An Equitably Fair On-line Auction Scheme*

Emmanouil Magkos[1], Mike Burmester[1,2], Vassilios Chrissikopoulos[1]

[1] Department of Informatics, University of Pireaus, Greece
{emagos, chris}@unipi.gr
[2] Information Security Group, Royal Holloway, University of London, UK
mikeb@dcs.rhbnc.ac.uk

Abstract. We present a sealed-bid electronic auction scheme that is *equitably fair* for the bidders and the seller. In this scheme, the interests of both the bidders and the seller are safeguarded: the identity of the non-winning bidders and their bidding behavior are protected (anonymity), and the bidders cannot withdraw their bids without being detected (non-repudiation). The scheme fulfills the requirements of a secure auction scheme and is verifiable. It extends the Stubblebine & Syverson auction scheme that is *not* equitably fair (it does not prevent bid withdrawals). Our scheme employs a Registrar and an Auctioneer for which no special trust assumptions are made.

1 Introduction

Electronic auctions are increasingly popular among the members of the Internet community. Many auction houses adopt security mechanisms that are fortified by, and result in, the non-anonymity of bidders and/or the non-privacy of their bids. To hold bidders accountable, bids are authenticated and transactions are logged. As a result, buying profiles may be constructed and the personal information of users (e.g., their bidding behavior) may be used in several ways.

In this paper we propose a cryptographically secure scheme for sealed (first or second-price) electronic auctions that is *equitably fair* [4] for the bidders and "society". That is, while the identity of the bidders and their bidding behavior are protected, bidders are accountable for their actions (i.e., they cannot withdraw their bids). This protects "society" (the seller or/and the auctioneer) from being abused by irresponsible bidders. Therefore, our system treats the bidder and the seller/auctioneer equitably: bidders cannot withdraw their bids, and the Auctioneer cannot find out the identity of a bidder.

We built a sealed-bid auction protocol, which satisfies all the requirements of a secure auction system and differs from [33] in that, while preserving anonymity and privacy prior to the auctioneer's commitment, it prevents bidders from withdrawing their bids. We believe that *bid-withdrawal*, even if the bid has not yet been revealed, may be *fair* for the bidder but is not *equitable* [4] towards "society" (e.g., the seller/auctioneer). As argued in [4], if altered circumstances make a bid unprofitable

* Research supported by the Secretariat of Research and Technology of Greece.

K. Bauknecht, S. Kumar Madria, and G. Pernul (Eds.): EC-Web 2000, LNCS 1875, pp. 72–83, 2000.

or loss making, and a bidder is allowed to withdraw a bid, then "society" is threatened by the individual. Allowing bid withdrawal is as fair as allowing a seller to withdraw the item being auctioned, because altered circumstances make the sale unprofitable.

In our approach, bid-withdrawal can be traced after the auction has ended. For this purpose we make use of Time-Lock Puzzles[1] [29] for non-repudiation. We also make use of Blind Signatures[2] [9] for anonymity, a Cut-and-Choose[3] technique [9] for correctness, and a Certified-Delivery mechanism [5] to prevent denial-of-service attacks. Checks are also made to ensure that only eligible bidders submit valid bids.

Our Scenario. We consider sealed auctions where non-winning bidders retain their anonymity, but no bidder can withdraw a bid. There are several applications in which the anonymity of bidders is an important design feature of auctioning. For example, the bidding behavior of non-winning bidders might be of commercial value. Furthermore, by preventing bid withdrawals, bidders cannot dynamically control an auction by withdrawing their bids when altered circumstances make these unprofitable. Our scenario is appropriate for high security level auctions, where correctness and anonymity are important.

1.1 Related Work

Franklin and Reiter [17] designed and implemented a distributed service for performing sealed-bid auctions. This makes use of *Threshold Secret Sharing* [31] and *Verifiable Signature Sharing* [18] for protection against faulty auction servers, and off-line *Digital Cash* [7] for non-repudiation. Franklin and Reiter also proposed a modification of their protocol to establish anonymity for loosing bidders, but in this case, a coalition between either two faulty servers from different auctions or a faulty server and the bank, may reveal the identity of loosing bidders. Furthermore, threshold mechanisms are not applicable for auctions run by small organizations where all parties involved may be corrupted [25]. Finally, the use of Digital Cash creates an opportunity cost, especially in the case of large bids.

Harkavy, Tygar and Kikuchi [21] used *Verifiable Secret Sharing* [11] and *Secure Distributed Computations* [2] to perform sealed-bid electronic auctions. Their protocol establishes privacy for all but the winning bidder, even after the end of the bidding period. They also suggested the use of *Identity Escrow* [23] mechanisms to establish non-repudiation while preserving anonymity. Their protocol cannot handle tie-breaking (i.e., when several bidders tie for the highest bid) without sacrificing privacy. In [22], they deal with the tie-breaking problem by adding an extra auction

[1] With Time-Lock Puzzles, a message is encrypted so that it cannot be decrypted without running a computer continuously for at least a certain amount of time.

[2] Blind Signatures are the equivalent of signing carbon-paper-lined envelopes. A user seals a slip of a paper inside such an envelope, which is later signed on the outside. When the envelope is opened, the slip will bear the carbon image of the signature.

[3] Cut-and-Choose techniques are used to establish correctness in a blind signature protocol. The signer opens all but one envelope and then signs the remaining envelope.

round. In both protocols, as well as in [17], security relies on the fact that no more than a threshold of auction servers behave maliciously.

Stajano and Anderson [32] propose an anonymous ascending auction between mistrustful principles with no trusted arbitrator. Their protocol assumes that the seller and the bidders anonymously broadcast messages over a Local Area Network, using the Chaum's *Dining-Cryptographers* scheme [8]. The bid submission and the seller's commitment are made by using the *Diffie-Hellman* key exchange [16]. While there is no privacy for the bids, due to the nature of the auction, all loosing bidders remain anonymous and the identity of the winner is revealed to the seller (provided that the seller commits to the highest bid). For non-repudiation, the public keys are *escrowed* [3,12], while accuracy is achieved with a Cut-and-Choose mechanism. The protocol can be implemented in local networks, and is not practical for open networks (such as the Internet).

Stubblebine and Syverson [33] propose a high-level ascending scheme for on-line auctions. The auction is fair in that the auctioneer commits to the submitted bids prior to their disclosure and cannot selectively close the auction after a particular bid is received. To achieve fairness, the protocol makes use of public notaries [34] and certified-delivery services [6]. A bidder constructs a message that consists of the bid and information binding the bid back to the bidder, then commits to this message by using a *Secret Bit Commitment* scheme [30] and finally submits the commitment to the auctioneer using a certified-delivery service. The auctioneer commits to the bid by using a trusted time source (i.e., a public notary) and the bidder opens his commitment. If the communication channel is anonymous the bidder has a choice not to open his commitment. This provides for limited bid-withdrawal.

Summary of Results. This paper presents an *equitably fair* auction scheme, which protects the bidders and their bidding behavior by concealing their identity, while at the same time preventing bidders from abusing the scheme. In particular, (a) non-winning bidders remain anonymous, (b) no bidder is able to withdraw a bid without being detected.

The paper is organized as follows. In Section 2, we overview various auction types presented in the literature. We present a list of desirable properties for secure electronic auctions. In Section 3 we list the basic security assumptions for our scheme and in Section 4 we describe our auction protocol. In Section 5 we show that this protocol satisfies the requirements of Section 2. We conclude in Section 6.

2 Background: Auction-Types and Requirements

In this paper we are mainly concerned with *sealed* auctions, first or second-price [36]. In such auctions bidders submit their bid before the end of a previously agreed bidding period. Each bidder is allowed one bid. After the bidding period ends, bids are opened and the winner is determined. The highest bidder wins and pays the amount bid (first price) or an amount equal to the second highest bid (second-price). We focus on *one-sided* auctions for which there is one seller and many buyers.

There are several other types of auctions such as *ascending* (English) auctions [15], *descending* (Dutch) auctions and their variants (for a survey of auction types see [24, 35]). In ascending auctions, bidders submit bids to overcome the current highest bid, and the auction ends when, within a time interval, no bidder submits a higher bid. In descending auctions, the auctioneer starts the bidding at a high price that lowers gradually, and the first bidder that bids the current price wins the item at that price. Ascending auctions are strategically equivalent to second-price sealed auctions under some preconditions [24].

Sealed bid electronic auctions emphasize security issues inherent in every e-commerce activity, while ascending electronic auctions pose novel problems because of their time-dependence [21]. Agent technology promises to ameliorate these temporal issues [37]. Our system, when used in a second-price auction, achieves both the price-discovery virtue of an ascending auction and the simplicity of a sealed-bid mechanism.

Depending on the type of auction, there is a need to adopt the following requirements.

Anonymity. During the auction, the identity of bidders is not revealed to anyone. After the auction ends, the identity of the winner (this could be a pseudonym) is revealed to the auctioneer, while the identity of loosing bidders remains secret.

Privacy. Bids are not revealed to anyone unless a precondition is satisfied. In a sealed-bid auction, this may be the end of the bidding period.

Correctness. The following properties must be satisfied to achieve correctness:

- Only eligible bidders can submit bids.
- No one can impersonate a bidder.
- Valid bids cannot be altered/eliminated by the auctioneer.
- Bids are valid only for the specified auction.
- The winner of the auction is always the highest bidder.

Non-Repudiation. Bidders cannot repudiate (withdraw) submitted bids.

Verifiability. All participants are able to verify the fairness of the results.

3 Basic Security Assumptions

Our protocol uses cryptographic tools and techniques that are publicly known and have been proposed during the past years, such as *Time-Lock Puzzles* [29] for non-repudiation, *Blind Signatures* [9] for anonymity and *Cut-and-Choose* techniques [7] for correctness. We make the following assumptions:

Certificate Infrastructure. There is a *Certificate Infrastructure* and the users are legally bound by their signature. Mechanisms to establish non-repudiation for digitally signed messages are discussed in [38]. We also assume that bidders, prior to their registration, possess a private/public key pair and a corresponding certificate, issued by a trusted Certification Authority (CA). This means that they have already proved to a trusted authority their ability to pay for a transaction.

Channel Anonymity. There is an *anonymous* channel where bidders can send/accept messages that cannot be traced (e.g., by using traffic analysis). For example, e-mail anonymity can be established using *Mixmaster* re-mailers[4] [10, 14]. HTTP anonymity can be established by using services such as the *Anonymizer* [13], *Crowds* [28], the *Lucent Personalized Web Assistant* (LPWA) [26], and *Onion-Routing* [20]. LPWA and Onion-Routing can handle e-mail as well as HTTP. Onion-Routing also supports "reply onions" that allow anonymous replies to be sent in response to a previously received anonymous e-mail.

Asynchronous Communication. Communication during the auction is *asynchronous* i.e. messages by the sender are received within a bounded (but unknown) time interval [1]. Thus, all bids are supposed to be received before the closing of the bidding period.

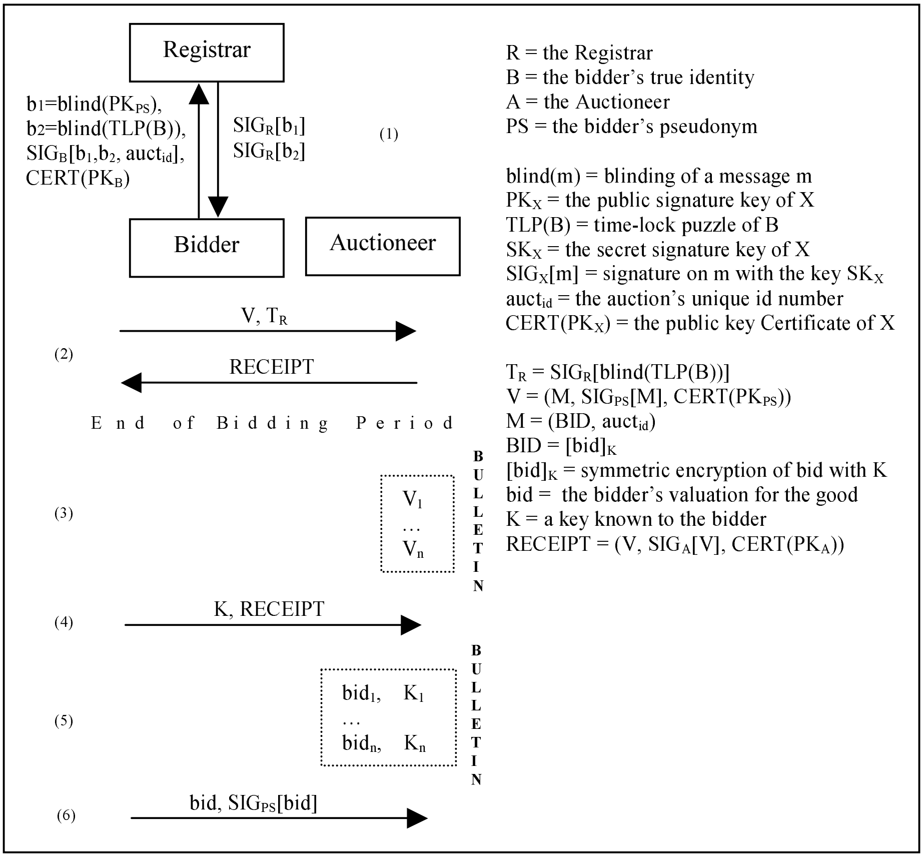
Certified Delivery. All entities participating in the protocol agree on a C*ertified-Delivery* Service. We assume that this Service provides for anonymity and *atomicity* [1, 5]. This means that a bidder can prove, while preserving his anonymity, that a bid has been submitted to the auctioneer and that the auctioneer accepted the bid at a specific time, with no intermediate situations (in which, for example, the auctioneer would have a proof of origin while the bidder would not have a proof of receipt). Optionally, the seller may be allowed to submit test-bids periodically, in order to ensure that the auctioneer is operational [33].

Tie Breaking. We assume that bids submitted during the protocol are in a "dollars//cents" form (e.g. "one thousand nine hundred and ninety-nine dollars and ninety-nine cents") so that the possibility of a tie between two bidders is practically impossible. This assumption can be circumvented by using *Coin Flipping* [30] in order to determine a winner, or the techniques used in [22].

4 The Auction Protocol

Our system employs two authorities, a Registrar and an Auctioneer. The Registrar blindly authenticates eligible bidders while the Auctioneer processes valid bids. The auction requires six steps that we describe below –see Fig. 1.

[4] A Mixmaster re-mailer re-mails the messages it gets after a random time-interval (latency). It also re-mails messages in a different order.



R = the Registrar
B = the bidder's true identity
A = the Auctioneer
PS = the bidder's pseudonym

blind(m) = blinding of a message m
PK_X = the public signature key of X
TLP(B) = time-lock puzzle of B
SK_X = the secret signature key of X
$SIG_X[m]$ = signature on m with the key SK_X
$auct_{id}$ = the auction's unique id number
$CERT(PK_X)$ = the public key Certificate of X

$T_R = SIG_R[blind(TLP(B))]$
$V = (M, SIG_{PS}[M], CERT(PK_{PS}))$
$M = (BID, auct_{id})$
$BID = [bid]_K$
$[bid]_K$ = symmetric encryption of bid with K
bid = the bidder's valuation for the good
K = a key known to the bidder
$RECEIPT = (V, SIG_A[V], CERT(PK_A))$

Fig. 1. A First/Second price auction protocol

Step 1, Registration. A bidder, say Bob, gets a pseudonym that will identify him to the Auctioneer. To do that, Bob creates a private/public key pair (SK_{PS} , PK_{PS}*)* and a Time-Lock Puzzle[5] of his real identity, TLP(B). Bob blinds (e.g., see [30]) both PK_{PS} and TLP(B) to create the blindings b_1 and b_2 respectively, and then signs a message consisting of the blindings b_1, b_2, and the unique auction identification number $auct_{id}$. Bob sends these to the Registrar and gets the blindings authenticated by the Registrar. For the correctness of the blindings, a Cut-and-Choose[6] protocol is used. This guarantees that TLP(B) can be solved back to Bob's identity in case of repudiation, while at the same time the Registrar cannot link the puzzle with Bob directly.

[5] There are several ways to implement Time-Lock Puzzles. In [20], the message (Bob's identity) is encrypted with an appropriately large symmetric key, which in turn is encrypted in such a way that it cannot be decrypted in a parallelizable way.

[6] Bob sends *n* blinded messages to the Registrar, then unblinds any n-1 indicated by the registrar. The Registrar signs the remaining message. There is a tradeoff between choosing a large n (strong correctness), and a small n (efficiency).

After Step 1, Bob unblinds the Registrar's signatures on b_1 and b_2. The public key PK_{PS}, certified by the Registrar (and unblinded by Bob), is Bob's official pseudonym [10] and can been seen as a Certificate CERT(PK_{PS}) that will be used by the Auctioneer, in Step 2, to verify signatures under Bob's pseudonymous identity PS. From now on, the Time-Lock Puzzle, when signed by the Registrar (and unblinded by Bob), will be denoted by T_R.

Step 2, Bid Submission. Bob encrypts his bid with a secret symmetric key K, then prepares a message M that consists of $[bid]_K$ and $auct_{id}$. Bob signs M under his pseudonym (i.e., by using SK_{PS}) to create a valid bid V. He anonymously sends V and T_R to the Auctioneer, using the Certified-Delivery service. Bob gets a RECEIPT from the Auctioneer. The Auctioneer uses CERT(PK_{PS}) to verify the pseudonymous signature, checks $auct_{id}$, verifies the Registrar's signature in T_R. If all checks are valid the Auctioneer records V, T_R, otherwise the bid is discarded.

Step 3, Publication of Committed Bids. After the bidding period ends, the eligibility proofs V_i (including the encrypted bids) are published by the Auctioneer. In this way, the Auctioneer commits to the encrypted results. Optionally, the Auctioneer could as well publish a receipt of origin for each message, issued by the Certified-Delivery service, where the time of bid submission would be noted to ensure that the Auctioneer does not accept bids beyond the pre-specified closing time.

Step 4, Bids Revelation. Bob reveals his bid by anonymously sending the pair (K, RECEIPT) to the Auctioneer. The Auctioneer will use RECEIPT to retrieve Bob's record from his database, and the key K to decrypt the encrypted bid. If Bob will not submit K within a predetermined time interval, the bid can be traced back to Bob by solving the Time-Lock Puzzle T_R.

Step 5, Final Results. The Auctioneer publishes all decrypted bids and the keys used to decrypt them. The winner is then determined and all parties are able to verify the auction results.

Step 6, The Winner's Proof. If Bob is the winner, he sends in Step 6 his signature on the winning bid. If Bob repudiates the winning bid, his identity can be retrieved by solving the Time-Lock Puzzle T_R.

5 Security Analysis

Our auction scheme provides protection for the bidders, the Auctioneer and the Registrar against malicious behavior by any number of participants. We do not make any special trust assumptions for the Registrar and the Auctioneer: both authorities may misbehave. We evaluate the security of our protocol by examining the requirements listed in Section 2.

5.1 Anonymity

The Registrar checks the identity of a bidder who submits a pseudonym (the pseudonym is authenticated by the bidder). However, the pseudonym is blindly signed in Step 1. Consequently, the Registrar cannot trace any encrypted bid, published in Step 3, back to the bidder's real identity.

The Auctioneer receives messages that cannot be traced back to the sender (the communication channel is anonymous) and that are signed under a certified pseudonym. The Auctioneer cannot link the pseudonym with the bidder's real identity, so the only way to find out the bidder's identity is by solving the puzzle T_R, submitted with the encrypted bid in Step 2.

If the Auctioneer conspires with the Registrar, they cannot learn more than they each know separately. However, if a bidder submits a bid to the Auctioneer in Step 2 immediately after Step 1, the two conspiring authorities might guess correctly which bidder bids what. This problem can be solved in part by using a Mixmaster re-mailer that incorporates *latency* and *reordering* mechanisms [14]. Additionally, bidders may be instructed not to submit their bids to the Auctioneer immediately after registration in Step 1. The time-independence of the auction type being proposed (i.e., a sealed-bid) favors this solution.

5.2 Privacy

After Step 1 and until the end of the bidding period, bids are protected by symmetric encryption. One has to break the symmetric encryption in order to break the bidder's privacy. After Step 4, when all bidders reveal the encryption keys, there is no bid privacy. This poses no security threats because at this stage the auction is essentially completed and the hidden bids already committed by the Auctioneer. Furthermore, bids are revealed to enable verification. Finally, anonymity throughout the auction procedure compensates for the loss of privacy.

5.3 Correctness

Only eligible bidders can submit bids. There are two things that determine the user's eligibility through the auction procedure: the certificate $CERT(PK_{PS})$ and the Time-Lock Puzzle T_R (signed by the Registrar).

The Auctioneer uses $CERT(PK_{PS})$ to verify that the bidder is a valid user and rejects all bids that are not authenticated. This filtering makes the auction procedure flexible, saves the Auctioneer from useless bid storage and processing time, and discourages denial-of-service attacks. Independent users also use $CERT(PK_{PS})$ to verify that the auction results are correct (e.g., they verify that bids published in Step 3 have been submitted by eligible bidders and not by the Auctioneer).

The Time-Lock Puzzle T_R is used by the Auctioneer in case of bid repudiation. A bidder gets T_R from the Registrar in Step 1 by proving, during the Cut-and-Choose protocol, that it is linked to his identity. Only the bidder can unblind T_R, so the

Auctioneer knows that the owner of T_R is an eligible bidder whose identity will be uncovered in case of repudiation.

No one can impersonate a bidder. There are several reasons why someone would want to link their bid to another bidder, say Bob. For example, a bidder may wish to incriminate Bob in case of bid withdrawal, or for high bogus bids.

The Registrar knows Bob's identity so can make a fake T_R^* and impersonate Bob to the Auctioneer (or give T_R^* to a friend). However, T_R^* does not establish non-repudiation for Bob if the fake bid is the winning bid (or if it is withdrawn). Bob can later prove his innocence by revealing his own Time-Lock Puzzle T_R. If T_R is different than T_R^* (and it will be, with a very high probability since the bidder got T_R in Step 1 using a Cut-and-Choose protocol) then everybody knows that the Registrar has cheated.

The Auctioneer sees Bob's Time-Lock Puzzle T_R after Step 2, so he might want to use it to create a fake bid (e.g., by giving it away to a friend) in order to establish non-repudiation for Bob. Normally, the Auctioneer should check his database and reject all bids containing a T_R already submitted. Even if the Auctioneer is not supposed to check his database and just accepts bids, Bob can prove that the Auctioneer has cheated: when Bob submits his bid along with the authentic T_R, he gets a proof of receipt, signed at a time determined by an external trusted source such as the Certified-Delivery Service. This enables Bob to prove that his bid was submitted earlier.

Valid bids cannot be altered/eliminated by the Auctioneer. The use of the Certified-Delivery Service in Step 2 prevents the Auctioneer from altering or eliminating valid bids. The service enables bidders to prove to an arbitrator that, for example, the Auctioneer received a message M at time t. Consequently, the Auctioneer cannot eliminate a correct bid pretending that it is incorrect (or that it has not been submitted). In addition, the Auctioneer cannot reject a bid pretending that it has been submitted at a time later than the end of the bidding period. After the publication in Step 3, the Auctioneer commits to the encrypted results of the auction and cannot alter them without being detected.

Bids are valid only for the specified auction and cannot be reused. During the protocol, $auct_{id}$ is used as a freshness indicator. The Auctioneer rejects all messages that are signed by the bidder and do not contain a valid $auct_{id}$ number. In Step 3, $auct_{id}$ is published next to the encrypted bid, as part of message V.

No one but the highest bidder is the winner of the auction. This requirement is always satisfied because of the *verifiability* feature discussed next.

5.4 Verifiability

All participants can independently verify the results of the auction. The encrypted results are published in Step 3, prior to the decryption of bids in Step 4. In Step 5 all decrypted bids are published along with the keys used to decrypt them. The results in Step 5 are the Auctioneer's commitment to the outcome of the auction so they must be consistent with the results in Step 3. The Auctioneer will be responsible for any inconsistency. A bidder can verify the results concerning other bidders by decrypting the encrypted bids with the published keys and by verifying the signed bids.

5.5 Non-Repudiation

The "point of no return" for a bidder can be either the anonymous bid submission in Step 2, before the closing of the bidding period (*strong non-repudiation*) or optionally the anonymous sending of the decryption key K in Step 4, after the closing of the bidding period (*weak non-repudiation*).

In any case the winner cannot repudiate his bid. If the winner does not initiate Step 6 within a pre-specified time interval, then the Auctioneer can discover the identity of the winner by solving the Time-Lock Puzzle. The winner will then be subject to a penalty price, *a priori* known and agreed upon by all participants [33]. For example, this penalty price could be equal to the cost of solving the puzzle, plus the unpaid (repudiated) bid.

Strong Non-Repudiation (no Bid-Withdrawal). Bidders commit to the bids published in Step 3. All bidders whose bids are published in Step 3 must provide the keys necessary to decrypt them. For each bidder who does not submit K the Auctioneer solves the Time-Lock Puzzle to retrieve the bidder's identity. By not allowing bidders to repudiate submitted bids, the auction is *equitably fair* for both bidders and the auctioneer/seller, as argued in Section 1.

Weak Non-Repudiation (Bid-Withdrawal). Each bidder may be allowed not to reveal the key K necessary to decrypt the encrypted bid published in Step 3 (i.e., to withdraw his bid). In this case, at least one bidder has to initiate Step 4 for the Auctioneer to declare a winner. All bids for which a key K has been submitted within a predefined time interval are published in Step 5. Bidders commit only to the bids published in Step 5.

6 Conclusion

We have presented an equitably fair sealed on-line auction scheme with no special trust assumptions. The system is equitable in that, while preserving anonymity for the non-winning bidders, it does not allow the withdrawal of any submitted bid. The bidders use one-time pseudonyms and commit to their identity in such a way that one has to solve a Time-Lock Puzzle in order to reveal it, for non-repudiation. Because the pseudonyms and the identity commitments are one-time, it is not possible to trace the identity of loosing bidders, except by solving a time-consuming computational problem. Our scheme extends the Stubblebine & Syverson auction scheme [33] that does *not* prevent bid withdrawals.

Our protocol, while quite efficient, uses a Cut-and-Choose mechanism to establish correctness, which requires a certain number of interactions. This can be costly. Obviously there is a trade-off between security and efficiency. Our protocol is designed for auctions that require a high security level, and is not suitable for low value auctions for which correctness and anonymity are of little consequence.

It is easy to see how to extend this scheme to equitable ascending auctions. It is also possible to extend this scheme to support equitable *Double Auctions* [19] and equitable *Continuous Double Auctions* (with multiple sellers and buyers) [27].

References

1. Asokan, N., Shoup, V., Waidner, M.: Asynchronous Protocols for Optimistic Fair Exchange. In: Proceedings of 1998 IEEE Symposium on Security and Privacy. IEEE CS Press (1998) 86-99
2. Ben-Or, M., Goldwasser, S., Wigderson, A.: Completeness Theorems for Non-Cryptographic Fault-Tolerant Distributed Computing. In: 20th Annual ACM Symposium on Theory of Computing. ACM (1988) 1-10
3. Boneh, D., Franklin, M.: Efficient Generation of RSA keys. In: Advances in Cryptology – CRYPTO 97, Lecture Notes in Computer Science, Vol. 1233. Springer-Verlag (1997) 425-439
4. Burmester, M., Desmedt, Y., Seberry, J.: Equitable Key Escrow with Limited Time Span (or How to Enforce Time Expiration Cryptographically). In: Advances in Cryptology - ASIACRYPT '98, Lecture Notes in Computer Science, Vol. 1514. Springer-Verlag (1998) 380-391
5. Camp, J., Harkavy, M., Tygar, K., Yee, B.: Anonymous Atomic Transactions. In: 2nd USENIX Workshop on Electronic Commerce. USENIX Press (1996) 123-133
6. Certmail: The Certified Electronic Mail System, http://www.certmail.com/
7. Chaum, D., Fiat, A., Naor, M.: Untraceable Electronic Cash. In: Advances in Cryptology – CRYPTO 88, Lecture Notes in Computer Science, Vol. 1440. Springer-Verlag (1988) 319-327
8. Chaum, D.: The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability. Journal of Cryptology, Vol. 1(1), (1988) 65-75
9. Chaum, D.: Security Without Identification: Transaction Systems to Make Big Brother Obsolete. Communications of the ACM, Vol. 28(10), (1985) 1030-1044
10. Chaum, D.: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. Communications of the ACM, Vol. 24(2), (1981) 84-88
11. Chor, B., Goldwasser, S., Micali, S., Awerbuch, B.: Verifiable Secret Sharing and Achieving Simultaneity in the Presence of Faults. In: 26th IEEE Symposium on the Foundations of Computer Science. IEEE Press (1985) 383-395
12. Cocks, K.: Split Knowledge Generation of RSA Parameters. In: 6th IMA Conference on Cryptography and Coding. Springer-Verlag (1997) 89-95
13. Community ConneXion, Inc., http://www.anonymizer.com
14. Cottrell, L.: Mixmaster and Remailer Attacks. Available from http://obscura.obscura.com/~loki/remailer/remailer-essay.html
15. Crampton, P.: Ascending Auctions. European Economic Review, Vol. 42, (1998) 745-756
16. Diffie, W., Hellman, M.: New Directions in Cryptography. IEEE Transactions on Information Theory, Vol. 22(6), (1976) 644-654
17. Franklin, M., Reiter, M.: The Design and Implementation of a Secure Auction Service. IEEE Transactions on Software Engineering, Vol. 22(5), (1996) 302-311

18. Franklin, M., Reiter, M.: Verifiable Signature Sharing. In: Advances in Cryptology – EUROCRYPT 95, Lecture Notes in Computer Science, Vol. 921. Springer-Verlag (1995) 50-63
19. Friedman, D., Rust, J.: The Double Auction Market: Institutions, Theories and Evidence. Addison-Wesley, MA (1993)
20. Goldschlag, D., Reed, M., Syverson, P.: Onion Routing for Anonymous and Private Communications. Communications of the ACM, Vol. 42(2), (1999) 39-41
21. Harkavy, M., Kikuchi, H., Tygar, J.: Electronic Auctions with Private Bids. In: 3rd USENIX Workshop on Electronic Commerce. USENIX Press (1998) 61-74
22. Harkavy, M., Kikuchi, H., Tygar, J.: Multi-Round Anonymous Auction Protocols. In: 1st IEEE Workshop on Dependable and Real-Time E-Commerce Systems (DARE 99). IEEE Press (1999) 62-69
23. Kilian, J., Petrank, E.: Identity Escrow. In: Advances in Cryptology – CRYPTO 98, Lecture Notes in Computer Science, Vol. 1462. Springer-Verlag (1998) 169-185
24. Klemperer, P.: Auction Theory: A Guide to the Literature. Journal of Economic Surveys, Vol. 13, (1999) at http://econwpa.wustl.edu:8089/eps/mic/papers/9903/9903002.pdf
25. Kumar, M., Feldman, S.: Internet Auctions. In: 3rd USENIX Workshop on Electronic Commerce. USENIX Press (1998) 49-60
26. The Lucent Personalized Web Assistant. Available from http://lpwa.com
27. McCabe, K., Rassenti, S., Smith, V.: Auction Institutional Design: Theory and Behavior of Simultaneous Multiple-Unit Generalizations of the Dutch and English Auctions. American Economic Review, Vol. 80(5), (1990) 1276-1283
28. Reiter, M., Rubin, A.: Crowds, Anonymity for Web Transactions. DIMACS Technical Report 97-15, (1997) available from http://www.research.att.com/projects/crowds/
29. Rivest, R., Shamir, A., Wagner, D.: Time-Lock Puzzles and Timed-Release Crypto. LCS Tech. Memo MIT/LCS/TR-684, (1996) available from http://theory.lcs.mit.edu/~rivest/RivestShamirWagner-timelock.ps
30. Schneier, B.: Applied Cryptography, Second Edition: Protocols, Algorithm and Source Code in C. John Wiley and Sons (1996)
31. Shamir, A.: How to Share a Secret. Communications of the ACM, Vol. 22(11), (1979) 612-613
32. Stajano, F., Anderson, R.: The Cocaine Auction Protocol: On the Power of Anonymous Broadcast. In: 3rd International Workshop on Information Hiding. Lecture Notes in Computer Science, Vol. 1768. Springer-Verlag (1999) 434-448
33. Stubblebine, S., Syverson, P.: Fair On-line Auctions Without Special Trusted Parties. In: Financial Cryptography 99, Lecture Notes in Computer Science, Vol. 1468. Springer - Verlag (1999) 231-241
34. Surety Technologies, Inc., http://www.e-timestamp.com/
35. Ungar, L., Parkes, D., Foster, D.: Cost and Trust Issues in On-line Auctions. In: Agents-98 Workshop on Agent-Mediated Electronic Trading, Minneapolis. MN (1998) 161-172
36. Vickrey, W.: Counterspeculation, Auctions, and Competitive Sealed Tenders. Journal of Finance, Vol. 16(8), (1961) 8-37
37. Wellman, M., Wurman, P.: Real time Issues for Internet Auctions. In: 1st IEEE Workshop DARE 98, (1998) available from http://ftp.eecs.umich.edu/people/wellman/dare98.ps
38. You, C., Zhou, J., Lam, K.: On the Efficient Implementation of Fair Non-Repudiation. In: Proceedings of the 1997 IEEE Computer Security Foundations Workshop. IEEE CS Press (1997) 126-132