R U T C O R
R ESEARCH
R E P O R T

PROTOCOL COMPLETION INCENTIVE PROBLEMS IN CRYPTOGRAPHIC VICKREY AUCTIONS

Phillip G. Bradford[a] Sunju Park[b]
Michael H. Rothkopf[c]

RRR 3-2004, FEBRUARY, 2004

RUTCOR
Rutgers Center for
Operations Research
Rutgers University
640 Bartholomew Road
Piscataway, New Jersey
08854-8003
Telephone: 732-445-3804
Telefax: 732-445-5472
Email: rrr@rutcor.rutgers.edu
http://rutcor.rutgers.edu/~rrr

[a] Department of Computer Science, The University of Alabama, Tuscaloosa, AL 35487
[b] Management Science and Information Systems Department, Rutgers Business School, Rutgers University, Newark NJ 07102
[c] Rutgers Center for Operation Research, Rutgers Business School, 640 Bartholomew Road, Piscataway NJ 08854.

RUTCOR RESEARCH REPORT
RRR 3-2004, FEBRUARY, 2004

PROTOCOL COMPLETION INCENTIVE PROBLEMS IN CRYPTOGRAPHIC VICKREY AUCTIONS

Phillip G. Bradford Sunju Park Michael H. Rothkopf

Abstract. In spite of attractive theoretical properties, Vickrey auctions are seldom actually used due to information revelation and fear of cheating. Cryptographic Vickrey Auctions (CVAs) have been proposed to protect bidders' privacy or to prevent the bid taker from cheating. This paper has three parts. First, it identifies ideal goals for CVAs. One of the criteria identifies an incentive problem that is new to the literature on cryptographic Vickrey auctions: the disincentive of a bidder who has learned that she has lost the auction to complete the protocol. Any auction protocol that requires losing bidders to do additional work after learning they have lost needs to provide the losers with proper incentives to follow the protocol. Second, it shows that in a class of CVAs, some losers must continue to participate. Finally, it describes a new CVA protocol that solves the protocol-completion incentive problem. A proper treatment of incentives using cryptography, however, may make the auction too complicated for practical use. One possible alternative is the use of bonds as a way of providing an incentive to losers.

Acknowledgements: The second author is partially funded by Rutgers Research Council Grant.

1 Introduction

Designing "good" mechanisms is a fundamental research issue in auction theory. Goodness can involve a variety of criteria, including economic efficiency, security, privacy, revenue maximization, fairness, *etc*. Practical auction design may involve tradeoffs between such criteria.

Sealed second-price auctions, called Vickrey auctions after the Nobel-Prize-winning economist who first analyzed them (Vickrey, 1961), have some attractive theoretical properties, but they are seldom used. Rothkopf, *et al*. (1990) pointed out that information revelation and fear of cheating by the bid taker contribute to the rarity of Vickrey auctions. Rothkopf and Harstad (1995) modeled the concern with cheating by the bid taker and Lucking-Reiley (2000) confirmed its existence in practice. In addition, Robinson (1985) gave insight into the potential problem of collusion by bidders in Vickrey auctions. In response to the concerns raised in Rothkopf, *et al*. (1990), Nurmi and Salomaa (1993) proposed the use of cryptography to protect bidders' privacy. Since then, there have been a number of additional proposals for cryptographic Vickrey auction protocols (Franklin and Reiter 1996, Kikuchi, *et al.* 1999, Cachin 1999, Naor, *et al*. 1999, Jakobsson and Juels 2000, Abe and Suzuki 2002, and Brandt 2002, 2003).

This paper begins with a discussion of ideal goals for cryptographic Vickrey auctions (CVAs). One of the criteria it considers is new to the literature on CVAs: the incentive of bidders who have learned that they have lost the auction to complete the protocol. The paper then proves this incentive problem is unavoidable in a class of CVAs. Finally, this paper gives a new CVA protocol that solves the incentive problem.

2 Related Work

Vickrey auctions have some nice properties under certain critical assumptions (Vickrey 1961). It is well known that under these assumptions revealing one's true valuation is the dominant strategy in Vickrey auctions. Moreover, the resulting allocation is Pareto optimal and perfectly efficient. That is, no other allocation will lead to a situation that is preferred by all to the allocation of the Vickrey auction and no other allocation can create more total value. Despite nice theoretical properties, however, Vickrey auctions have been rarely used in practice. Rothkopf, et al. (1990) explain two key reasons Vickrey auctions are not as popular as one might expect. First, bidders may have reason to fear the disclosure of their bids. Second, a cheating auctioneer may artificially inflate the price-setting bid for the seller's advantage (or deflate the price-setting bid for the winning bidder).

Many have proposed cryptographic versions of Vickrey auctions to overcome these two obstacles. Nurmi and Salomma (1993) prevent artificial bid inflation by posting all encrypted bids in public before the auction starts and then making bids public (but not necessarily who made them) after the close of the bidding. To allow pairs of bidders themselves to determine which of their bids is larger (without revealing the bids), they further discuss a protocol based on Yao's "Millionaire Problem" (1982).

To prevent the auctioneer from cheating, Franklin and Reiter (1996) used distributed auctioneers with encryption so that without consent among at least a third of them, there could

not be any price inflation. Their basic system releases all bids after the close of bidding, though they briefly discuss keeping bidders secret and concealing bids permanently. Their system is robust against malicious bidders and up to one-third of dishonest auctioneers. The threshold-trust model has been studied by many others (Schneier 1996).

To minimize information revelation, on the other hand, Brandt proposes a mechanism that gives full privacy to losing agents (Brandt 2002, 2003). Jakobsson and Juels (2000) use Yao's Millionaire Problem as well as mix-nets. While they never discuss this issue of the incentives for losing bidders to complete the protocol, Brandt (2002, 2003) and Jakobsson and Juels (2000) both provide full privacy, thereby implicitly avoiding the incentive problem. In both cases, this is done by having the bidders give their encrypted bids to some or all of the other bidders. Brandt, Jakobson and Juels, as well as with Abe and Suzuki (2002), work directly with the binary representations of the bids.

Naor, Pinkas, and Sumner (1999) propose a mechanism that utilizes the third party. Their mechanism separates the third party into the auctioneer and the auction-issuer. The auction-issuer sends a program to the auctioneer for securely computing the winning bidder(s). If the auctioneer and the auction-issuer do not collude, then this protocol does not reveal the bids and the associated bidders.

Mutual verifiability, which allows bidders to verify the relationships of each other's bids, removes the need for assuming a `trusted' third party (Pedersen 1991). Brandt uses a number of tools including mutual verifiable secret sharing schemes and homomorphic encryption (2002,2003). He shows after the close of bidding in a (M+1) general Vickrey auction, only the winning bidder knows the (M+1)-st highest bid. The other bids are never revealed. Abe and Suzuki (2002) assume a trusted party, but Brandt does not.

Many different cryptographic techniques are used in designing cryptographic auctions. Homomorphic encryption, which plays an important role in electronic voting, has been applied to generalized Vickrey auctions. For example, Abe and Suzuki (2002) apply homomorphism encryption to ensure bidding secrecy. After the close of bids, public verifiability is performed by publicly opening the bids. While this approach will help limit cheating, it suffers from the revelation of sensitive information.

A bidder may illicitly make false-name bids. These are bids in another's name to improperly influence an auction. Wang, Hidvegi and Whinston (2001-2002) investigate protocols for variations on sealed-bid auctions for multi-unit identical items. Their protocol uses economic utility to discourage bidders from exploiting security weaknesses. Our paper does not deal with the control of the identities of bidders.

Along with the cost of protocols, one must consider trust establishment and the verifiability of auction systems. More precisely, even for a protocol that is deemed secure, how good is its implementation? Protocol failures are discussed by Simmons (Simmons 1994). How easy is it to verify the fairness of an auction protocol? It would seem the more sophisticated and innovative a cryptographic-bidding protocol, the more participants assume risk.

3 Evaluation Criteria for Cryptographic Vickrey Auctions

Auctions are only one way of conducting business. In addition to the revenue they can expect to receive, a number of concerns may motivate people to choose a procedure for conducting business. These include the actual and perceived fairness of the results, the efficiency of allocating what is being sold to the party valuing it most highly, the low costs of the procedure, the resistance to cheating, and the ability to keep secret the private valuations of the participants. In the context of a cryptographic Vickrey auction, these translate into the following specific goals:

1. Winning bidders should know that they have won and that there was a bid (the second highest bid) made at the level setting the price. It is also probably necessary that the identity of the bidder making the price-setting bid be revealed to the winner. This allows winning bidders to be confident that the price they are being asked to pay is being determined fairly.
2. Every losing bidder should know that another bidder made a higher bid. This allows losing bidders to be confident that they should, in fact, have lost.
3. The seller should know the amount of the second highest bid, that the winner made a higher bid, and that all other bids are lower. This allows the seller to be confident that the correct winner and price have been determined. It may be desirable as well for the seller to receive some additional information on the bids. First, the identity of the winning bidder may need to be revealed to complete the transaction and to allow the seller to assure the winner's eligibility to win. Secondly, the commercial value to the seller of additional information on losing bids may exceed the cost of revelation of the information to the losing bidders, especially if the identity of the losing bidders is not revealed to the seller.
4. Aside from the information discussed in goals 1, 2, and 3, no other information should be revealed at the conclusion of the auction. This secrecy serves several purposes. First, it protects private information of the bidders that is potentially commercially sensitive. (See Rothkopf et al. 1990, Englebrecht-Wiggans and Kahn 1991). Second, it keeps secret information that might be of use to potential cheaters—a seller who wants to insert a fictitious bid and bidders who wish to collude.
5. The costs of the auction should be as small as possible. This includes bid preparation costs, communication costs, the costs of winner determination, and the costs, if any, of performance bonds by the bidders.
6. The auction should only rely on bidders acting in their own self interest. In particular, no reliance should be placed on actions to complete a protocol by bidders who have learned that they cannot win the auction and who may have nothing to lose by failing to complete it. While cryptographic Vickrey auction protocols have been proposed for supporting the honesty of the auctioneer and the privacy of bids, no one has addressed providing proper incentives for losing agents to follow the auction protocol to the end. This can be a critical issue, as cryptographic auction protocols often require additional work by losing agents. Without proper incentives, the losers may have no reason to continue the protocol and ensure that the auction process works.

4 Sometimes Losers Must Do Additional Work

Let us use the term atomic-revelation auction model to describe auction models where the outcome of each comparison is known immediately. In the following, we review Nurmi and Salomaa's protocol (1993), an example of the atomic-revelation model. Then, we demonstrate the existence of an incentive problem in the atomic-revelation CVAs, by proving that some losers may need to continue to participate in the auction after they learn they have lost.

4.1 Nurmi and Salomaa's Protocol Revisited

This section examines the existing auction protocol by Nurmi and Salomaa (1993). Nurmi and Salomaa (N&S) focus on two issues when they apply cryptography to Vickrey auctions: (1) preventing the inflation (or deflation) of the price-setting bid, and (2) minimizing the revelation of bidders' private information. (They also discuss the use of classic public key encryption to support secure transmission of bids, but since this way of using cryptography is accepted and widely used in practice, we do not discuss it in this paper.)

To prevent the auctioneer from changing the price-setting bid, N&S propose the following straightforward application of cryptography. The auctioneer posts for public view all the bids, each encrypted with the bidder's public key. Once the bidding period terminates, the auctioneer receives from bidders their private keys and makes them public. Then, anyone (all the bidders and the seller) can verify the price-setting bid. This protocol, however, exposes *all* the bids placed in the auction. The identities of bidders need not be exposed with their private keys (as long as the auctioneer publishes the private keys while keeping the identity of the bidder to herself), but the fear of exposing bidders' true valuations may deter them from participating in the auction in the first place. Therefore, it is desirable to have a protocol that reveals as few bids as possible.

In order to minimize the number of bids that are to be known, N&S utilize the millionaire protocol (Yao 1982). Consider two bidders, A and B. Let *A*'s bid be *Abid* and *B*'s bid be *Bbid*, and without loss of generality, let *Abid* and *Bbid* $\in \{1, \ldots, 100\}$. The following protocol determines whether $Abid \leq Bbid$ or $Abid \geq Bbid$ while revealing only the value of the losing bid. We write E_A to denote encrypting with A's *public* key. Likewise, we write D_A to mean decrypting with A's *private* key. We use E_C to represent the bid-taker's public encryption key.

The protection from bidders' collusion is provided by the bid-taker who is able to recover the value of the losing bid in Step 6. The protocol can also be made to ensure that the losing bidder does not inflate the bid price, by forcing the losing bidder to inform the winner of the critical encryption information needed to recover her bid. If *B* is the losing bidder, she informs *A* of B_{bid} and *x*. Then, *A* can check that *B* is not inflating the price of the good. If *A* is the loser, she informs *B* about *y* sequence, and then *B* can check the correctness of the result reached.

This protocol can be used multiple times to solve the case with multiple bidders. A straightforward application requires *n(n-1)/2* pairwise comparisons, and Nurmi and Salomaa show a way of using rounds to conduct Vickrey auctions with *(2n-2)* comparisons while not revealing the highest bid. Note that during pairwise comparisons, only the order of bids (not the values) is known. Even when the loser is required to reveal additional information to prevent bid

inflation, only the losing bid is revealed. Therefore, the protocol ensures that bidders may know only some subset of bids, the losing bids they encountered.

Step 1: B privately chooses a large random number x and computes $k = E_A(x)$.
Both A and B send to the bid-taker their bids in the following form:
$E_C(E_A(A_{bid} S_A)), E_C(E_A(S_A))$ and $E_C(E_B(B_{bid} S_B)), E_C(E_B(S_B))$, respectively.
S_A (S_B) represents a random number privately chosen by A (B).

Step 2: B sends A the value $(k - B_{bid})$.

Step 3: A privately computes $y_i \leftarrow D_A(k - B_{bid} + i)$ for all $i \in \{1,...,100\}$.
A secretly finds a prime $p < x$ such that
$z_i \leftarrow y_i \bmod p$ for all $i \in \{1,...,100\}$,
$z_i < p - 1$ for $i, j \in \{1,...,100\}$, and
$|z_i - z_j| \geq 2$ for all $i \neq j$.

Step 4: A sends the following sequence to B.
$z_1, ..., z_{A_{bid}}, z_{A_{bid}+1} + 1, z_{A_{bid}+2} + 1, ..., z_{100} + 1, p$.

Step 5: B determines the following.
If $z_{B_{bid}} = x \bmod p$, then $B_{bid} \leq A_{bid}$
If $z_{B_{bid}} \neq x \bmod p$, then $B_{bid} > A_{bid}$

Step 6: B informs A about her conclusion in Step 5. The losing bidder sends her decryption key to the bid-taker. The bid-taker recovers the loser's bid (see Step 1), and thus the price to charge the winner.

Figure 1: N&S Application of Yao's Protocol (summarizing Nurmi & Salomaa 1993).

4.2 Proof that Sometimes Losers Must Do Additional Work

Requiring losing bidders to do extra work once they learn they have lost may be a serious incentive problem. We show why this is unavoidable in the atomic-revelation auctions that use pairwise comparisons (such as N&S in Figure 1), and argue that bonding may be necessary to support the proper execution of CVAs.

The result of the next lemma uses the standard proof that the lower bound of selecting the second largest element requires $n + \lceil \log_2 n \rceil - 2$, comparisons in the worst case (Knuth 1973, Aigner 1988). This is applicable for the atomic revelation model. Here, we show the $n + \lceil \log_2 n \rceil - 2$ lower bound implies $\lceil \log_2 n \rceil - 1$ bidders lose two times.

Lemma 1. When selecting the second best bid using pairwise ≤ comparisons, ($\lceil \log_2 n \rceil - 1$) bidders must lose at least twice.

Proof. Suppose n ≥ 2. Assume there exist no ties among *n* bids. Using the pairwise comparison, the most efficient algorithm can select the second largest bid in $n+\lceil \log_2 n \rceil - 2$ comparisons in the worst case (Aigner 1988).

The following are known facts about pairwise comparisons. Each pairwise comparison between any two bidders gives one win and one loss (Fact 1). The same comparisons never need to be repeated (Fact 2). The highest bidder never loses, and the second highest bidder loses only once (Fact 3). In selecting the second largest bid, it makes no sense for an algorithm to have a bidder lose three or more times, since a bidder that has lost twice cannot have the second largest bid (Fact 4). From Fact 3 and Fact 4, it is clear that any bidder can lose at most two times in any optimal algorithm. To find the second highest bid, every bidder must participate in at least one comparison (Fact 5).

As $n+\lceil \log_2 n \rceil - 2$ comparisons result in one loss each, there should be a total of $n+\lceil \log_2 n \rceil - 2$ losses. Excluding the highest bidder who never loses and the second highest bidder who loses only once, the remaining $n-2$ bidders should account for the $n+\lceil \log_2 n \rceil - 3$ losses, which is the total number of losses minus 1 (for excluding the second highest bidder's loss). From Fact 5 and from the fact that they are not the winner or the second highest bidder, (n – 2) bidders must lose at least once. The remaining losses, (i.e., $(n+\lceil \log_2 n \rceil - 3) - (n-2)$), should be attributed to them as well. Since a bidder cannot lose more than twice, at least ($\lceil \log_2 n \rceil - 1$) bidders must lose two times in the worst case. □

When the above lemma is applied to the atomic-revelation auction model where the outcome of each comparison is known immediately after the comparison is performed, we have the following result.

Corollary 1. Using ≤ comparisons in the atomic-revelation model, any auction protocol for three or more bidders must depend on losing bidders to complete the Vickrey auction.

When n=2, a single comparison is all that is needed, and therefore no bidder loses twice. This is consistent with Lemma 1 (i.e., $\lceil \log_2 2 \rceil - 1 = 0$). When n=3, two bidders engage in a pairwise comparison. The winner of the two then performs a pairwise comparison with the third bidder. If the third bidder is the winner of the two, then the order of bids is known and no other comparison is necessary. However, if the winner of the first comparison is also the winner of the second comparison, an additional comparison between two losers is needed to find out who is the second highest. So, in the worst case, losers need to participate in the auction after they learn they have lost. Similar examples can be construed for n > 3 cases. That is, when n ≥ 3, there always exists a case in which one or more bidders who need to lose at least[1] twice.

In the atomic-revelation CVA with pairwise comparisons, therefore, the auctioneer may need to impose bonds on bidders such that if they do not follow the pre-agreed protocol to the end, they will forfeit the bonds. Imposing bonds to auction participants is an additional burden that may well be reflected in their willingness to participate in the auction. Without bonding, however, there is no guarantee of the proper execution of the atomic-revelation cryptographic

1 "At least" because the bidders can lose more than twice if a less-efficient algorithm is used.

Vickrey auctions where the bid comparisons are known to the bidders immediately after the comparisons are made.

5 Solving the Loser's Incentive Problem in CVAs

An obvious way of introducing proper incentives is not to reveal the loser during pairwise comparisons. By deferring the revelation of comparison results, the protocol does not let the losing bidders know whether they are the losers and therefore forces them to continue to participate in the auction. We define the deferred-revelation auction model as the model where the comparison results are not revealed immediately. In this section, we give a deferred-revelation CVA that solves the incentive problem.

One way of achieving deferred-revelation is to modify N&S's application of Yao's protocol by introducing the bit-commitment scheme. In the modified protocol, all participants bit-commit a private bit determining the outcome of the comparison. Figure 2 shows the modification of Steps 4 through 6 of N&S's application of Yao's protocol presented in Figure 1. Step 4 changes so bidder *A* cryptographically commits her random choice of *X* using a bit-commitment scheme. Likewise, in Step 6, *B* cryptographically commits her determination of whether or not to let the result of $z_{B_{bid}} = x \bmod p$ is presented correctly. *Y* denotes this commitment. If *Y* = 0 then *B* posts the correct value of $z_{B_{bid}}$, otherwise, *B* posts the opposite value of $z_{B_{bid}}$.

The objective of the new protocol is to let neither *A* nor *B* have the power of knowing the correct outcome of the auction until all the pairwise comparisons are made. In step 4, A sends the sequence same as in the original protocol if *X* is 0, or the opposite if *X* is 1. By doing so, *A* prevents *B* from knowing who is the winner in Step 5 without knowing the value of *X*. Similarly, *B* does not want to tell *A* the correct outcome of Step 5 (as the honest revelation will let *A* figure out the winner). Instead, *B* randomly selects *Y* in Step 6, and posts the correct outcome if *Y* = 0, or the opposite if *Y* = 1. By doing so, *B* prevents *A* from knowing who's the winner without the value of *Y*.

Step 0 ~ Step 3: (Same as Figure 1.)

Step 4: A secretly chooses $X \in \{0,1\}$, then A bit-commits X and sends the following sequence to B.

$$z_1 + C_1, ..., z_{A_{bid}} + C_{A_{bid}}, z_{A_{bid}+1} + \overline{C_{A_{bid}+1}}, ..., z_{100} + \overline{C_{100}}, p$$

where $C_i = X$ and $\overline{C_i} = 1 - C_i$ for all $i \in \{1,...,100\}$

Step 5: B computes the following and determines the value Z such that:

Z = 0 if $z_{B_{bid}} = x \bmod p$. (If $X = 0$ then $B_{bid} \le A_{bid}$ else $B_{bid} > A_{bid}$.)

Z = 1 if $z_{B_{bid}} \neq x \bmod p$. (If $X = 0$ then $B_{bid} > A_{bid}$ else $B_{bid} \le A_{bid}$.)

Step 6: B randomly selects $Y \in \{0,1\}$, and bit-commits Y. If Y = 0, post the nominal value Z. If Y = 1, post the opposite of the value Z.

Figure 2: Basic Modification of N&S 's Application of Yao's Protocol.

When there are two bidders, *A* and *B* reveal the values of *X* and *Y*, respectively, after Step 6. If one of them has changed the value of her computational result, the correct outcome is the *opposite* of what was reported. That is, if Z=0 was reported, then accept Z=1; if Z=1 was reported, then accept Z=0. If both of them have reported the correct results or both of them have reported the opposites, the outcome reported by our modification of Yao's protocol is the correct outcome.

For the auction with multiple bidders, the protocol can be extended such that the value of Xs and Ys of all comparisons will be revealed after *all* of these comparisons are made between all bidders. No player will drop out of participation, as long as they are interested in winning. Using this, the auction can find the highest and second highest bids in a single round.

The new protocol thus solves the incentive problem (using bit-commitment) while minimizing the information revelation (using Yao's protocol). Jakobsson and Juels (2000) proposed a "mix and match" cryptography and applied it to sealed-bid auctions.[2] Under their auction protocol, the "servers," who do not have incentives to drop out of participation, receive the encrypted bids from bidders and engage in pairwise comparisons in a tennis-tournament format. By letting "servers" follow the protocol, J&J *implicitly* avoid the incentive problem.

6 Discussion

This paper makes three contributions. First, it identifies desiderata for designing and analyzing cryptographic Vickrey auctions. Second, it proves that atomic-revelation CVAs with pairwise comparisons requires losers do additional work. Finally, it provides a new cryptographic Vickrey auction protocol that solves this incentive problem.

A potential problem with using the new protocol in practice is the number of comparisons needed. As the results of comparisons are not revealed until all pairwise comparisons are done, the new protocol cannot use the efficient algorithm for finding the second highest element (which takes advantage of previous comparison results to minimize the number of comparisons). Therefore, the new protocol requires $n(n-1)/2$ comparisons.

Using more than a single round can reduce the total number of comparisons required, however. The idea is to perform comparisons in rounds by dividing the bidders into groups (Bollobas 2001, page 426, Gasarch, Golub, and Kruskal 2000). In each round, comparisons are performed between the members of each group with no one knowing their outcomes until after all the comparisons are made. After a round is completed, the outcomes of the comparisons are revealed to everyone within the group. Then, the two highest bidders in each group advance to the next round for additional comparisons, and so on. Note that, however, a direct application of our protocol would face the incentive problem again. If the bidder with the second highest bid knows that she is the second highest in the group, she loses her incentive to participate in the second round. To avoid this loss of incentive, therefore, the auction must select the two highest bids from each group without revealing who is the winner. We are currently investigating a multi-round CVA that minimizes the number of comparisons while avoiding the protocol-completion incentive problem.

[2] They described a model for first-price sealed bid auctions, but noted that Vickrey auctions may be achieved through simple modifications.

The present study shows there exist tradeoffs. A practical CVA protocol may suffer an incentive problem. On the other hand, a proper treatment of the incentive problem using cryptography may become too complex to be practical. The use of performance bonds may be desirable to provide an incentive for losers to participate after the auction reveals the winner. How large should the bonds be? Should they be set relative to the cost of completing the protocol, the value of the information revealed, or the damage to the process that noncompliance would cause? We conjecture that some combination of these along with other incentives the losing bidders may already have will determine the appropriate amount of bonds.

7 References

M. Abe and K. Suzuki: "M+1-st price auction using homomorphic encryption," *In the Proceedings of the 5th International Workshop on the Practice and Theory of Public Key Cryptosystems (PKC 2002),* Volume # 2274 of LNCS, pages 115-224, Springer Verlag, 2002.

M. Aigner: *Combinatorial Search*, Wiley-Teubner, 1988.

M. Blum: "Coin flipping by telephone," *IEEE Spring COMPCOM*, 133-137, Feb. 1982.

B. Bollobas: *Random Graphs*, second edition, Cambridge University Press, 2001.

F. Brandt: "A Verifiable, Bidder-Resolved Auction Protocol," *In Proceedings of First International Joint Conference on Autonomous Agents and Multi-Agent Systems (AAMAS 2002),* R. Falcone, S. Barber, L. Korba, M. Singh (eds.), pages 18-25, 2002.

F. Brandt:``Fully Private Auctions in a Constant Number of Rounds," *In the Proceedings of Financial Cryptography (FC 2003)*, pages 223-238, 2003.

M. K. Franklin and M. K. Reiter: "The Design and Implementation of a Secure Auction Service," *IEEE Transactions on Software Engineering*, Vol. **22**, No. 5, pages 302-312, 1996.

W. I. Gasarch, E. Golub, C. P. Kruskal: "A Survey of Constant Time Parallel Sorting," *Bulletin of the EATCS (European Association of Theoretical Computer Science)* **72**: pages 84-102, 2000.

B. Horne, B. Pinkas and T. Sander: "Escrow Services and Incentives in Peer-to-Peer Networks," *In Proceedings of the ACM Conference on Electronic Commerce EC'01,* pages 85-94, Oct. 2001.

M. Jakobsson and A. Juels: ``Mix and Match: Secure Function Evaluation via Ciphertexts," In T. Okamoto (ed.), *Advances in Cryptography - ASIACRYPT '00,* pages 162-177, LNCS# 1976, 2000.

H. Kikuchi, M. Harkavy, J. D. Tygar: "Multi-round Anonymous Auction Protocols," TIEICE: *IEICE Transactions on Communications/Electronics/Information and Systems, pages 62-69,* 1999.

D. E. Knuth. *Sorting and Searching*, Volume 3. Addison-Wesley, Reading, MA, 1973.

M. Naor, B. Pinkas, R. Sumner: "Privacy Preserving Auctions and Mechanism Design," In 1st *ACM Conf. on Electronic Commerce*, pages 129-139. ACM, 1999.

T. Pedersen: "A threshold cryptosystem without a trusted party (extended abstract)," *In Advances in cryptology--EUROCRYPT '91: Workshop on the Theory and Application of Cryptographic Techniques,* Springer-Verlag, LNCS #547, 522-526, 1991.

D. Lucking-Reiley, "Vickrey Auctions in Practice: From Nineteenth-Century Philately to Twenty-First-Century E-Commerce." *Journal of Economic Perspectives*, vol. **14**, no. 3, pages 183-192, 2000.

A. Salomaa: *Public-Key Cryptography,* Springer-Verlag, 1990.

B. Schneier: *Applied Cryptography,* Second Edition*,* John Wiley & Sons, 1996.

G. J. Simmons 94: ``Cryptanalysis and Protocol Failures," *Communications of the ACM*, Vol. **37**, No. 11, pages 56-65, November 1994.

W. Vickrey: "Counterspeculation, Auctions, and Competitive Sealed Tenders," *Journal of Finance,* Vol. **16**, pages 8-37, 1961.

W. Wang, Z. Hidvegi and A. B. Whinston: "Designing Mechanisms for E-Commerce Security: An Example from Sealed-Bid Auctions," *International Journal of Electronic Commerce*, Vol. 6, No. 2, pages 113-130 , Winter 2001-2002.