Analysis and Design of an Online “Discreet” Vickrey Auction Protocol

Tetsuji Okamoto

May 1, 2002

Abstract

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, consumer 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 discourage collusive, entry-deterring and predatory behavior, as well as to prevent sub-optimal pricing of items. This paper introduces a new protocol that improves on the Vickrey (second-price, sealed-bid) auction used for multiagent systems. We assess the advantages and disadvantages of the original Vickrey auction over other types of auctions and explain how our “discreet” Vickrey auction increases privacy and decreases fraudulent behavior beyond the original model. We will describe how our design enables bidders to check if other bidders and/or the auctioneer are engaging in fraudulent activities without forcing them to reveal their actual bid values. The issues of bidder anonymity, fraudulent auctioneers, withdrawal threats and anti-social agents are also addressed. From our analysis, it can be found that the “discreet” Vickrey auction design reduces the risk of a lying auctioneer and prevents private corporate information from being revealed to the public. The current paper will focus on business-to-business (B2B) transactions involving repetitive auctions of homogenous items. However, most of the game-theory logic found in this paper can be applied to any auction scheme involving a multiagent system.
## Contents

1 Introduction 3

2 Vickrey Auction Explained 3
   2.1 The General Protocol 3
   2.2 Advantages of the Vickrey Auction 4
      2.2.1 Dominant Strategy 4
      2.2.2 Elimination of Winner’s Curse 5
      2.2.3 Low Bandwidth and Time Consumption Requirements 6
      2.2.4 Shilling Avoidance 6
      2.2.5 Private Information is Kept Private 7
      2.2.6 Reducing Collusion Among Bidders and Entry Deterrence 7
   2.3 Problems with the Original Model 8

3 A “Discreet” Vickrey Auction Design 9
   3.1 Overall Protocol 9
      3.1.1 Bidding Stage 10
      3.1.2 Winner-Determination Stage 10
      3.1.3 Verification Stage 11
   3.2 Circuit Implementation 11
   3.3 Why Only The Second Bid Is Revealed 12

4 Improvements From Vickrey Auction 13
   4.1 Privacy Issues 13
   4.2 Limiting the Power of the Auctioneer 14
      4.2.1 Bid-revealing Auctioneer 14
      4.2.2 Bidder-Auctioneer 14
      4.2.3 Lying Auctioneer 15
   4.3 Summary of Improvements 16

5 Problems With Design and Possible Remedies 16
   5.1 Withdrawals From Auction 16
   5.2 Anonymity and Encryption Key Storage Issues 17
   5.3 Solving Ties 20
   5.4 Anti-social Agents 21

6 Possible Real-world Applications 21

7 Concluding Remarks 22
1 Introduction

In recent years, there has been an increased interest in the area of multiagent systems and auction protocols. Due to the explosive popularity of the Internet, the use of electronic commerce as a revenue-generating business has also surged. Governments, corporations, as well as small businesses are eager to find ways of efficiently allocating their resources with the use of auction-type mechanisms. There are several auction protocols used on the market today. The most prevalent form is the English auction. Bidders successively offer higher prices (each bid must exceed the previous bid by some minimal bid increment). The item is rewarded to the highest bidder. In the Dutch auction, the auctioneer starts with a high price and gradually lowers it until someone is willing to buy the item. Recently, there has been increased interest in a type of auction called the Vickrey auction. In this auction, the item is awarded to the highest bidder at the second-highest price. For business-to-business and e-commerce applications, the Vickrey auction seems to be a very attractive auction protocol since it efficiently allocates resources, requires low-bandwidth connections, and provides more privacy compared to other types such as the English or Dutch auctions. Despite such theoretical advantages, the Vickrey auction is rarely used in practice due to several limitations. In the current paper, we will introduce a design of the Vickrey auction that uses a type of cryptographic primitive called “selective disclosure” envelopes to “seal” the bids - a technique that allows participating agents to securely perform second-price auctions [Per02a]. The goal of this work is to introduce a Vickrey-type auction that diminishes fraud and reduces the dependence on the auctioneer. Not all types of fraud will be considered. We will not address the issues concerning false or misrepresented sale items and how payments should be made. We will attempt to show how our design solves some problems that the original Vickrey auction fails to address as well as to identify potential problems that still may persist. Compared to players in business-to-consumer (B2C) transactions, players in business-to-business (B2B) transactions are more likely to collude, more sensitive to private information being revealed, and more likely to big large amounts of money. Because there seems to be more inherent risk involved in B2B auctions, the focus of the current paper will be on such transactions.

2 Vickrey Auction Explained

Before we introduce the “discreet” Vickrey auction protocol, it is important to understand the original Vickrey auction since it forms the basis on which we build our protocol. The attractive features of the original Vickrey auction are retained in our design.

2.1 The General Protocol

The Vickrey auction (named after 1996 Nobel Prize winner William Vickrey) is a second-price, sealed-bid auction. The item is awarded to the highest bidder at a price
equal to the second-highest bid. Thus, the winner does not pay his/her own bid amount but rather a lower one, bid by the second-highest bidder. All bids are “sealed” and each bidder is ignorant of the other bids (it is important to note that William Vickrey did not specify how these bids were to be “sealed” - in the 1960’s when his paper was published, research in cryptography and exchanging messages over a network were in their early developmental stages). Each bidder is allowed one bid per round and there is only one round of bidding (therefore a bidder can bid once for a particular item). After all bids are submitted, the auctioneer opens all bids to determine the highest bid (to identify the winner) and the second-highest bids (to identify the price the winner pays). Once again, it is important to note that Vickrey does not describe how the bids are “opened” and how all bidders are able to verify that the auctioneer is executing the auction truthfully.

2.2 Advantages of the Vickrey Auction

Several studies have shown that Vickrey auctions have several advantages over other types of auctions. The following characteristics make this auction scheme particularly attractive for multiagent applications.

- The auction has a bidder dominant strategy - to submit a bid equal to his/her true valuation
- Avoids winner’s curse - paying more for an item than its true value
- Assuming auction is done online and auctioneer is fully trusted, it requires low bandwidth and time consumption
- Avoids shilling phenomenon
- Bidding information is kept private except from auctioneer (depends on how cryptographically secure the encryption is)
- Reduces collusion and entry deterrence compared to ascending-price auctions

The following subsections will explain each advantage in detail and provide insight as to why the Vickrey auction is a great candidate for the allocation of resources.

2.2.1 Dominant Strategy

One of the most attractive features of the Vickrey auction is that participating bidders have a dominant strategy - a strategy that creates the highest possible payoff independently of the strategies used by other bidders. This dominant strategy is to bid one’s true valuation of the item[Bra97]. Even if a bidder knows all the other bids in advance, he/she will do best by bidding his/her private valuation. Using an example should clarify this phenomenon. Consider that you (bidder A) are bidding against many other bidders. It suffices to model only one opposing agent (bidder B) representing the entire competition because A only cares whether he/she wins or loses. There is no distinction between the bidders - all that matters is the highest bidder which we will denote as $B_b$. Denote your true valuation as $V_a$. 
Scenario 1: Does bidding a higher price \( (B_a) \) increase the return?
(a) If \( B_b > V_a \) (bidding true valuation loses auction)
If you bid \( B_a > B_b \), you win the auction but pay \( B_b > V_a \) so payoff is negative.
If you bid \( B_b > B_a > V_a \), you still lose and payoff is zero.
(b) If \( B_b < V_a \) (bidding true valuation wins auction)
If you bid \( B_a > V_a \), you still win the auction and payoff is \( V_a - B_b \).

Scenario 2: Does bidding a lower price increase the return?
(a) If \( B_b > V_a \) (bidding true valuation loses auction)
If you bid \( B_a < B_b \), you still lose and payoff is zero.
(b) If \( B_b > V_a \) (bidding true valuation wins auction)
If you bid \( B_a > B_b \), you still win the auction and payoff is \( V_a - B_b \).
If you bid \( B_a < B_b \), you lose the auction and payoff is zero.

From this example, it is clear that bidding higher will raise the probability of winning but the payoffs to winning are not higher and may end up being negative (seen in scenario 1). Bidding lower will only raise the probability of losing without raising the payoff to winning[Con02]. Thus, the optimal strategy is to bid \( V_a \).

2.2.2 Elimination of Winner’s Curse

The Winner’s Curse refers to the fact that the bidder with the highest private valuation wins the auction. However, that winner has paid more for the object than any other bidder would, meaning other participants estimated a lower market value than the winner. The highest bidder wins the auction, but in essence, loses (decrease profits) because he/she could have bid lower and still won. If bidders have reasonable information about the worth of the item, then the average of all guesses is likely to be correct. However, the winner offers the highest bid, which is the furthest from the actual value. Thus, the bidder who makes the largest positive error in his/her valuation is declared the winner. Because of this Winner’s curse, participants of an auction often defer from bidding out of fear that he/she will pay too high a price - preventing optimal allocation of resources. Unlike English and Dutch auctions wherein the highest bidder wins by paying the highest price, the Vickrey auction’s second-pricing and sealed-bid scheme helps eliminate the effects of the Winner’s Curse. No one is deterred out of fear that he/she will pay too high a price since all bids are sealed. A bidder does not know the valuations of the other bidders and can bid more aggressively - up to the bidder’s true valuation of the item. The second-pricing scheme further enables bidders to overcome fears of the Winner’s Curse since they may bid over the market consensus but still pay less than they bid. Since the amount that bidders bid will not be relative to what their competitors bid, the fear of the Winner’s Curse is diminished, bidders will bid their true valuations, and there will be better allocation of resources.
2.2.3 Low Bandwidth and Time Consumption Requirements

As indicated in the Vickrey auction protocol description, there is only one round of bidding. Current online auctions use open-cry, English-type auctions that involve multiple rounds of biddings. Studies by Roth and Ockenfels have shown that 20% of all bidders made their last bids in the last hour before closing on eBay (14% in the last 10 minutes). Also, 68% of auctions on eBay had the last bid received in the last hour of bidding (55% during last 10 minutes) [RO01]. These findings show that current Internet auctions are highly concentrated near the end. This is not an desirable feature, especially for the Internet wherein people use different connection services to access the network (ISDN, phone dial-up, CATV, fiber optics, ADSL, wireless). The bidders with persistent connection to the Internet has a definite advantage since they are able to see the prices change in real-time and place bids accordingly. Current Internet auctions require bidders to be online at the last few minutes of the bidding stage to win the auction. For the Vickrey auction (assuming it is implemented online), the winner can be a bidder that placed a bid during the early stages of the bidding process. A bidder can simply log on, place his/her bid and go offline since other bidders’ valuations will not be influenced by the placement of earlier bids. In this way, there is a low requirement for bandwidth and time consumption. Due to the fact that the winning bid can be placed anytime, the Vickrey auction will appeal to a greater audience. This feature is also appealing because it solves the problem of sniping wherein bidders wait for the last seconds to bid. In regular ascending-type auctions sniping prevents other competitors from winning the item - they simply run out of time to submit their bid. Since Vickrey auctions are not ascending-bid auctions with time constraints, the effects of sniping will be minimal. Preventing a last-second bid from being submitted will not guarantee a win because the winning bid can be submitted any time during the bidding phase. The low time consumption requirement will enable people that cannot be present at the end of the bidding process to place bids early and still be the winning bidder. This auction will bring in bidders that previously did not want to spend time sitting in front of the PC during the bidding process. From this point of view, the Vickrey auction is more attractive than the English or Dutch auctions.

2.2.4 Shilling Avoidance

Shilling is a type of fraudulent behavior used on Internet auction sites in which sellers bid on their own items or persuade others to do so in order to drive up the price. When a non-group member bids at a price that the seller is satisfied with, the group members stop their shilling. The problem of shill bidding is becoming a growing concern for Internet auction site overseers. Vickrey auctions prevent shilling since the bids are sealed and not revealed until the verification stage. Bidders cannot falsely increase the bidding price because the “bidding price” simply does not exist. Unlike English auctions wherein the bidding price increases as the auction proceeds, the Vickrey auction does not reveal any information about the individual bids until all bids are submitted. Therefore, potential shill bidders who place numerous bids will most likely win the auction, end up paying the transaction fee (2-3% of the item value) to the auction site, and receive nothing in return (since he/she buys back what he/she sold). In the Vickrey
auction model, shill bidding is not an attractive strategy. By reducing the occurrence of shilling, online auction sites will not have to heavily invest in expensive shilling-detection software and shilling-related watchdog services that eBay currently does. It also decreases fraudulent behavior concerning bidders the use multiple user names to perform shilling. In this way, Vickrey auction can accommodate bidders who use multiple users.

2.2.5 Private Information is Kept Private

In business transactions, participating agents would want to prevent other competitors from knowing their valuations of the auctioned items. If the valuations are made public, competitors can utilize them to forecast future bids in subsequent auctions concerning the homogeneous item. Since Vickrey auctions use “sealed” bids, the participating agents should not be able to figure out the values of the submitted bids and hence the internal demands of the other competitors. The auctioneer “opens” and compares the bids privately to determine the winner (highest bidder) and price (second-highest bid value). In ascending-type, unsealed bidding auctions, each bid value is revealed to the public. Since each participant’s internal demands can be estimated by looking at their bid prices, competitors can perform various collusive tactics to shut out others from the market in subsequent rounds (several such tactics will be described in the next subsection). Thus, the optimal strategy for corporations is not to reveal internal information to competitors. The Vickrey auction’s sealed-bid design enables private values to remain secret (except to the auctioneer). However, as indicated previously, the original Vickrey auction model does not specify how the bids should be sealed to prevent competitors from obtaining private information or how the bids should be opened. Our discreet Vickrey auction design will introduce a secure scheme wherein bids can be “sealed” and “opened” (detailed description in next section).

2.2.6 Reducing Collusion Among Bidders and Entry Deterrence

Ascending and uniform-price auctions are particularly vulnerable to collusion while the Vickrey auction provides good ways of reducing such sub-optimal resource allocation schemes. In multi-agent ascending auctions, bidders can use the early stages when prices are still low to signal their views about who should win which objects[Kle00]. After a consensus is reached they can agree not to increase the price and “divide the pie”. Let’s say there are two bidders (A, B) for two identical items (1, 2), and a bidder must bid $5 above the previous bid. On the first round of bidding, ’A’ bids $20 and $15 on the two items (let’s say it values the item at $40) while ’B’ bids very low. In an open auction scheme, ’A’ could use this scheme to indicate to ’B’ that it hopes to buy ’1’ at $20 and that if ’B’ bids on ’2’, it would not outbid ’B’. On the subsequent round, ’B’ will bid up ’2’ to $20 and both companies will walk away with the item at the same low price. Since the Vickrey auction is a sealed bid, each participating agent must make a single, “best” offer for each object so participants would be unable to exchange signals.
According to Klemperer, ascending auctions allow punishment of rivals who fail to cooperate [Kle00]. In Vickrey auctions, participating agents cannot identify non-cooperating players since the bids are sealed. Unless the auctioneer colludes and reveals the bidders’ identities, punishment for non-cooperation can be prevented. This thus reduces the time and costs used by corporations to predict what others will bid.

On top of reducing collusion among bidders, the Vickrey auction also reduces entry deterrence. Studies have shown that low participation rates in auctions cause inefficiency in the process and lower profitability for the auctioneer [BK96] - two unattractive qualities. In ascending-price auctions, participants often presume that the firm that intends on winning will continue to outbid its competitors. Small, “weaker” firms thus have little incentive to enter the auction, especially when there is a transaction fee involved in participating [Kle00]. In a Vickrey auction, there is a higher probability that a weaker firm wins. Since it is a single-bid auction, the large firm cannot use the strategy of bidding low (to maximize the return) and continuously outbidding any other incoming bids. Thus, Vickrey auction can attract more entrants. Also, outcomes in ascending auction can be dramatically influenced by apparently small advantages in valuation or in reputation for being a strong bidder [Kle00]. From the points made above, it can be said that ascending auctions have several vulnerabilities that can be alleviated using the second-price, sealed-bid auction scheme.

2.3 Problems with the Original Model

Although the original Vickrey auction protocol has several attractive features, it is seldomly found in real-world applications. The two most notable deterrents are the vulnerability to a lying auctioneer and the reluctance of bidders to reveal their private valuations [Bra01]. In the original model, the auctioneer is the agent that opens all bids and determines the winner. Under this protocol, the highest bidder has to trust the auctioneer when he/she is told the second highest price (the amount he/she has to pay). In any multi-agent system, giving one party too much authority will create opportunities for members of that party to engage in self-optimizing behaviors that may not be globally optimizing. The original Vickrey auction is no exception. For example, a non-trustworthy auctioneer could open the bids (once all bids have been submitted), find the winner and insert a new bid just barely under that to ensure higher revenues. Other types of auctioneer-led fraudulent behavior are described in subsequent sections. A new design that reduces the power of the auctioneer should be introduced to weaken the auctioneer’s position in collusive agreements. Another problem with the original Vickrey auction is that each participating agent will reveal their private valuations to the auctioneer. As stated previously, one attractive feature of the Vickrey auction is that participants have a dominant strategy of bidding their true valuations. Since most auctions are not one-time transactions (especially in business-to-business auctions for raw materials), corporations prefer to keep the true valuations of auctioned items private and to prevent others from accessing such sensitive information. The new protocol must find a way of securely encrypting the bids so no other competitor can see the bid values. Moreover, it should prevent the auctioneer from finding out the true valuations.
since a corrupt auctioneer may accept bribes in exchange for private bid values. The original Vickrey auction models fail to explain how the bids will be sealed, opened, and verified. It also does not address the issue of anonymity - should the participants have an ID number, should their encryption keys have an identification? In our design, we will attempt to solve these shortcomings and provide a sound protocol that will be robust to fraudulent behavior involving the bidders, auctioneer, and/or the seller.

3 A “Discreet” Vickrey Auction Design

From the previous section, it can be seen that the Vickrey-type auction scheme has several attractive features, namely the low bandwidth and time consumption requirement, optimal allocation of resources, and increased privacy due to the sealing of bids. Although the Vickrey auction idea has recently found many supporters, this type of auction is rarely implemented and utilized in practice. The description of the auction indicates that all bids must be “sealed”, but it does not specify how it should be sealed. Also, the protocol does not specify how to verify that the winner did indeed bid the highest price or that the price he/she pays is indeed the second highest price. Our discreet Vickrey auction protocol will explain one way of implementing a valid Vickrey auction. In other words, we will attempt to introduce a working design that retains the attractive features of the original Vickrey auction and solves the problems stated in the previous section. We will also explain the reasons why we chose to implement this auction in the ways described below.

3.1 Overall Protocol

As stated before, this “discreet” Vickrey auction will attempt to decrease the power of the auctioneer, prevent private information from being released, and reduce collusive behavior. In this protocol, we will be using “selective disclosure envelopes” (SD-envelopes) as a mechanism for sealing the bids [Per02a]. These envelopes consist of an encrypted and committed string of bits. The originator of the envelope can publicly reveal any partial information of the string to the auctioneer using a disclosure method called the “discreet proof”. This particular type of proof can successfully convince the auctioneer that a statement made concerning the string of bits is true without revealing any other information[BDP00]. It can show that a string of encoded bits is either greater or less than the second-highest value (which is revealed to the public) while keeping the actual bid value private. A comprehensive study of this mechanism can be found in Boyar, Damgards, and Peralta’s article on “Short Non-interactive Cryptographic Proofs” [BDP00]. In essence, this mechanisms enables bidders to send sealed, committed bids that other competitors are unable to see. Moreover, the auctioneer will not see the value of any bids except the second-highest one (which is revealed to the public). The highest bid will only be revealed to the auctioneer and not to the public. Although we can implement this protocol so that no one, including the auctioneer, is unaware of the highest bid value, it may prove to be too computationally expensive and cause inefficiencies in our protocol. Therefore, we recommend a scheme wherein
only the auctioneer knows the highest value.
The protocol can be divided into three general stages:

- Bidding Stage
- Winner-Determination Stage
- Verification Stage

3.1.1 Bidding Stage

During the bidding stage, bidders will send “selective disclosure envelopes” to an Internet bulletin board set up by the auctioneer. Each time a bid is made, the Internet bulletin board signals the occurrence of this new bid. As stated previously, these SD-envelopes contain encrypted individual bid values that cannot be decrypted without the private key owned by the originator [BDP00]. The actual encoding scheme used is a bit-commitment scheme based on the quadratic residue assumption (QRA) which encrypts each bit of the bid value (in bit form) into a string such that outside parties cannot tell if the encryption is that of a 0 or 1. Goldwasser and Micali has written an in-depth explanation of the QRA [GM84]. Another property of this scheme is that the bidder binds the encrypted bit, meaning he/she cannot change the actual bid value after it is encrypted. When the encrypted string is opened, the bidder cannot decrypt a particular string as both 0 or 1. We also assume the trapdoor property which means that the bidder can interpret any bid string of the appropriate length as a bit commitment and open it, regardless of how that string was produced [BDP00]. For this trapdoor QR-bit commitment scheme to work, the bidder must generate a Blum integer $N = P^r Q^s$ with $P$ and $Q$ primes such that $P \equiv Q \equiv 3 (\mod 4)$ and $r$ and $s$ are odd. The use of this Blum integer and the overall encryption procedure is specified in Boyar, Damgard, and Peralta’s article [BDP00]. The bidding stage terminates when time expires. At this time, none of the bidders nor the auctioneer know the values of the bids. All they know is the number of bids made for the particular item and the encrypted bit-commitment strings.

3.1.2 Winner-Determination Stage

In this protocol, valid offers are assumed to range from integers $L$ to $R$ wherein each distinct bid is divisible by a set monetary units (e.g. 5 dollars). Values for $L$, $R$ and the incremental value can be determined by the auctioneer to regulate the lowest and highest possible prices as well as the resolution of the bid space [Per02b]. During the winner-determination stage, the auctioneer starts off at the high price $H$ and works his/her way down. At each price, all bidders indicate whether their bid value was that called price. These replies are one-bit messages that should utilize authentication mechanisms when sent over unsecure networks. If all bidders indicate that they did not bid at that price, the auctioneer decreases the price by an incremental value and repeats the interrogation procedure. This stage terminates when the top two bids have been determined. Since this stage continues until the second highest bid is determined, the bidders do not know what the highest bid value was. When this stage is completed, the
auctioneer only knows the value of the highest and second-highest prices. The bidders still are unaware of their competitors’ bids.

3.1.3 Verification Stage

During the verification stage, the highest and second-highest bidders must prove that they were not lying in the previous stage by “opening” their SD-envelopes. The remaining bidders issue discreet proofs to show that their SD-envelopes had encrypted bid values that were below the second-highest bid (the sale price). The discreet proof provides a clever way of convincing the auctioneer as well as the other bidders without revealing the bid values themselves. A circuit will compute a one-bit output which tells whether it is less than the second-highest bid. The length of the proof in bits (omitting lower order terms) is: $4\theta \log_2(2\theta) + 2r(2\theta + k)$. The derivation of this equation can be obtained in Boyar, Damgard, and Peralta’s work [BDP00]. $\theta$ is the number of conjunctions in the circuit to arrive at the partial information. Since the circuit is assumed to perform only arithmetic modulo 2, conjunctions are multiplications (i.e. AND gates). Thus, the fewer AND gates in the circuit, the more efficient the proof. $k$ is the length of each bit commitment and $r$ is a security parameter ensuring that the probability that a fraudulent discreet proof is not detected is at most $(\frac{1}{2})^r$ [Per02b]. A bit commitment scheme using the QRA has been shown to be secure when $k$ is about 1000. $r$ can range from 10 to 100 depending on the desired security level of the auctioneer [Per02b]. During this stage, the highest and second-highest bidders send their private keys, both are verified by the auctioneer, and the highest bid value is made public. The auctioneer or the other bidders can use the circuit to compare and convince themselves that these two bids were indeed the two highest bids. The Internet bulletin board should be implemented so that if a bidder wants to check whether a competitor’s bid is indeed below the second highest bid, he/she simply clicks on the bidder’s bid icon. Upon clicking, the computer will go through the circuit and output a 1-bit answer. It is important to note that none of the bidders will know the actual bid values of each bidder since the discreet proof is used.

3.2 Circuit Implementation

As stated above, we must compare all bids except the highest bid to the now-public, second-highest bid during the verification stage. The circuit verifies that all other bids are indeed lower than the second-highest bid. This circuit will enable the auctioneer to compare two bids in an efficient manner without obtaining information about the actual bid values. The circuit merely outputs 1 if $A > B$ and 0 if $A \leq B$. By reducing the number of AND gates (our implementation uses a single AND gate per compared bit), we have optimized the efficiency of the calculation. Using AND gates for bit-commitment schemes have been shown to be computationally expensive [BDP00]. Therefore, reducing the number of AND gates used is an attractive quality. The actual computations that must be performed to implement the XOR and AND gates can be found in Boyar, Damgard, and Peralta’s work [BDP00]. The following circuit (see figure 1) compares two 5-bit strings (Y is encrypted, X is the second-highest bid that
has been revealed to the public). Note that it outputs a one-bit string.

3.3 Why Only The Second Bid Is Revealed

In the original Vickrey auction, the auctioneer was able to open all of the bids. To reduce the power of the auctioneer, we decided that only the second-highest bid needed to be revealed for the auction protocol to be executed successfully. If all bids were revealed to the public, then each bidder would know their competitors’ demand for the item and their true valuations. During the next round of auctions, the two that previously paid the highest prices can collude - one bids for a very high price and the other bids a price just above the third highest bid in the previous round (third highest bid is predicted by using past results). Although this is not a perfect scheme wherein the second highest bidder can successfully predict the third highest bid 100% accurately, making the third highest bid will increase the probability of a successful bidder-bidder collusion scheme. In this way, revealing the rest of the bids can reveal too much private information about the states of the competing firms and enable the two highest-paying firms to reduce their costs. This would hurt the profitability of the selling side as well as the auctioneer. Also, by revealing the bids, competitors
may increase their bids and subsequent rounds to intentionally outbid a participant to
shut them out of the market. Although they will take a short-term loss, it may end up
becoming a long-term gain for them when that competitors goes out of business and
reduces competition. Thus, there are incentives to engage in fraudulent behavior that
bring about sub-optimal allocation of resources. If all bids are not revealed, the cost of
effectively “shutting out” a competitor rises, which in effect decreases the occurrence
of the scheme described above. Bid values should not be revealed to the auctioneer
because they may then reveal private information to competitors, produce false bids to
help out a bidder, or falsely increase the second-highest price to increase transaction
fees. Because of these qualities, it is desirable to keep bids secret from both the bidders
and the auctioneer. We feel that only the second highest bid needs to be revealed. The
highest bid value does not have to be revealed - the bidder must be identified, but
the SD-envelope does not have to be opened. The auctioneer and the participating
bidders can check using the discreet proof that this bid is indeed the highest price
by comparing it to the second highest price (which is revealed). This is a remarkable
improvement from the original Vickrey auction wherein all bid values were revealed to
the auctioneer. Our design enables each bidder to check that the two highest bids were
indeed the two highest bids by running the circuit described above. However, no one
is able to decrypt the bid values. Nothing is revealed except whether a bid is greater
or less than the second-highest bid. This effectively controls the outflow of private
information that can later be used for collusive bidder-bidder, bidder-auctioneer and
seller-auctioneer schemes (the latter two schemes are described in the next section).

4 Improvements From Vickrey Auction

In the beginning of this paper, we indicated that the major reasons why Vickrey auc-
tions are not used extensively in the real-world is because of the reluctance of bidders
to reveal their private valuations. Also, the original Vickrey auction fails to describe
how the bids would be encrypted and verified. Our discreet Vickrey auction addresses
each of these shortcomings and introduces ways in which they can be solved. This
section explains the improvements made in our design and how these improvements
help alleviate some of the problems present in the original model.

4.1 Privacy Issues

Corporations have not embraced the Vickrey auction because of fears that their private
valuations of items will be revealed, mainly to the auctioneer. Once these valuations
are revealed to the public or to competitors, it can be utilized to form expectations
about future bids, find out the internal demand of a product, and internal capital in-
vestment strategies. The original Vickrey auction does not ensure that information
flowing over the network will remain private - the auctioneer has the power to open
the bids. If he/she chooses to collude with the participating bidders, private informa-
tion can be revealed. In our discreet Vickrey auction, the information that is revealed
to the auctioneer is reduced to a minimum - he/she only knows the second-highest
bid value. In our design, the SD-envelope containing the second-highest bid value is opened by the auctioneer. It then compares all the encrypted bids (bit-commitment strings) to this value to see whether it is indeed the second highest bid. In this process, the actual value of the bids are not revealed. Also, we recommend that our design should maintain a high level of anonymity by introducing a third-party (key escrow service agency) to hold all the identities of bidders. This will be described in later sections. In these ways, our discreet Vickrey auction is an attractive design that minimizes the amount of private information that is revealed.

4.2 Limiting the Power of the Auctioneer

In the original model, the auctioneer received all the bids, opened them, found out the highest and second highest prices and reported them back to the participating bidders. These procedures were carried out by the auctioneer without the supervision of outside parties. Therefore, an auctioneer could engage in fraudulent behavior such as creating false bids, colluding with the bidders and/or colluding with the seller. Our discreet Vickrey auction protocol significantly reduces such risks. There are several types of schemes that the auctioneer can engage in to make the auction procedure “flawed”.

4.2.1 Bid-revealing Auctioneer

A bid-revealing auctioneer reveals to a colluding bidder the bids that have been submitted so far in the auction process. The bidder can then know the lowest price to win the entire auction (he/she will bid right before the auction ends). After the verification stage, this type of auctioneer can reveal the bidder ID and rankings in terms of price to a colluding bidder. From this extra information, a bidder can increase his/her probability of predicting each bidder’s price for subsequent rounds correctly. Since the auctioneer can enable some bidders to obtain more information than others, the Vickrey auction may be subject to “unfair” pricing. The original Vickrey auction cannot control such fraudulent behavior of the auctioneer because the auctioneer has the power to open all bids as early as the bidding stage. In our discreet Vickrey auction, the auctioneer is unable to open the SD-envelopes until the verification stage. This means that the auctioneer will not know the “current” highest bid during the bidding stage and relay the value back to a colluding bidder. Moreover, the auctioneer only sees the second-highest price. Since he/she is unable to decrypt and “see” any other bid, he/she can relay only limited information to a colluding bidder. This bidder will have a difficult time generating expectations about subsequent rounds due to the lack of information regarding the other competitors. Thus, our discreet Vickrey auction protocol substantially reduces the threat of a bid-revealing auctioneer.

4.2.2 Bidder-Auctioneer

A bidder-auctioneer attempts to increase the price of the item in order to generate more auction fees. This type of auctioneer can be the seller of the auctioned item who hopes
to find the highest possible second highest price. The bidder-auctioneer uses numerous false identities to make various bids. During the winner-determination stage, the auctioneer waits for the highest bid to be called (he/she withdraws any of his/her own bids that exceed the highest price). Soon after, the bidder-auctioneer “raises his/her hand” for one of his/her bids made that is slightly below the highest bid - thereby locking in the highest possible price for the item. The problems with the original Vickrey auction is that it does not address the problem of withdrawing bids. Also, it does not mention how to prevent such behavior. In our discreet Vickrey auction, we have made withdrawals an illegal procedure and any withdrawing bidder is subject to a fine (detailed explanation is in the next section). During the bidding stage, we will also use an Internet bulletin board so that all participating bidders can see the number of bids made and the encrypted bid-commitment values of each bidder. During the verification stage, all bidders can check if their bids and the other competitors’ bids are indeed below the second highest price. If the bidder-auctioneer withdraws several bids that were higher than the second highest price, all other bidders can catch this illegal action and report it to the key escrow service agency that stores the identity and private keys of that fraudulent bidder (detailed explanation in the next section). The auctioneer’s identity will then be revealed. By incorporating these check-mechanisms, we are able to prevent bidder-auctioneers from manipulating the auction.

### 4.2.3 Lying Auctioneer

A lying auctioneer lies during the winner-determination stage that certain bids were placed when in actuality, they were not. The auctioneer can help out a bidder by falsely claiming the highest bid to win the auction, the lowest second-highest bid to minimize the price paid by the highest bidder, or falsely creating the highest second-highest bid to hurt the winner. This problem is controlled in our discreet Vickrey auction protocol because we use an Internet graphic interface for the bidding process. For a bid to exist, it must actually be placed on this interface for the public to see. Also, since each bidder can check if other bids were lower than the second-highest price, he/she can check whether one bid among all the bids was higher than the second-highest bid and it is the same encrypted bid as the one the auctioneer claims is the highest bid (if we are checking to see if the auctioneer has falsely created the highest bid or not). If we are testing whether the auctioneer falsely created the second-highest price, all bidders can compare the encrypted value of the auctioneer’s claimed bid with the encrypted value of the second-highest priced bid on the bulletin board to see if they are identical. If not, we would know the auctioneer was lying. Another way in which an auctioneer can lie is by overstating the second highest bid to increase the seller’s revenue[Br01]. Bidders can check if this is true by comparing the encrypted second-highest bid (taken from the bulletin board) to the now-opened second-highest bid (the claimed value by the auctioneer). If one is different from the other, then he/she would know that the auctioneer is overestimating the second-highest bid. In these ways, our discreet Vickrey auction controls lying auctioneers. The original Vickrey auction has no mechanism of controlling such fraudulent behavior.
4.3 Summary of Improvements

As shown above, our discreet Vickrey auction design has very attractive features for real-world use. It does not reveal private corporate information (by using SD-envelopes and discreet proofs). It also reduces the risk of fraudulent auctioneers by controlling both auctioneer-seller and auctioneer-bidder collusion. The control mechanisms that we have recommended for our design are important because they prevent agents from receiving sensitive information from the auctioneer. Our discreet Vickrey auction prevents the auctioneer from knowing the actual bid values (except for the second highest bid). Our design also enables bidders to confirm that the price the auctioneer tells him/her to pay is really the second highest bid. Also, the bidders are capable of detecting whether the given price is one of the submitted bids. With the use of the bulletin board, the auctioneer is unable to alter existing or add fake bids without detection. Even during the verification stage, the auctioneer can be caught by the participating bidders by procedures described previously. These are remarkable improvements from the original Vickrey auction. Thus, the two risks that have prevented Vickrey auctions from being used in the real-world can be substantially reduced by using our design.

5 Problems With Design and Possible Remedies

While our discreet Vickrey auction design has solved some of the problems with the original Vickrey auction, there are some things still unresolved. In this section, we will attempt to describe several issues related to the current design and how they can be solved.

5.1 Withdrawals From Auction

One major problem that we must address is the possibility of bidders withdrawing after the bidding process. After participants make a bid, they may refuse to “raise their hand” during the winner-determination stage. Moreover, such bidders can simply choose not to give their private keys so that the SD-envelopes are never revealed and compared with other bids. There are incentives for bidders to act in such ways. For the 2nd highest bidder, there are no gains in the auction since he/she does not obtain the item. Without gaining anything, this bidder must reveal his/her private value to the public - a clearly undesirable feature. If the 2nd highest bidder decides to collude with the highest bidder, it can reduce the price paid by the winner by not “raising his/her hand”. Since the winner will pay a price lower than the supposed second-highest price (since it was withdrawn), this scheme will prove to be beneficial for the winner. Thus, there are incentives for the 2nd highest bidder to withdraw before the verification stage. Other bidders also have incentives to withdraw. Consider a bidder that uses multiple user names to make various bids on an item. In essence, he/she “floods” the auction with high, medium, and low bid amounts. If his/her intention is to hurt the highest paying bidder, he/she can wait until a bid is called during the winner-verification stage.
(withdraw any higher bids he/she has made) and “raise his/her hand” for the next-lower bid amount. As shown, all bidders have incentives to withdraw. To prevent such actions, any bidder that withdraws must be punished. We recommend requiring each participating member to deposit money before bidding - if they choose to withdraw, they will not recover this deposit. From studies conducted in game theory, economists and psychologists have noted that participants behave differently when a new option is introduced - that of punishing the co-players [SFN02]. By punishing a bidder that withdraws, there will be better regulation of the protocol and less incentives for bidders to perform fraudulent behavior described previously.

5.2 Anonymity and Encryption Key Storage Issues

As stated above, bidders do have incentives to withdraw. Moreover, some bidders may choose to withdraw despite losing the deposit made before the bidding process. We chose this pre-payment scheme for preventing withdrawals because the protocol was designed to keep bidder identities anonymous. The goal is not to individually identify each bidder who withdraws but to punish them “anonymously”. There are several attractive qualities of keeping bidder identities anonymous. First, anonymity prevents competitors from knowing the internal demand and pricing strategies of a specific corporation. In auctions where the identities are known, agents can keep track of previous bids made by a certain bidder, calculate future expected bid values and change their bids accordingly. Anonymity prevents competitors from matching bids with the bidder, thus reducing the use of game theory applications and time spent calculating the competitors’ expected bid values. As a result, bidders will be more inclined to bid their true valuations. Because of these qualities, anonymity is desired. According to Karl Sigmund, Ernst Fehr and Martin A. Nowak, people do not adopt a purely self-centered viewpoint but take account of their co-player’s outlook [SFN02]. Recent studies have found that real people can be ruled as much by emotion as by cold logic. Studies have suggested that under non-strict anonymity, people expect competitors to notice their decisions and because of that, emotions start to affect the decision-making process. This results in sub-optimal allocation of resources. Strict anonymity will alleviate this problem. Although anonymity has attractive features, it does have some drawbacks. When fraudulent transactions occur (collusion, false bids, etc.), it will be difficult to identify the culprit - an incentive for bidders to engage in such illegal behavior. Also, when the winner fails to pay for the item, he/she cannot be identified. Thus, we must find an optimal level of anonymity that maximizes the attractive features of keeping bidder users anonymous while controlling the incentives for fraud.

There are several scenarios in the e-commerce world regarding privacy of our discreet Vickrey auction - each level provides a different level of anonymity. We will describe each scenario and suggest the optimal one for our design. These various scenarios can be best described by using a tree-format (see figure 2).

In implementing the discreet Vickrey auction, it is vital to set up a system wherein legitimate and secure keys are used for encryption and the identity of the owner is
verifiable in some way (for prevention of fraudulent practices). However, as indicated previously, it is also important to maximize the level of anonymity. Our protocol, which involves the QR-bit commitment scheme, utilizes an integer $N$ - the public key that can be factored into primes $P$ and $Q$ (private). The $N$ is used to encrypt the bid value which is sent over an unsecure network to the auctioneer. As shown on the top of the tree diagram, the first classification is whether or not $N$ is non-certified or certified by an authority that gives its stamp of approval indicating key $N$ is a “good” key.

For non-certified keys, the bidder (i.e. prover) can either prove that the key is a Blum integer using a computationally-expensive proof or give no guarantee that he/she is using a Blum integer. According to [BDP00], a QR-bit commitment scheme assumes the use of a Blum integer $N$ for which the prover knows the factors $P$ and $Q$. Therefore, without a guarantee, this protocol will be prone to attacks and the auction will no longer be “discreet” - an undesired feature. Although the key can be proven to be a Blum integer, the proof has been found to be computationally expensive, especially when each bidder must conduct this proof for every auction round. A detailed description of such proof can be found in the work of Van de Graaf and Peralta [vdGP88]. Therefore, non-certified keys are not optimal choices for our Vickrey auction.

An implementation using certified keys can have the identities of their owners (name, method of payment, value of $N$, etc.) either held anonymously (owner’s identity is not known to the world) or revealed (to either the public or solely to the auctioneer). As mentioned before, we want to maximize the anonymity of the bidders’ identities. Therefore, it will not be an optimal strategy to reveal the owners’ identities to the pub-
lic. However, the design wherein the bidders disclose their identities privately to the auctioneer is not a bad choice since other competitors will be unable to correctly identify each bidder. However, this gives the auctioneer more authority - an undesirable feature that has been cited to be one of the major deterrents of Vickrey auction usage in the real-world. Since one of a major goals in our design is to reduce the auctioneer’s power, we feel that privately disclosing the identities of the bidders to the auctioneer is not optimal. The auctioneer can engage in collusive behavior with other bidders and reveal bidder identities in the process.

Implementations using anonymous keys can be further split into “good Blum integer” or “good key + authority knows owner identity”. In the “good Blum integer” classification, the trusted authority (a government entity or private corporation) will verify that the key being used is a legitimate Blum integer. This is done using an interactive proof since the primes \( P \) and \( Q \) will not be revealed. If the authority figure is well respected and considered trustworthy, the owner can use this Blum integer numerous times for his/her encryption schemes. The authority will not keep track of the identity of the owner or the primes associated with \( N \). Although this may seem like a good implementation, the problem here is that auctioneers cannot identify participants that choose to withdraw or engage in other illegal behavior. A better implementation is when the owner’s identity is kept anonymous from the auctioneer and other bidders, but stored in a trusted authority’s (third-party) database. When a bidder performs a fraudulent act, the auctioneer has the right to request the identity of the bidder. This limits the power of the auctioneer but at the same time prevents frauds from slipping by unnoticed - two desirable features.

This category can be split further into “using key escrow services” and “not using key escrow services”. For our discreet Vickrey auction, we feel that an implementation that uses a good Blum integer and some form of identification of the bidders are desirable features. We believe that these two types of implementations have good qualities that enable us to find a balance between anonymity and fraud prevention. Key escrow systems are systems in which part or all of the secret keys (how to break up \( N \) into \( P \) and \( Q \)) are kept “in escrow” (entrusted to) a third party. Ideally, these keys are released only upon proper authorization to allow someone other than the sender or receiver of a message to “open” it. If a key escrow system is used, not only does it keep track of the identities of the bidders (name, \( N \) value, payment method, etc.), the third party knows how to split the keys and hence knows the method of decoding the message. This has both pros and cons. By giving this third party such authority, it provides a quick mechanism to identify participants engaging in fraudulent behavior. We previously described a fraudulent scheme called “flooding” wherein a fraudulent seller uses multiple user names to flood the auction site with bids. His/her goal is to maximize the price of the item he/she is trying to sell. Until a bidder raises his/her hand, this seller withdraws all his/her high bids. When the highest bid is made, the seller immediately calls the next lower bid. In this scheme, the seller is able to sell the item at the maximum price (slightly below the highest bid). Although the deposit system introduced before will help limit such behavior, some bidders may continue
to perform this if they are confident that their extra payoff received using this scheme will exceed the possible cost of losing the pre-bid deposit. To control such bidders, the auctioneer, upon seeing several withdrawals in one auction round, can use the key escrow service to identify the owners of the keys and decode the encrypted bids (since these bidders may refuse to give out their private keys). If the bids originate from the same owner, the seller may be subject to law infringement. This can be verified since the third party has the identities stored along with the private keys. Also, when the withdrawn bids are opened and they end up being higher than the highest bid, the fraudulent bidder may be forced to pay a fine.

In this way, key escrow services will reduce the incentives of engaging in flooding schemes and other fraudulent practices. However, using these services does introduce privacy issues. As state before, the anonymity of bidder identities is a very desirable quality. Our discreet Vickrey auction protocol will not be commercially attractive unless anonymity is emphasized. Thus, the key escrow service agent must be a trustworthy entity. A suggested method is having a key escrow service agency completely separate from the auctioneer that only gets involved if it has a legitimate reason to believe that people are engaging in illegal activity. In this way, people maintain their privacy, the auctioneer’s powers are reduced, and the third-party can still read messages it believes are important. This assumes that we trust this third-party key escrow service. Although a fraudulent key escrow service agency may lead to improper disclosures of keys and theft of valuable key information, we feel that it will be in their best interests to not reveal private information and maintain trust from the bidders as well as the auctioneer. Although fully functional key recovery infrastructure is said to be an extraordinary complex system, there are working models in parts of Europe and on the web (i.e. i-Escrow.com), indicating that such schemes can be successfully implemented. Another option is not to use key escrow services at all. The authority does not know how to decode the bits. Not using a key escrow service will decrease the probability of private information from being released (by a fraudulent key escrow service agency), but it will increase fraudulent behavior since auctioneers will not be able to open the SD-envelopes if the bidder refuses to give his/her private keys $P$ and $Q$. Without key escrow services, the auctioneer must confront the bidder and force him/her to give up the private keys. Because this may prove to be time consuming, we believe that our design should use certified Blum integers as keys, keep the keys’ owners anonymous to the world, and use a key escrow service to store the bidders’ identities and private keys. Implementing the discreet Vickrey auction under these criteria will help prevent fraud while maintaining a high level of anonymity among the bidders and auctioneer.

### 5.3 Solving Ties

A subtle problem that exists in auctions is how to deal with ties in the highest bid. We must come up with a method of allocating the auctioned item to the highest bidder in a fair way. For two-way ties, we recommend implementing the ’XOR’ method. Both bidders (those that bid the highest prices) will send an encrypted string representing
a bit (0 or 1) to the auctioneer. If the XOR of the two bidders’ bits is 0, one of the bidders wins, and if the XOR is 1, the other bidder wins. For n-way ties, all bidders submit a value ranging from 0 to n. The auctioneer will do the following computation: $\sum_{i=1}^{n} V_i \pmod{n}$ where $V_i$ is the value submitted by bidder $i$. This scheme provides fair allocation of the item to one of the highest bidders when ties occur.

5.4 Anti-social Agents

A recent paper by Felix Brandt and Gerhard Weiβ has indicated that Vickrey auctions are vulnerable to antisocial agents whose main goal is to reduce the profit of competitors rather than maximizing their own profits [Bra97]. Brandt and Weiβ have shown that such agents deviate from the truth-telling strategy and choose not to bid their true valuations. Anti-social agents define success by the amount competitors “lose” in the auction. One scheme in which such agents can engage in predatory behavior is in auctions where identical items are sold in multiple rounds. In the first round, the anti-social agent loses and remembers the second-highest bid (the price that is revealed). Then, he/she bids a very high price in the subsequent round and remembers the second-highest bid (which is in effect the highest bid). In the next round, this agent will bid halfway between the two values revealed in the previous two rounds. Although the agent loses the difference between both values once, he/she can safely cut off 50% of the competitor’s profit for all following rounds. Brandt and Weiβ claims that if there are many subsequent rounds, this investment will pay off [Bra97]. Although this problem is not addressed in our design, we believe that it will not be a big threat. First, if there is more than one anti-social agent in the auction, these agents will end up losing money once without harming anyone in subsequent rounds. If the auctioneer sees a jump in the price of the item, then he/she should see if there are anti-social agents within the auction. Because of this, anti-social agents may not choose to behave in such ways. Second, since the bid values are anonymous and kept secret for our discreet Vickrey auction protocol, when internal demands change (depending on market conditions and the overall economy), these agents must perform this scheme again and lose money in the process. Thus, it seems that maladaptive behavior by anti-social agents can be controlled. However, it is important that more research is done concerning anti-social agents and possible prevention measures for their fraudulent practices.

6 Possible Real-world Applications

Our Vickrey auction protocol can be used for various real-world applications. For example, this type of auction can be used to allocate network bandwidth among ISPs and/or network carriers from the Federal Communications Commission (FCC) wherein several rounds of auctions for homogenous goods are conducted or for the mergers and acquisitions (M&A) market where bids must be made privately and anonymously during the bidding phase to prevent market reactions to the news. The U.S. Treasury Department is currently experimenting with a type of Vickrey auction
to sell the national debt and the former Czechoslovakia has used it to refinance credit [Rey96]. Since our discreet Vickrey auction minimizes the amount of private information that is revealed, it is an attractive protocol for transactions that require high levels of secrecy.

Our discreet Vickrey auction can also be used for task assignment scenarios. In such scenarios, bidders who are willing to perform a certain task makes a bid expressing the amount he/she wants to be paid for task execution [Bra97]. The winner of this auction scheme is the bidder who bids the lowest price. He/she will end up receiving the second-lowest bid for completing the task. This reverse Vickrey auction scheme can be used in the investment banking industry to decide the investment banks who underwrite an initial public offering (during this offering, a company’s stock is sold on the stock exchanges for the first time). Since the initial public offering (IPO) procedure is similar for most investment banks, companies who want their securities to be underwritten can minimize the amount of fees paid by using this task assignment scenario. Although the reverse Vickrey auction may introduce a new set of problems, it is recommended that further research be conducted to find possible uses for it. As shown, our design of the Vickrey auction can be used in the real-world for the optimal allocation of resources. The future looks promising for this type of auctioning scheme.

7 Concluding Remarks

In this paper, we have introduced a particular design of the Vickrey auction that minimizes the release of private information, maintains a high level of anonymity, and limits the power of the auctioneer. Since it uses the original Vickrey auction as the basis of its design, it retains its attractive features. We believe that our bit-commitment scheme using SD-envelopes and discreet proofs will enable bidders to make bids without revealing private valuations. The scheme significantly reduces potential collusive threats by the auctioneer, the bidders, and/or the seller. As the Internet grows and more users embrace e-Commerce, it has become increasingly important to create an auction protocol that reduces fraud. Our discreet Vickrey auction not only reduces fraud, but maintains the property that bidders bid their true valuations. There are numerous attractive features about our design that are not found in other types of auctions or the original Vickrey auction. As indicated before, the future of our discreet Vickrey auction protocol is extremely promising and we hope that corporations and individuals will utilize this scheme when auctioning their assets.
References


