

Fair On-line Auctions Without Special Trusted Parties

Stuart G. Stubblebine¹ and Paul F. Syverson²

¹ CertCo, 55 Broad St. - Suite 22, New York, NY 10004, USA,
stubblebine@{cs.columbia.edu, CertCo.com}^{***}

² Center for High Assurance Computer Systems,
Naval Research Laboratory, Washington, DC 20375, USA,
syverson@itd.nrl.navy.mil

Abstract. Traditional face-to-face (English) auctions rely on the auctioneer to fairly interact with bidders to accept the highest bid on behalf of the seller. On-line auctions also require fair negotiation. However, unlike face-to-face auctions, on-line auctions are inherently subject to attacks because the bidders and auctioneer are not copresent. These attacks include selectively blocking bids based on the bidder and amount and selectively closing the auction after a particular bid is received. In this paper, we present an on-line English auction in which bids are processed fairly and the auction closes fairly without specialized trusted parties. In particular, there is no need to trust the auctioneer to obtain a fair outcome to the auction.

1 Introduction

The number of on-line auctions is rapidly growing. In fact, forecasts indicate that on-line auctions and barter will generally replace conventional purchase of set-price items in the future [4]. Currently, there are nearly one hundred on-line auction houses [21].

A limitation on existing auctions is that bidders must trust the auctioneer concerning a fair outcome. Without detection, the auctioneer may selectively block bids based on the bidder and amount. Also, the bidders must trust that the auctioneer doesn't selectively close the auction after a particular bid is received. An English auction ends when effectively there is a timeout interval following the highest bid. The on-line auctions approximate this property by setting an expiration time and allowing the auction to continue beyond the expiration time as long as higher bids continue to be submitted within a short timeout interval. However, whether they have a fixed expiration time or allow continued bidding, all current on-line auctions still trust the auctioneer to be fair in enforcing this closing time.

There are existing auction designs that provide assurance against repudiation of bids and assurance of fairly closing the bidding, e.g., [5, 8]. However, these

^{***} Work, by this author, was primarily performed at AT&T Research.

auctions are sealed-bid, which may not be appropriate to all applications.¹ More importantly, they involve the use of trusted auctioneers. Assurance of auctioneers is increased by employing threshold methods so that a high percentage of compromised trusted auctioneers is necessary to violate the assumed trust. As noted in [7], this approach is not applicable unless the auction is run by a large organization. “In simplistic terms, it is reasonable to expect that, say three out of five employees (servers or server administrators) in a government organization or *xyz_megacorp* will be honest. But it is different to assume that three out of five servers deployed by the relatively small *xyz_little_corp* will not collude.” It would therefore be useful to also have assurance in the necessary trust for auctions conducted by small auction houses—or better still to remove the trust entirely.

We present an auction design that provides for the fair close of an auction and makes bid refusal by the auctioneer provable by bidders and others. At the same time, there is no need for the bidders to trust the auctioneer, or vice versa. The only trusted elements employed are ones that are currently available or in development for independent use in the public information infrastructure. These include public-key authorities, public notaries, and certified delivery services.

In Section 2, we present desirable properties and requirements of on-line auctions. In Section 3, we present our basic auction design and some variants. We also informally argue that our design meets the requirements set out in Section 2.

2 Properties and Requirements of Auctions

2.1 Auction Types

In this paper we focus on versions of the English-type auction: bid amounts are revealed during the auction, and bidders attempt to outbid the previous highest bid amount.

Bid Confidentiality.

1. *Open.* The bid amounts are known to all bidders during the auction.
2. *Sealed.* The bid amounts are only known by the bidder until the auction closes.

We will be concerned with open auctions; however, in our auctions bid amounts are not revealed until after they are committed. We will discuss this temporary secrecy of the bids below. Because we are concerned with open-bid auctions, we will not consider subtleties of sealed-bid auctions. (For example, in the auctions of [5, 8] bids are concealed even from the auctioneers until after close. In fact in [8], even after the close of the auction, only the high bids are ever revealed—to anyone.)

¹ The auction in [8] is a Vickrey-type auction, i.e., bids are sealed, and the item goes to the highest bidder—but at the second highest price. This should mean that bid amounts reflect the true valuations people place on the item, despite the auction being sealed-bid. For more, cf. [8].

Bid Cancellation.

1. *Cancellation.* A bidder can cancel a bid.
2. *No Cancellation.* A bidder can *not* cancel a bid.

Auction Closings. The method of closing an auction depends on whether the auction is sealed or open.

1. *Expiration Time (For open or sealed bid auctions).* The auction closes at a predetermined expiration time.
2. *Timeout (For open bid auctions).* The auction closes when no bids higher than the current high bid are made within a predetermined timeout interval.
3. *Combination of Expiration and Timeout (For open bid auctions).* The auction closes when there is a timeout after the expiration time.

Identity confidentiality may also be an issue in certain lotteries. An auction is *conditionally anonymous* if the bidder identity is confidential unless certain parties agree to uncover the identity. An auction is *weakly anonymous* if the bidder identity is anonymous however the identity can be uncovered with time. For example, uncovering occurs when the auctioneer commits to receiving the bid. Finally, an auction is *profile free* if the auctioneer cannot produce profiles of the bidders (even pseudonymous profiles)[15]. Profile freedom may be with respect to different parties such as to the auctioneer versus to other bidders. In this version of the paper, we do not directly address forms of identity confidentiality. We believe orthogonal mechanisms are available to address issues of identity confidentiality.

2.2 Auction Requirements

Integrity.

1. *Bidder Integrity.* Only authorized clients can submit a bid.

The integrity of the auction is compromised if unqualified bidders are able to make bids.

Fairness.

1. *Opportunity to Out-Bid.* Bidders have the opportunity to out-bid the leading bid.
2. *Non-discrimination of Bids.* When committing to bids (and to the bid order), the auctioneer cannot discriminate between bids based on the bidder or bid amount.
3. *Ordering of Bids.* Only bids made within a reasonably small interval of the present time can be reordered.
4. *Timely Bids.*
Bids can only be committed that are submitted before the prescribed auction closing.

Non-repudiation.

1. *Auctioneer's Remorse.* The auctioneer cannot disavow a committed bid.

Verification.

1. *Timely Verification.* Bidders and sellers can verify the correct operation of the auction in an acceptable amount of time.

3 High Level Auction Design

The basic structure of our design involves a publicly posted database (DB) associated with each auction. The DB should contain a description of the item, and various parameters associated with the auction, e.g., the time bids will begin being taken and conditions for the auction to close. Auction close will be discussed below. There should be an optional minimum bid amount. There should also be a high sales price (effectively a penalty that the auctioneer pays the item owner) that can be invoked if there is evidence that the auctioneer did not perform his duties properly. It should be higher than any reasonable expectation of the maximum bid amount. (The auctioneer and the item owner may want to keep this private between them in case the actual bids are substantially higher than expected.) The DB should also include a history of the bids that have been made so far. This will be used to commit the auctioneer to the status of the auction as it progresses. The commitment takes the form of signatures by a notary on the DB status at regular *notarization intervals* and, within those intervals, signatures on the DB status by the auctioneer. Bids are submitted using secret bit commitment (SBC). (A discussion of various approaches to SBC can be found in [14].) This allows that the auctioneer to commit to a bid before he knows who it is from (even pseudonymously) or what the bid amount is. One way to do SBC is for the bidder to submit his bid encrypted with a secret key. After the auctioneer has committed to the bid submission, the bidder can reveal the key.

We will indicate SBC to a given message M using a secret S by $\langle M \rangle_S$. To prevent the auctioneer from identifying the bidder's address prior to release of the SBC secret, bids should be submitted through an anonymizing mechanism, e.g., Mixmaster remailers [3] or onion routing [11].

The owner of an item up for auction has a vested interest in the auctioneer continuing to accept new (potentially higher) bids until the auction is over. In order for him to be able to test that this is happening, we allow him to submit test bids. These can be explicitly indicated as test bids (once the bit commitment is opened). If he detects that his test bids are not being committed during the auction, he should then attempt to send his test bid via a *certified delivery service*, such as CertMail [1], which is available now, or similar schemes being developed by the US Postal Service. If, within a reasonable period of time, the item owner (or any bidder) can produce evidence that bids were sent without being acknowledged or processed, then the item goes to the highest bidder. But, the sales price is either the high sales amount or the amount of the highest bid,

whichever is larger. More specifically, the owner is paid this amount (minus any commission based on the actual highest bid amount). The winning bidder pays only the amount that he bid. The auctioneer is obligated to cover, at his own expense, any difference between this and the amount owed the item owner. Such a circumstance need not imply any wrongdoing on the part of the auctioneer. It may be the result of a technical fault. Of course, an auctioneer clearly has a vested interest in keeping such faults to a minimum.

Note that, while we assume the existence of a certified delivery mechanism, its primary function is not to deliver bids but to act as a deterrent against the auctioneer refusing to commit to received bids. It need only be employed only rarely, when there is indication that the auctioneer might be doing just that. Which of the acceptable certified delivery services are being used should be stipulated with the auction parameters, so that the auctioneer knows where to check periodically for messages whether or not she is notified that a message has arrived for her. Furthermore, the bidder can decide if it trusts the delivery mechanism when deciding on participating in the auction.

3.1 Auction Protocol

Registration Anyone wishing to bid must register with the auction service. We assume that the bidder registers in some standard fashion. For example, he provides the auction service with whatever credentials and evidence of ability to pay are stipulated, e.g., a credit card number, and he receives a public signature key certificate for use in auctions.

In describing our basic design we will not make any provision for anonymity or related privacy protections in the registration of a bidder. Various mechanisms might be incorporated to make this pseudonymous. Alternatively, registration might incorporate an identity escrow mechanism [6] so that the identity of a winning bidder might only be revealed if he failed to pay. In any case, such techniques are orthogonal to our basic design and we will say no more about them.

If signature keys are used in the straightforward way, then bidders must produce one signature per bid. In order to improve performance, we introduce a way that the bidder need only submit one signature per auction, rather than one signature per bid. We will present this in Section 3.1.

Notarizing the Bid History Within intervals published in the auction parameters, the auctioneer must commit to the bids she has received. To do this, she obtains a notarized (timestamped) version of the bid history from an on-line notary. Several of these digital notaries already exist [20, 10, 16], and legislation has been adopted or is being proposed to standardize the industry. The notary's sole action is to issue a certificate that binds its time-stamp to any file sent to it. (To maintain confidentiality, the image of a one-way hash computation of the document to be protected is what is actually sent.) We will use $\prec M, t_N \succ_N$ to indicate the notarization of M by the notary N at time t_N .

Since these notaries exist independently for various purposes, they are no more specific to the auction service than is an issuer of certificates for public signature verification keys or a certified delivery service. The reasons for the notary in our auction are (1) to provide a nonrepudiable record of the auctioneer's claimed auction history at the time of notarization, and (2) to provide a trusted time source on which the auctioneer and bidders must synchronize. (This prevents, e.g., the auctioneer from terminating the auction early by speeding up her own clock.)

The auctioneer should post the notarized bid history at the public site for the auction, e.g., a Web site. If a bidder cannot obtain an appropriately recent bid history, then he may request one by certified delivery. The auctioneer must then respond by making a copy of the history available via the certified delivery service. The auctioneer would no doubt prefer to minimize her sending of certified messages. Thus, she has an interest in making sure that she posts appropriately updated notarized histories. The auctioneer is obligated to maintain a complete collection of the notarized histories for a reasonable period after the sale of the auctioned item is finalized. This must be produced if any disputes arise as to what happened during the auction. As with evidence that the auctioneer has not accepted appropriately submitted bids, evidence that she has not adequately maintained and made available committed bid histories would mean that the auction is subject to the high-sales-price sanction described above.

By using the notary at regular intervals, the auctioneer commits not only to the received bids, but to the order in which they are received. However, this limitation on reordering is only up to the notarization update interval. And, this is likely to be infrequent. Because submitted bids are protected by SBC until they are committed, the auctioneer has no way to distinguish valid bids unless bidders tell her. Thus, it may be of limited concern whether or not she can reorder the bids she cannot distinguish; although she can always list the bids of colluders ahead of those of others in any given interval, even if she cannot determine whether they are higher than the other bids or whose the other bids are.

Bid Submission To submit a bid, a registered bidder downloads the notarized history from the most recent interval (resorting to certified delivery only if necessary). The bidder then submits the bid. The first bid a bidder submits in an auction is different from the later bids. The first bid has the form

$$Bid = AuctionID, \langle Bidder\ ID, [h(parameters), \prec history_A, t_N \succ_N, bid\ amount]_{K_{bid}} \rangle_S$$

(Recall our notation: $\langle M \rangle_K$ indicates the SBC to a message M using a secret K .) The bid amount is indicated by the number of elements that are sent from a reverse hash chain. Reverse hash chains are now widely employed for various applications, such as micropayments. A reverse hash chain is formed by repeatedly hashing a random value some large number of times n . The first element

of the chain c_0 is then the n^{th} hash of the random value. As each link of the chain is revealed, it is easy to confirm that it is the next link by confirming that its hash is the most recent previously revealed link. So, for the first bid that a bidder submits in an auction

$$bid\ amount = c_0, (i, c_i).$$

The number of chain links revealed reflects the intended amount of the bid. Chain elements have a previously agreed value as part of the auction parameters.

We use $[M]_{K_{bid}}$ to indicate the signature of message M using signing key K_{bid} . The bid key K_{bid} binds the bid back to the bidder, so that the auctioneer can collect on the winning bid. (As noted above this binding may be indirect in various ways so as to protect the privacy of the bidder. The only essential characteristic is that the auctioneer can use this key to collect payment from the bidder, anonymously or otherwise.)

Here, t_N is the time given by the notary in the most recent notarized history submitted by the auctioneer, $history_A, t_N$. The auctioneer must commit to a bid by the end of the notarization interval following the one in which it was received. Of course in the interest of moving the auction along, she will want to commit to it as soon as possible; thus, she will include it in the history submitted for current notarization interval if possible. We will see presently that she can do still more in this respect.

In subsequently sent bids, there is no need for the bidder to sign the bid. Subsequent bids have the form

$$Bid = AuctionID, \langle Bidder\ ID, \prec\ history_A, t_N \succ_N, bid\ amount \rangle_S$$

In these bids,

$$bid\ amount = (j, c_j).$$

The amount of this bid is indicated by j : the bidder has bid j times the value of a chain link. There is no need to sign this since the auctioneer can always authenticate the bid by binding this back to K_{bid} via the hash chain. The auctioneer can thus show that the bidder has sent whatever total number of chain elements he has sent in that auction. But, the auctioneer cannot frame the bidder for a higher bid since she cannot produce the next unexposed chain element. Nor can she unpack the bid and claim it was for a lower amount since she will have committed to the bid before she knows the amount it contains. This also suffices to bind the bidder to the auction parameters.

The commitment that the auctioneer makes to a bid is contingent on the bidder sending his SBC secret (thus revealing his *Bidder ID* and the *bid amount*). For the bid to be valid, this must be done by the end of the notarization interval following the one in which the auctioneer commits to accepting the bid; although it can be done as soon as the bidder has evidence of the auctioneer's commitment to his bid. To provide this evidence between notarizations, the auctioneer can commit by herself signing (and posting) histories since the last notarization.

Once a bidder has downloaded the auctioneer’s signed commitment to a history, he can reveal his secret, even within the same notarization interval.

Just as with bids themselves, if necessary, a bidder should submit his SBC secret through a certified delivery service. The auctioneer should then send a certified response that commits receipt of the SBC secret. The need for certified delivery can be reduced by use of the auctioneer-signed histories just mentioned. To further minimize the need for certified delivery, the bidder should submit his SBC secret early in the interval in which it is due (or sooner if possible) and the auctioneer should sign and post a history including receipt of the SBC secret well before the end of the interval.

In [7] it was noted that since “open cry cyber auctions can take hours or days to conclude, the potential bidders will be hesitant to make such an open ended commitment to buy. Hence the Internet open cry auction mechanisms must give the bidder an opportunity to ask the seller for a commitment or withdraw his bid.” In our auction design, bidders cannot withdraw a complete committed bid; nonetheless, a bidder can decide not to reveal his SBC secret, even after the bid is committed by the auctioneer. This amounts to a limited bid-cancellation capability with an added advantage: if the bidder chooses to cancel the bid in this way, then the *Bidder ID* and *bid amount* are never revealed.

Closing the Auction In the published auction parameters there is an auction start time, an expiration time, and a regular timeout interval. The regular timeout interval is an interval during which no new bids that exceed the previous high bid are received. The auction must remain open until at least the expiration time has been passed. This time should be long enough that the item owner, or others, can determine whether the auctioneer is accepting bids and thus can send bids via a certified delivery service if necessary.

If more recently than the timeout interval before the expiration time any new high bids have been received, then a new timeout is set and auction continues until a timeout interval passes without a new high bid. It should be clear that someone waiting until the last moment to submit a bid (or SBC secret) must use a certified delivery service to be sure of receipt (or evidence of availability), even if the auctioneer has not shown any signs of failing to accept bids. The auction parameters should be set so that ordinary bidders paying reasonable attention to the auction should not be forced to resort to such means unless the auctioneer is not committing to bids.

In our auction design, the timeout interval must be at least as long as the notarization interval.

3.2 Auction Design Variants

Eliminating Regular Use of the Notary The above protocol makes only minimal use of (independent) trusted parties: certified delivery is used only when something does not function properly, and notarization is done only periodically. Still, it would be good to further limit the use of trusted parties to just those

times when something does not happen as it ordinarily should. We now sketch how to do so.

The reasons for the notary in our auction design are (1) to provide a non-repudiable record of the auctioneer's claimed auction history at the time of notarization, and (2) to provide a trusted time source on which the auctioneer and bidders must synchronize. We can use auctioneer signatures to provide a record of claimed auction history at a time stated by the auctioneer. But, how can we force synchronization of this time without regular use of the notary?

Bidders (and item owners) can use notaries and certified communication (which includes the time-stamp of a trusted authority) to catch the auctioneer in extreme clock skews. In the absence of a notarized history, the auctioneer should post her own time-stamped, signed histories at regular intervals. Bidders or item owners who want to keep the auction honest should now download and keep these so that the auctioneer cannot later produce a conflicting record and deny the previously posted record. (This was not necessary when the notary was used since the auctioneer could not later produce a conflicting *notarized* history.)

As before, if auction participants notice that the auctioneer has not posted an update within the current interval, they can request one by certified delivery. And, the auctioneer should respond with a post via certified delivery. Unlike before, participants must now watch for extreme clock skews on the part of the auctioneer. In this case, they should also download the posted history with the advanced clock and submit it for notarization (or perhaps post it via certified delivery). In this case the difference between the auctioneer's clock and the trusted clock of the notary will show that the auctioneer's clock is skewed beyond acceptable bounds (which should be stipulated in the auction parameters). The auction should then close using the high-sales-price sanction described earlier.

Temporarily Secret *Bid* Commitment Instead of using secret bit commitment in our auction, we could use temporarily secret bit commitment (TSBC) [17]. TSBC is similar to the notion of time-lock puzzles [12]. The basic idea is to commit to a secret that can be uncovered after a predictable amount of time. For example, the secret can be encrypted with a key that is recoverable after an inherently sequential computation of fixed length. Someone receiving such a message would be able to decrypt it after a fixed amount of computation. Nonetheless, the message is not readable until that computation has been performed. Thus, committing to receipt of a TSBC message is committing to the ability to read the message as well (after performing the computation). This removes the contingency of auctioneer commitment to a bid. It is not necessary to reveal any commitment secret.

Nonetheless, it would be good if it were possible to avoid performing that computation once the bid has been committed. If desired, the secret key can be revealed, providing a 'shortcut' access to the TSBC message. We could imagine features of the auction to make it likely that shortcuts to TSBC are revealed. Perhaps client software reveals the bid when proper conditions are met. There could be any number of carrots or sticks to further motivate bidders. A deposit

could be collected and returned at the end of the lottery if the client actually reveals all shortcuts. An auctioneer would not likely cheat to keep the deposit at the expense of tarnishing his image with the bidding community. Alternatively, bidders could be given a financial incentive (e.g., they could be entered in a lottery or provided with coupons or rebate offers).

The reason our default design uses SBC rather than TSBC is that, if despite the incentives and/or automation, shortcuts are not revealed for many bids, then a denial-of-service attack on auctioneer performance is possible.

4 Conclusion

We have presented properties of fair English auctions as well as a design for an on-line auction. In current on-line auctions, there are strong trust assumptions about auctioneers. Our auction design uses no specialized trusted parties, it uses only trusted parties that exist independently in the information infrastructure. And, use of those trusted parties is minimized: a notary is used only for periodic updates to insure fair closing conditions, while a certified delivery service is used only when ordinary communication fails or the auctioneer does not perform properly. (And, the auctioneer has disincentives both to not performing properly and to receiving certified deliveries.) In fact, in one of our variants, the notary also is only used when the auctioneer does not operate properly. Despite this minimal use of (only independent) trusted parties, we have been able to give informal arguments that our design meets the properties we set out. In sum, we have presented an auction design that provides for the fair close of an auction and makes bid refusal by the auctioneer provable by bidders and others.

References

1. Certmail: The Certified Electronic Mail System., www.certmail.com.
2. D. Chaum. "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms", *Communications of the ACM*, v. 24, n. 2, Feb. 1981, pages 84-88.
3. L. Cottrell. "Mixmaster and Remailer Attacks", <http://obscura.obscura.com/~loki/remailer/remailer-essay.html>.
Note: Mixmaster remailers are based on the original mix design of Chaum [2].
4. S. Feldman. "Research Directions in Electronic Commerce", Keynote address to the 3rd *USENIX Workshop on Electronic Commerce*, Boston, Mass. September 1998.
5. M. K. Franklin and M. K. Reiter, "The Design and Implementation of a Secure Auction Service", *IEEE Trans. on Software Eng.*, 22(5), May 1996, pp. 302-312.
6. J. Kilian and E. Petrank. "Identity Escrow", in *Advances in Cryptology—CRYPTO '98*, H. Krawczyk (ed.), Springer-Verlag, LNCS vol. 1462, pp. 169–185, 1998.
7. M. Kumar and S. Feldman. "Internet Auctions", 3rd *USENIX Workshop on Electronic Commerce*, Boston, Mass. September 1998, pp. 49-60.

8. M. Harkavy, J.D. Tygar and H. Kikuchi. "Electronic Auctions with Private Bids", *3rd USENIX Workshop on Electronic Commerce*, Boston, Mass. September 1998, pp. 61-73.
9. R. P. McAfee and J. McMillan, "Auctions and Bidding", *Journal of Economic Literature*, Vol 25, No. 2, June 1987, pp. 699-738.
10. Netdox, Inc., www.netdox.com.
11. M. Reed, P. Syverson, and D. Goldschlag. "Anonymous Connections and Onion Routing", *IEEE Journal on Selected Areas in Communications*, vol. 16 no. 4, May 1998, pp. 482-494. (More information and further publications at www.onion-router.net)
12. R. Rivest, A. Shamir, and D. Wagner. Time-lock puzzles and timed-release Crypto. Unpublished manuscript, February, 1996.
13. P. Sanders, S. Rhodes, and A. Patel, "Auctioning by Satellite using Trusted Third Party Security Services", *11th IFIP conference on Information Security*, 1995, pp. 205-219.
14. B. Schneier. *Applied Cryptography, Second Edition: Protocols, Algorithms and Source Code in C*, John Wiley and Sons, 1996.
15. S.G. Stubblebine, P.F. Syverson, and D.M. Goldschlag, "Unlinkable Serial Transactions: Protocols and Applications", forthcoming in *ACM Transactions on Information and System Security*, November 1999. (A preliminary version of this paper appears in [18].)
16. Surety Technologies, Inc., www.surety.com.
17. P. Syverson. "Weakly Secret Bit Commitment: Applications to Lotteries and Fair Exchange", *1998 IEEE Computer Security Foundations Workshop (CSFW11)*, Rockport Mass. June 1998, pp. 2-13.
18. P.F. Syverson, S.G. Stubblebine, and D.M. Goldschlag, "Unlinkable Serial Transactions", in *Financial Cryptography: FC '97, Proceedings*, R. Hirschfeld (ed.), Springer-Verlag, LNCS vol. 1318, pp. 39-55, 1998.
19. E. Turban. Auctions and bidding on the internet: An assessment. *International Journal of Electronic Markets*, 7(4), 1997, www.electronicmarkets.org.
20. P. Wayner. Digital Timestamps: Punching an Electronic Clock, *The New York Times on the Web: CyberTimes*, Jan. 10, 1999, www.nytimes.com/library/tech/99/01/cyber/articles/10notary.html.
21. www.auctioninsider.com/every.html (List of almost a hundred on-line auction houses.)