Economic Analysis and Implementation of a Discrete Vickrey Auction Over the Internet

Tetsuji Okamoto

February 7, 2002

Adviser: Rene Peralta
Senior Project Proposal

1 Introduction

Each year, millions of Internet users utilize online auctions to purchase and sell various products. Despite the recent economic slowdown, consumers and businesses continue to spend money online (according to Nielsen/NetRatings, consumers online spending in the United States jumped 104 percent in the last year, from $2.6 billion in 2000 to $5.4 billion in 2001). As online auctions become a mainstream business, it is crucial for auction protocol developers to find ways to limit fraud and prevent sub-optimal pricing of items. According to Internet Fraud Watch, over 80 percent of Internet frauds in 2001 were related to online auctions. This suggests that more secure auction protocols are vital for the online auction industry to remain popular to its users. The entire system works only when buyers can trust the sellers. Uncontrolled fraudulent behavior on auction sites will break the system and cause these sites to suffer. A sound implementation of an auction protocol that provides solutions for the various problems online auction sites today will be beneficial for the industry as a whole.

2 Vickrey Auction Overview

The current project focuses on one type of auctioning called the Vickrey auction (named after Nobel Prize winner William Vickrey) that reduces certain fraudulent behavior and induces each bidder to bid his/her true valuation of the auctioned item. It consists of each bidder submitting a sealed bid. After all bids are submitted, the auctioneer starts by asking the bidders if any of them bid for a certain amount. If everyone answers "no", the auctioneer will decrease the bid by the minimum incremental amount and continue with the questioning. The auction finishes when the top two bidders are identified. Then these
bidders will have to verify that they had previously committed to that amount by opening
their sealed bids. The winner of the auction is the bidder with the highest bid. However,
this person will purchase the item at a price equal to the second-highest bid (or highest
unsuccessful bid). The assumption is that each bidder is ignorant of the other bids.

The Vickrey auction is advantageous to use compared to other types of auctions because
it 1.) provides solutions to control several types of fraudulent behavior and 2.) induces
bidders to bid their true valuations, while the expected revenue for Vickrey auctions, with
some assumptions, is the same as for English or Dutch auctions. The fraudulent behaviors
that the Vickrey auction currently addresses are bid shielding, shilling, and sniping. Bid
shielding occurs when a high bid is withdrawn at the last minute, allowing a lower bid to
become the winning bid. The Vickrey auction forces every bidder to commit to his/her bid
beforehand. If bid shielding occurs, the protocol will catch it during the verification stage.
Shilling occurs when spurious bids are used to force up the price. This can be prevented
with the Vickrey auction because the bids are sealed (meaning the bidders will not know
that the price is being forced up and thus, there is a low probability of success). Sniping
occurs when a bidder bids immediately before the auction is closed in hopes of prevent-
ing other bidders from responding. Because the Vickrey auction is not an English auction
wherein only higher bids may be made subsequently, a bidder that engages in sniping will
have very little effect on the outcome of the auction.

3 The “Discreet” Vickrey Auction

While the above behaviors can be controlled, the current protocol is not at its complete
state since it is still vulnerable to other attacks. The goal of this senior project is to in-
troduce those possible attacks on the protocol and to deal with them in an efficient and
logical manner, making the protocol more robust and acceptable for commercial use. Be-
cause this protocol was created from an economic perspective, it does not explain how the
bids will be sealed or how the auctioneer will verify them. Our discreet Vickrey auction
will utilize the bit commitment scheme (based on the quadratic residuosity assumption) to
cryptographically encrypt the bids. Also, to reduce the power of the auctioneer, the pro-
tocol will introduce a way of hiding the bid amounts from the auctioneer (except for the
two highest bids) even during the verification process. Previously, in the regular Vickrey
auction, the auctioneer had the power to open each bid during the verification stage. Giving
the auctioneer such authority over the bidding process can lead to numerous problems (this
will be elaborated on in the report). Also, the discreet Vickrey auction protocol will only
reveal the highest two bids - the other bids will not be disclosed to the public even when
the auction is completed. This report will include an analysis of these new features. This
protocol will be analyzed from an economic viewpoint, incorporating both game theory
concepts and real-world situations. Possible fraudulent behavior resulting from collusion
and the usage of multiple identities will also be analyzed. This report will also focus on
real-world situations where actions by bidders will cause sub-optimal valuations of items and attempt to find ways of preventing such occurrences. This paper will not focus on finding solutions for reducing the sale of pirated goods online or reducing the risk of online credit card fraud.

4 Deliverables

This senior project will require the following deliverables:

4.1 15-20 page report which includes the following topics:

- A general explanation of the online auction industry
- A careful overview of the Vickrey auction protocol and the new additions in our discreet Vickrey auction
- Current problems online auctions such as E-bay, Yahoo! Auctions, and UBid face
- Possible fraudulent behaviors that may occur (considering both C2C and B2B situations) and why the discreet Vickrey auction will help alleviate some of those problems
- If such behaviors cannot be solved with the current protocol, alter the protocol to accommodate those possible threats
- Provide economic reasons as to why bidding amounts (except for the top two bids) should not be revealed to the bidders or the auctioneer
- Discuss ramifications of a fraudulent aucioneer (i.e. the person who checks the bids and decides the winner)
- Whether this auction procedure is commercially feasible (i.e. revenue generating)
- Why it is important to keep bids encrypted and secret - possible economic problems that will emerge when the bids are revealed
- To what extent should the bidder’s identity remain anonymous
- Possible real-world scenarios that might occur during the Vickrey auction (i.e. withdrawal of bids, going offline after a bid is made, errors during transmission of bids, other system errors)
4.2 Partial implementation of the protocol, which includes:

- Electronic circuit that compares two bids to see if one is indeed higher than the other (used during verification stage) and minimizes the use of AND gates which have been shown to be computationally expensive

- Possible complexity analysis of the auctioning protocol