$M + 1$-st Price Auction Using Homomorphic Encryption

Masayuki Abe and Koutarou Suzuki

NTT Information Sharing Platform Laboratories
1-1 Hikari-no-oka, Yokosuka, Kanagawa, 239-0847 Japan
{abe,koutarou}@isl.ntt.co.jp

Abstract. This paper provides a $M + 1$-st price auction scheme using homomorphic encryption and the mix and match technique; it offers secrecy of bidding price and public verifiability. Our scheme has low round communication complexity: 1 round from each bidder to auctioneer in bidding and $\log p$ rounds from auctioneer to trusted authority in opening when prices are selected from p prefixed choices.

1 Introduction

The $M + 1$-st price auction is a type of sealed-bid auction for selling M units of a single kind of goods, and is famous as the Vickrey auction in the case of $M = 1$. In this auction, the $M + 1$-st (highest) price is the winning price, M bidders who bid higher prices than the winning price are winning bidders, and each winning bidder buys one unit of the goods at the $M + 1$-st winning price. The $M + 1$-st price auction is celebrated in economics or game theory for having *incentive compatibility*, that is, the *dominant strategy* (optimal strategy) for each bidder is to bid honestly his own true value [Vic61]. Because the true value is assumed to be issued, keeping the bidding prices secret is more significant than is true in the usual highest price auction, where most bidding prices are not the bidder's honest price.

This paper proposes an $M+1$-st price auction that enjoys auction secrecy and public verifiability; it uses a homomorphic encryption and the mix and match technique from [JJ00]. Our scheme has low round communication complexity: 1 round from each bidder to one auctioneer in bidding and $\log p$ rounds from the auctioneer to trusted authority in opening, where p is the number of prices. The usual M-th highest price auction scheme can be created with slight modification.

In contrast to the many papers on first price sealed-bid auctions, as shown in Section 1.1, there are few papers on $M+1$-st price auctions. Harkavy, Tygar and Kikuchi proposed a Vickrey auction, where the bidding price is represented by polynomials that are shared by auctioneers [HTK98]. In their scheme, each bidder must communicate with plural auctioneers to bid. Naor, Pinkas and Sumner realized sealed-bid auctions by combining Yao's secure computation with oblivious transfer [NPS99]. Their scheme can compute any circuit, and so can realize various types of auctions, e.g., $M + 1$-st price auction. Though their scheme is

D. Naccache and P. Paillier (Eds.): PKC 2002, LNCS 2274, pp. 115–124, 2002.

versatile and efficient, the cut-and-choose technique is needed to achieve verifiability, so the atomic protocol must be executed k times, where k is the security parameter of cut-and-choose, and each bidder must communicate with not only the auctioneer but also the auction issuer to bid. Kikuchi proposed an $M+1$-st price auction, where the bidding price is represented by the degree of a polynomial shared by auctioneers [Kik01]. In his scheme, a large number of auctioneers is required (the number of auctioneers must be more than the number p of prices), and each bidder must communicate with these auctioneers not only to bid but also to determine the winning price and bidders.

In comparison to these schemes, our scheme has only one auctioneer and much simpler communication: each bidder sends his bid to just the auctioneer to bid and the auctioneer communicates with the trusted authority using $\log p$ rounds to open the bids. Thus our scheme is easy to implement.

Section 2 explains the $M+1$-st price auction and requirements. In section 3, we introduce our $M+1$-st price auction and discuss its security and efficiency. Section 4 concludes the paper.

1.1 Related Work

There are many papers on first price sealed-bid auctions, but few on $M+1$-st price auctions. Kikuchi, Harkavy and Tygar presented an anonymous sealed-bid auction that uses an encrypted vector to represent bidding price [KHT98]. Kudo used a time server to realize sealed-bid auctions [Kud98]. Cachin proposed a sealed-bid auction using homomorphic encryption and an oblivious third party [Cac99]; its complexity is a polynomial of the logarithm of the number of possible prices. Sakurai and Miyazaki proposed a sealed-bid auction in which a bid is represented by the bidder's undeniable signature of his bidding price [SM99]. Sako proposed a sealed-bid auction in which a bid is represented by an encrypted message with a public key that corresponds to his bidding price [Sak00]. Stubblebine and Syverson proposed an open-bid auction scheme that uses a hash chain technique[SS99]. Kobayashi, Morita and Suzuki proposed a sealed-bid auction that uses only hash chains [SKM00,KMSH01]. Omote and Miyaji proposed a sealed-bid auction with $\log p$ efficiency, however, it leaks some information [OM00]. Baudron and Stern proposed a sealed-bid auction based on circuit evaluation using homomorphic encryption [BS01]. Chida, Kobayashi and Morita proposed a sealed-bid auction with $\log p$ round complexity [CKM01].

2 $M+1$-st Price Auction

2.1 Auction Rules

The sealed-bid auction is a type of auction in which bids are kept secret during the bidding phase. In the bidding phase, each bidder sends his sealed bidding price. In the opening phase, the auctioneer opens the sealed bids and determines the winning price and winning bidders according to a predetermined rule. In the

case of an $M+1$-st price auction, the $M+1$-st (highest) price is the winning price and bidders who bid higher than the winning price are winning bidders. The $M+1$-st price auction is used for selling M units of a single kind of goods. If $M=1$, it is equivalent to the well-known Vickrey auction.

- *Bidding* : The auctioneer shows M units of a single kind of goods for auction, e.g., M Swiss watches, and calls the bidders to bid their price for the item. Each bidder then decides his price, seals his price, e.g., by envelope, and puts his sealed price into the auctioneer's ballot box.
- *Opening* : After all bidders have cast their sealed prices, the auctioneer opens his ballot box. He reveals each sealed price, determines winning price, the $M+1$-st (highest) price, and finds the wining bidders who bid higher than the winning price. Each winning bidder buys one unit of the goods at the $M+1$-st winning price. (If more than M bidders bid at the same highest price, the auction fails.)

The $M+1$-st price auction is celebrated in economics or game theory for having *incentive compatibility*, that is, the *dominant strategy* (optimal strategy) for each bidder is to bid honestly his own true value [Vic61]. The reason is that for each bidder his bidding price does not affect the winning price (in contrast with the usual highest price auction where higher bidding price yields higher winning price). Accordingly, the bidder finds that it is optimal to bid as high as he is willing to go.

2.2 Requirements

To achieve a fair auction, the $M+1$-st price auction must satisfy two requirements: secrecy and public verifiability.

First, only the winning price and bidders should be revealed. If the auctioneer can know the M-th bidding price (that is the lowest price of bidding prices of M winning bidders) before opening, he can tell a collusive bidder to bid at slightly cheaper price than the M-th bidding price, and can maximize the winning price to gain more money. Even if a bidder (or an auctioneer) can know the bidding prices of other bidders after opening, he can collect information about the bidding strategy or finances of the other bidders, and can utilize it to cheat at the next auction. Because of incentive compatibility, the bidding price is the bidder's honest price for the goods. It follows that information on bidding prices has more significance than is true in the usual highest price auction, where bidding price is not the bidder's honest price.

- *Secrecy* : The information revealed is the $M+1$-st winning price and the wining bidders. All other bidding prices must be kept secret, even from the auctioneer.

Due to the secrecy requirement, only the results of the auction can be known. Accordingly, it is necessary to convince all bidders that anyone can verify the correctness of the results of the auction.

– *Public verifiability* : Anyone must be able to verify the correctness of the auction.

3 Proposed $M+1$-st Price Auction

3.1 Underlying Idea

We can construct our $M+1$-st price auction by using probabilistic public key encryption $E(m)$ that provides indistinguishability, *homomorphic property*, and *randomizability*. The homomorphic property means that $E(a)E(b) = E(ab)$, and the randomizability means that one can compute a randomized ciphertext $E'(m)$ only from the original ciphertext $E(m)$, i.e. without knowing either the decryption key or the plaintext. For instance, ElGamal encryption or Paillier encryption [Pai99] have the properties desired, so our auction scheme can be built based on these encryption schemes.

One important technical issue is how to represent and encrypt the bidding prices so that the succeeding tasks are done easily. In this work, we assume that the possible bidding prices consist of p prices labelled $1, \ldots, p$. The correspondence between the label and real price is determined beforehand. A sealed bid, say $\boldsymbol{b}$, which represents price j $(1 \leq j \leq p)$ is a vector of ciphertexts

$$\boldsymbol{b}(j) = (\underbrace{E(z), ..., E(z)}_{j}, \underbrace{E(1), ..., E(1)}_{p-j})$$

where $E(1)$ and $E(z)$ denote encryption of 1 and common public element z $(\neq 1)$, respectively. Each encryption must be done independently so that they are indistinguishable from each other. The encryption is done using a public key generated and maintained by the authorities in the threshold manner.

Now, bidder B_i $(1 \leq i \leq b)$ posts $\boldsymbol{b}_i(p_i) = (b_{1,i}, \ldots, b_{p,i})$ as his bidding price p_i. Consider the component-wise product of all bids;

$$\prod_i \boldsymbol{b}_i(p_i) = (\prod_i b_{1,i}, \ldots, \prod_i b_{p,i}).$$

Observe that, due to the homomorphic property, the j-th component of this vector has the form

$$c_j = \prod_i b_{j,i} = E(z^{n(j)})$$

where $n(j) = \#\{i \mid j \leq p_i\}$ is the number of bidders whose bidding price is equal to or higher than j. Notice that $n(j)$ monotonically falls as j increases. Let us assume that the auctioneers can test whether $n(j) \leq M$ holds or not without gaining any further information such as $n(j)$ itself. By repeating this test, they can find the winning $M+1$-st bidding price, say p_{win}, that satisfies $n(p_{win}) \geq M+1$ and $n(p_{win}+1) \leq M$. The auctioneers then determine the wining bidders by opening all bids at the price $p_{win}+1$, i.e., decrypt $b_{p_{win}+1,i}$ $(1 \leq i \leq b)$ and find winning bidders B_i with $D(b_{p_{win}+1,i}) = z$.

To examine whether $n(j) \leq M$ or not without revealing any further information, we use the mix and match technique that allows us to determine whether the decryption $D(c)$ of ciphertext c belongs to a specified set S of some plaintexts. By homomorphicity and randomizability of encryption E, we can apply mix and match to accumulated bid c_j.

To provide public verifiability, each bidder must prove that his bid $\boldsymbol{b}(j)$ is valid, i.e. it suits the form described above, in zero-knowledge manner. This seems, however, difficult to do efficiently. To overcome this difficulty, we develop a technique that involves taking the "differential" and "integral" of a vector of homomorphic ciphertexts. Each bidder B_i posts the "differential" $\Delta\boldsymbol{b}(j)$ of $\boldsymbol{b}(j)$

$$\Delta\boldsymbol{b}(j) = (\underbrace{E(1), ..., E(1)}_{j-1}, E(z), \underbrace{E(1), ..., E(1)}_{p-j})$$

that contains $p-1$ $E(1)$'s and one $E(z)$ as j-th component (note that the "differential" of Heaviside's step function is Dirac's delta function). He then proves the correctness of his bid (this can be done efficiently by using the homomorphicity). To recover $\boldsymbol{b}(j)$, the auctioneers take the "integral" of $\Delta\boldsymbol{b}(j)$

$$\boldsymbol{b}(j)_p = \Delta\boldsymbol{b}(j)_p, \boldsymbol{b}(j)_{p-1} = \Delta\boldsymbol{b}(j)_{p-1}\boldsymbol{b}(j)_p, \ldots, \boldsymbol{b}(j)_1 = \Delta\boldsymbol{b}(j)_1\boldsymbol{b}(j)_2$$

where $\boldsymbol{b}(j)_i$ and $\Delta\boldsymbol{b}(j)_i$ denote the i-th components of vectors $\boldsymbol{b}(j)$ and $\Delta\boldsymbol{b}(j)$ respectively.

3.2 Building Blocks

We summarize the cryptographic tools used in our auction. We denote a ciphertext of ElGamal encryption with public key $g, y = g^x$ by $E(m) = (G = g^r, M = my^r)$.

We use the proof of equality of logarithms [CP92] and the proof of OR of statements [CDS94]. By using the proofs, we have the following verifiable encryption, decryption, powering, mix [Abe99], and mix and match [JJ00] processes.

- *Verifiable encryption* : We can prove that ciphertext $E(m) = (G = g^r, M = my^r)$ is an encryption of m without revealing the secret random r by proving $\log_g G = \log_y M/m$.
- *Verifiable decryption* : We can prove that plaintext $m = M/G^x$ is the decryption of $E(m) = (G, M)$ without revealing the secret key x by proving $\log_G M/m = \log_g y$.
- *Verifiable powering* : We can prove that ciphertext $E'(m^r) = (G' = G^r, M' = M^r)$ is a power of $E(m) = (G, M)$ without revealing the secret random r by proving $\log_G G' = \log_M M'$.
- *Verifiable mix* [Abe99] : The publicly verifiable mix randomizes and permutes its input ciphertexts without revealing the randomization and the permutation to hide the correspondence between inputs and outputs; a proof of the correctness of the mixing can be given.

First, we construct a publicly verifiable 2-input mix that randomizes and permutes two inputs in a publicly verifiable manner. We can prove that ciphertext $E'(m) = (G' = Gg^r, M' = My^r)$ is a randomization of $E(m) = (G, M)$ without revealing the secret random r by proving $\log_g G'/G = \log_y M'/M$. By combining this with the OR proof, we can prove that the 2-input mix randomizes and swaps OR randomizes and does not swap two inputs. We then can construct a publicly verifiable n-input mix by combining $n \log_2 n - n + 1$ 2-input mixes based on Waksman's permutation network.

– *Mix and match* [JJ00] : By using the mix and match one can examine whether the decryption $D(c)$ of ciphertext c belongs to a specific set $S = \{p_1, p_2, \ldots, p_n\}$ of plaintexts.
First, we construct n ciphertexts $c_i = c/E(p_i)$ $(0 \leq i \leq n)$. We then take the power $c_i^{r_i}$ of them using a secret random factor r_i, mix them, and decrypt the mixed n ciphertexts in a publicly verifiable manner. If there exists one plaintext 1, we are convinced that $c \in S$. If there exists no plaintext 1, we are convinced that $c \notin S$.

3.3 Protocol

There are bidders $B_1, \cdots, B_b$, auctioneer A, and trusted authority T. Auctioneer A plays the role of a bulletin board. Trusted authority T generates a secret key and a public key in the preparation phase. In the opening phase, it receives ciphertexts from auctioneer and performs mix and match and decrypts them. If desired, the trusted authority can be built in a distributed way to make it trustful in a threshold sense.

– *Preparation* : Trusted authority T generates a secret key and a public key for ElGamal encryption E, and publishes the public key.
Auctioneer A publishes a price list $P = \{1, 2, \cdots, p\}$ for the auction and a generator z of the cyclic group used for encryption.
– *Bidding* : In the bidding phase, each bidder B_i $(1 \leq i \leq b)$ decides his bidding price $p_i \in P$ and computes encrypted vector

$$\Delta b_{j,i} = \begin{cases} E(z) & \text{if } j = p_i \\ E(1) & \text{if } j \neq p_i \end{cases} \quad (1 \leq j \leq p)$$

and constructs the proofs of

"$\Delta b_{1,i} \cdots \Delta b_{p,i} = E(z)$" and "$\Delta b_{j,i} = E(1)$ OR $\Delta b_{j,i} = E(z)$".

He then publishes the encrypted vector and the proofs.
– *Opening* : In the opening phase, auctioneer A publicly takes "integral"

$$b_{p,i} = \Delta b_{p,i}, b_{p-1,i} = \Delta b_{p-1,i} b_{p,i}, \ldots, b_{1,i} = \Delta b_{1,i} b_{2,i} \quad (1 \leq i \leq b)$$

and "superimposition"

$$c_j = b_{j,1} \cdots b_{j,b} \quad (1 \leq j \leq p).$$

From the homomorphic property, we have the encrypted vector

$$c_j = E(z^{n(j)}) \quad (1 \leq j \leq p)$$

where $n(j) = \#\{i \mid j \leq p_i\}$. By applying the mix and match technique [JJ00] to c_j, we can examine whether $n(j) \leq M$ or not, i.e., we can examine whether $D(c_j) \in \{1, z, z^2, \ldots, z^M\}$ or not. To determine winning $M+1$-st bidding price, i.e., price p_{win} s.t. $n(p_{win}) \geq M+1$ and $n(p_{win}+1) \leq M$, we perform a binary search using the examination by mix and match; auctioneer A sends c_j to trusted authority T for $\lceil \log p \rceil$ rounds, and trusted authority T performs mix and match.

To determine winning bidders, we decrypt $b_{p_{win}+1,i}$ $(1 \leq i \leq b)$ and find winning bidders B_i with $D(b_{p_{win}+1,i}) = z$. Thus auctioneer A sends $b_{p_{win}+1,i}$ $(1 \leq i \leq b)$ to trusted authority T, and trusted authority T, who decrypts them.

Finally, auctioneer A publishes the winning price and the winning bidders.

Notice that we can also create the usual M-th price auction with some slight modification.

3.4 Security

We discuss the security of our auction. First, we consider the case where all bidders are honest and all input bids are independently and privately made. Against passively deviating auctioneers, our scheme leaks no information and achieves auction secrecy, since the underlying encryption scheme is indistinguishable and the building blocks, mix and mix and match, are secure. Against actively deviating auctioneers, all steps of our scheme except the bidding step are robust, i.e., an adversary can not manipulate the messages without detection, since all steps are publicly verifiable.

Now, we consider malicious bidders. In such a case, we are not sure whether the bids are still independent or not. Indeed, in the bidding step, the malicious bidder can bid at any price relative to the bidding price of other bidder. He can construct a bidding vector of any price by shifting and randomizing the components of another bidder's bidding vector. Fortunately, we can avoid such an attack by encrypting the whole bidding vector and its poof using non-malleable, publicly verifiable, threshold encryption scheme, e.g., Shoup and Gennaro's encryption [SG98]. After all bidders publish their encrypted bids, the auctioneers threshold decrypt them and check the proof, and continue the protocol. Since each bid is encrypted in a non-malleable manner, the malicious bidder can not create a dishonest bid by modifying the bid of another bidder.

Finally, notice that of course our protocol does not improve on the security offered by the original $M+1$-st price auction. For instance, consider that $M+1$ malicious bidders can fault the protocol by bidding at the highest price p and making $M+1$ winning bidders. Note, however, that the original $M+1$-st price auction also fails. Accordingly, this attack is against the original concept of the $M+1$-st price auction, not our protocol. Thus preventing this kind of attack exceeds the scope of this paper.

3.5 Efficiency

We discuss communication and computational complexity of our auction and compare it to the $M+1$-st price auction described in [Kik01].

Table 1. The communication complexity of our scheme.

	pattern	round	volume
Bidding (per one bidder)	$B_i \to A$	1	$O(p)$
Determining $M+1$-st price	$A \to T$	$\lceil \log p \rceil$	$O(M+1)$
Determining winning bidders	$A \to T$	1	$O(b)$

Table 2. The computational complexity of our scheme.

	computational complexity
Bidder (per one bidder)	p encryptions and $p+1$ proofs
Auctioneer	$2bp$ ciphertext multiplications
Mixing	$\lceil \log p \rceil$ times $M+1$ input mixings
Decrypting	$\lceil \log p \rceil (M+1) + b$ decryptions

Table 1 shows the communication pattern and the number of rounds and volume per communication round in our scheme when there are b bidders bid and there are p potential bidding prices. Since only 1 communication round from a bidder to the auctioneer is required in the bidding phase, our scheme achieves the "bid and go" concept. Only $\lceil \log p \rceil$ rounds of communication are required in the opening phase, since we can use binary searching by virtue of the mix and match technique.

In [Kik01], the number of auctioneers must be more than the number p of prices, and each bidder must communicate with these auctioneers not only to bid but also to determine the winning price and bidders. In comparison with these schemes, our scheme has only one auctioneer and the communications in our scheme is quite simple.

Table 2 shows the computational complexity of our scheme. The complexity of each bidder is proportional to p, so it might be heavy for a large price range. The complexity of the auctioneer is proportional to bp, and this dominates the cost of the whole protocol. The complexity of mixing is proportional to $\lceil \log p \rceil$, and the complexity of one $M+1$ input mix is proportional to $M \log M$ [Abe99,AH01]. The complexity of decryption is proportional to b, so it might be heavy for a large number of bidders.

In [Kik01], the number of auctioneers must exceed the number p of prices, and the complexity of each auctioneer is $O(bp)$. In our scheme, the factor dominating the complexity is the complexity of the auctioneer ($O(bp)$) so our scheme is more efficient than [Kik01].

4 Conclusion

We have introduced an $M+1$-st price sealed-bid auction scheme that offers bidding price secrecy and public verifiability; it uses homomorphic encryption. The scheme has low round communication complexity: 1 round from each bidder to auctioneer in bidding and $\log p$ rounds from auctioneer to decryptor in opening.

We can also construct an $M+1$-st price auction by using Paillier encryption [Pai99] instead of ElGamal encryption. The complexity of our auction, and almost all existing auction schemes, is proportional to the number p of prices. Accordingly, one important goal is to make the complexity proportional to the size $\log p$ of prices.

References

Abe99. M. Abe, "Mix-Networks on Permutation Networks", *Proceedings of ASIACRYPT '99*, pp. 317–324, (1999).

AH01. M. Abe and F. Hoshino, "Remarks on Mix-network based on Permutation Network", *Proceedings of PKC 2001*, pp. 317–324, (2001).

BS01. O. Baudron and J. Stern, "Non-interactive Private Auctions", *Proceedings of Financial Cryptography 2001*, , (2001).

Cac99. C. Cachin, "Efficient Private Bidding and Auctions with an Oblivious Third Party", *Proceedings of 6th ACM Conference on Computer and Communications Security*, pp. 120–127, (1999).

CDS94. R. Cramer, I. Damgård and B. Schoenmakers, "Proofs of Partial Knowledge and Simplified Design of Witness Hiding Protocol", *Proceedings of CRYPTO '94*, pp. 174–187, (1994).

CKM01. K. Chida, K. Kobayashi and H. Morita, "Efficient Sealed-bid Auctions for Massive Numbers of Bidders with Lump Comparison", *Proceedings of ISC '01*, , (2001).

CP92. D. L. Chaum and T. P. Pedersen, "Wallet Databases with Observers", *Proceedings of CRYPTO '92*, pp. 89–105, (1992).

HTK98. M. Harkavy, J. D. Tygar and H. Kikuchi, "Electronic Auctions with Private Bids", *Proceedings of Third USENIX Workshop on Electronic Commerce*, pp. 61–74, (1998).

JJ00. M. Jakobsson and A. Juels, "Mix and Match: Secure Function Evaluation via Ciphertexts", *Proceedings of ASIACRYPT 2000*, pp. 162–177, (2000).

Kik01. H. Kikuchi, "(M+1)st-Price Auction Protocol", *Proceedings of Financial Cryptography 2001*, , (2001).

KHT98. H. Kikuchi, M. Harkavy and J. D. Tygar, "Multi-round Anonymous Auction Protocols", *Proceedings of first IEEE Workshop on Dependable and Real-Time E-Commerce Systems*, pp. 62–69, (1998).

KMSH01. K. Kobayashi, H. Morita, K. Suzuki and M. Hakuta, "Efficient Sealed-bid Auction by using One-way Functions", *IEICE Trans. Fundamentals*, , (Jan. 2001).

Kud98. M. Kudo, "Secure Electronic Sealed-Bid Auction Protocol with Public Key Cryptography", *IEICE Trans. Fundamentals, vol. E81-A, no. 1*, pp. 20–27, (Jan. 1998).

NPS99. M. Naor, B. Pinkas and R. Sumner, "Privacy Preserving Auctions and Mechanism Design", *Proceedings of ACM conference on E-commerce*, pp. 129–139, (1999).

OM00. K. Omote and A. Myaji, "An Anonymous Auction Protocol with a Single Non-trusted Center Using Binary Trees", *Proceedings of ISW2000*, pp. 108–120, (2000).

Pai99. P. Paillier, "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes", *Proceedings of EUROCRYPT '99*, pp. 223–238, (1999).

Sak00. K. Sako, "Universally verifiable auction protocol which hides losing bids", *Proceedings of Public Key Cryptography 2000*, pp. 35–39, (2000).

SG98. V. Shoup and R. Gennaro, "Securing Threshold Cryptosystems against Chosen Ciphertext Attack", *Proceedings of EUROCRYPT '98*, pp. 1–16, (1998).

SKM00. K. Suzuki, K. Kobayashi and H. Morita, "Efficient Sealed-Bid Auction using Hash Chain", *Proceedings of ICISC 2000*, LNCS 2015, (2000).

SM99. K. Sakurai and S. Miyazaki, "A bulletin-board based digital auction scheme with bidding down strategy", *Proceedings of 1999 International Workshop on Cryptographic Techniques and E-Commerce*, pp. 180–187, (1999).

SS99. S. G. Stubblebine and P. F. Syverson, "Fair On-line Auctions Without Special Trusted Parties", *Proceedings of Financial Cryptography 99*, , (1999).

Vic61. W. Vickrey, "Counterspeculation, Auctions, and Competitive Sealed Tenders", *Journal of Finance*, pp. 8–37, (Mar. 1961).