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.

Keywords: cryptography; Internet privacy; Internet security; online auctions; online privacy

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 submit-
tation of the bids. 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 impossible to find a completely private mechanism to perform the Vickrey auction. This result imposes an upper bound of privacy-preserving efficiency in that framework. In particular, it shows that it is not possible to eliminate all of the previous collusion threats from the protocol. However, to the best of our knowledge, this is the protocol that provides the best privacy properties for performing the Vickrey auction without the necessity of any trusted third party.

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 impossible to find a completely private mechanism to perform the Vickrey auction. This result imposes an upper bound of privacy-preserving efficiency in that framework. In particular, it shows that it is not possible to eliminate all of the previous collusion threats from the protocol. However, to the best of our knowledge, this is the protocol that provides the best privacy properties for performing the Vickrey auction without the necessity of any trusted third party.
Related Content

Knowledge-Based Intermediaries
[www.igi-global.com/article/knowledge-based-intermediaries/1903?camid=4v1a](www.igi-global.com/article/knowledge-based-intermediaries/1903?camid=4v1a)

IoT for Hospitality Industry: Paperless Buffet Management
[www.igi-global.com/chapter/iot-for-hospitality-industry/180746?camid=4v1a](www.igi-global.com/chapter/iot-for-hospitality-industry/180746?camid=4v1a)

E-Retail Adoption in Emerging Markets: Applicability of an Integrated Trust and Technology Acceptance Model
[www.igi-global.com/article/e-retail-adoption-in-emerging-markets/157393?camid=4v1a](www.igi-global.com/article/e-retail-adoption-in-emerging-markets/157393?camid=4v1a)
The Roles of Online Intermediaries in Collective Memory-Supported Electronic Negotiation
[www.igi-global.com/chapter/roles-online-intermediaries-collective-memory/8705?camid=4v1a](www.igi-global.com/chapter/roles-online-intermediaries-collective-memory/8705?camid=4v1a)