keeping, as much as possible, the *privacy* of the bids. In other words, our goal is that at the end of the auction, each bidder is the only one who knows his/her own bid. Moreover, it would also be very desirable that neither the bidders nor the auctioneer know the value of other bids. Obviously, there always exist some minimal exceptions to complete privacy. In particular, we need to know the second-highest bid as well as the highest bidder. However, in order to resolve the auction, we need to know neither the highest bid nor the second-highest bidder.

Some protocols have been proposed to keep the good properties of the Vickrey auction while guaranteeing privacy (see, e.g., Lipmaa, Asokan, & Niemi, 2002; López et al. 2004; Naor, Pinkas, & Sumner, 1999). In Lipmaa et al. (2002), privacy is partially lost: although the *auction authority* cannot relate bids with bidders, he/she knows the value of all the bids that have been submitted. In the case of Naor et al. (1999), the collusion of the auctioneer and the *auction issuer* allows them to infer all the bids of the bidders. In López et al. (2004), bidders do not communicate their real bid to other agents (neither to other bidders nor to the auctioneer), so that protocol does not depend on a trusted third part as the previous protocols do. However, in that paper, some topics concerning its practical applicability were not addressed. Besides, some scenarios of privacy threat were tackled too briefly. In particular, some situations concerning the collusion of bidders were not properly discussed. Hence, a deeper analysis of this protocol is still needed.

In this paper, we present a (simple) implementation of that protocol and analyze some of its properties in a deeper way. In particular, we show that the collusion of bidders cannot breach the privacy with certainty unless n-2 bidders and the winner (that is, n-1 bidders) collude, where n is the number of bidders in the auction. Besides, we show that other collusion threats may appear *by chance*, though the probability of these situations decreases with the number of bidders. As it is stated in Brandt and Sandholm (2004), it is