

Secure Online English Auctions

Author

Trevathan, J, Read, Wayne

Published

2006

Conference Title

Communications in Computer and Information Science

Version

Accepted Manuscript (AM)

DOI

[10.1007/978-3-540-70760-8_10](https://doi.org/10.1007/978-3-540-70760-8_10)

Rights statement

© Springer-Verlag Berlin Heidelberg 2008. This is the author-manuscript version of this paper. Reproduced in accordance with the copyright policy of the publisher. The original publication is available at www.springerlink.com

Downloaded from

<http://hdl.handle.net/10072/410658>

Griffith Research Online

<https://research-repository.griffith.edu.au>

Secure Online English Auctions

Jarrod Trevathan

School of Mathematical and Physical Sciences
James Cook University
jarrod.trevathan@jcu.edu.au

Abstract. Security and privacy in online auctions is a major concern as auction participants have many opportunities to cheat (e.g., repudiate bids, not deliver items, etc.). Online auctions such as those used by eBay are based on a type of auction referred to as an English auction. Despite the English auction being the most popular type of auction, it has received less security coverage than other types of auctions (e.g., sealed-bid auctions). An existing proposal for a “secure” English auction prevents the Auctioneer from closing the auction early and from blocking bids, but does not protect a bidder’s anonymity. Another proposal provides anonymity, but does not stop an Auctioneer from skewing its clock or blocking bids. This paper proposes a new scheme for conducting secure and anonymous online English auctions using a modified type of group signature. Trust is divided among three servers owned by separate companies to ensure anonymity and fairness. Our scheme solves the problems of the existing English auction schemes and has following characteristics: *unforgeability, anonymity, unlinkability, exculpability, coalition-resistance, verifiability, robustness, traceability, revocation, one-off registration, unskewability* and *unblockability*. Our scheme has comparable efficiency to the existing schemes for the enhanced security and privacy it provides.

Keywords: Online auctions, event timing, anonymity, group signature.

1 Introduction

Online auctioning is now widely accepted as one of the premiere means to do business on the web. English auctions are the most common type of online auction employed by Internet auctioneers (e.g., eBay¹ and uBid²). Such auctions are used to sell various items from real estate to football tickets. An English auction allows one seller to offer an item for sale. Many potential buyers then submit bids for the item attempting to outbid each other. The winner is the bidder with the highest bid after a given time-out period where no bid higher than the current highest bid has been made. The winner must pay the seller an amount equal to the winning bid.

Since the participants are not physically present in an online auction, there exist many security concerns and opportunities for people to cheat. For example, a bidder might repudiate having made a bid or the seller doesn’t deliver the item. Furthermore, the Auctioneer could influence the auction in a manner inconsistent with its rules (e.g., block

¹ <http://www.ebay.com>

² <http://www.ubid.com>

bids). Security and privacy in electronic auctions has been covered in [3,7,10,15,18], and numerous “secure” auction schemes have been proposed. However, most of the schemes presented so far have been for *sealed bid* auctions (i.e., bids remain secret until the close of bidding). An English auction on the other hand is an *open bid* auction (i.e., everyone knows the values of the bids). This combined with the nature of the auctioning process makes English auctions more complicated than regular cryptographic auction schemes.

The timing of events in English auctions is much more critical than sealed bid auctions. As a result, this presents some unique security risks. An English auction requires a real-time link between the bidders and the Auctioneer. Frequent price quotes are issued to update bidders regarding the current highest bid. As bidders base their decisions on this information, its timeliness directly influences the auction. A corrupt Auctioneer could disadvantage certain bidders by delaying this information or by speeding up (skewing) the clock in order to close the auction early. Furthermore, the speed and ease of the bid submission process is significant, especially when an auction is nearing its end. A malicious Auctioneer could selectively block bids based on bidder identity and/or bid value.

[13] presented an English auction scheme that prevents the Auctioneer from closing the auction early and from blocking bids. However it does not protect a bidder’s anonymity. Alternately, a scheme by [12] provides anonymity, but does not stop an Auctioneer from skewing its clock or blocking bids. We believe the short-comings of the existing schemes can be solved by basing the auction protocol on a modified group signature scheme.

The concept of group signatures was introduced by [6]. A group signature scheme allows members of a group to sign messages on behalf of the group, such that the resulting signature does not reveal the identity of the signer. Signatures can be verified with respect to a single group public key. Only a designated group manager is able to open signatures, and thus reveal the signer’s identity. Due to these unique security characteristics, group signature schemes have recently been used as the basis for auction protocols (see [16,17]).

This paper presents a scheme for conducting online English auctions in a secure and anonymous manner. The new scheme solves the problems of the existing proposals while maintaining all of their features. The role of the Auctioneer is divided among two auction servers (owned by separate companies) to ensure that the correct timing of events is maintained and to prevent bid blocking. (see [10].) Our scheme uses a group signature that is altered so that the role of the group manager is also divided among two independent auction servers. This allows for bid verification and protects a bidder’s identity unless the two servers collude. In the case of a dispute (e.g., a bidder repudiates a bid), a court order can be used to reveal the bidder’s identity and he/she can be permanently revoked from the auction proceedings. The scheme is flexible and allows the group signature to be updated as better techniques for group signatures become available. Our scheme offers comparable efficiency trade-offs for its enhanced security and privacy characteristics.

This paper is organised as follows: the remainder of this section discusses security issues inherent in English auctions and our contribution. Existing English auction

schemes and their shortcomings are discussed in Section 2. The components of our new scheme are introduced in Section 3 and the auction protocol is described in Section 4. An informal security analysis of the new scheme is given in Section 5. Section 6 presents an efficiency comparison of the new scheme and Section 7 provides some concluding remarks.

1.1 Fundamentals of Online English Auctions

There are four main activities in an online English auction:

Initialisation – The Auctioneer sets up the auction and advertises it i.e., type of good being auctioned, starting time, etc.

Registration – In order to participate in the auction, bidders must first register with the Auctioneer.

Bidding – A registered bidder computes his/her bid and submits it to the Auctioneer. The Auctioneer checks the bid received to ensure that it conforms with the auction rules.

Winner Determination – The Auctioneer determines the winner according to the auction rules. Online English auctions can terminate according to the following rules (see [8,13]):

1. *Expiration Time* - The auction closes at a predetermined expiration time.
2. *Timeout* - The auction closes when no bids higher than the current highest bid are made within a predetermined timeout interval.
3. *Combination of Expiration and Timeout* - The auction closes when there is a timeout after the expiration time.

1.2 Security Issues in Online English Auctions

The core security requirements for an English auction include:

Unforgeability - Bids must be unforgeable, otherwise a bidder can be impersonated.

Verifiability - There must be publicly available information by which all parties can be verified as having correctly followed the auction protocol. This should include evidence of registration, bidding and proof of the winner of the auction.

Exculpability - Neither the Auctioneer nor a legitimate bidder can forge a valid signature of a bidder.

Coalition-resistance - No coalition of bidders can frame an innocent bidder by fabricating a bid.

Robustness - The auction process must not be affected by invalid bids or by participants not following the correct auction protocol.

Anonymity - The bidder-bid relationship must be concealed so that no bidder can be associated or identified with the bid they submit.

One-time registration - Registration is a one-off procedure, which means that once a bidder has registered, they can participate in future auctions held by the Auctioneer.

Unlinkability - Bids are unlinkable within an auction, and also between plural auctions.

Traceability - Once a bidder has submitted a bid, they must not be able to repudiate having made it. Otherwise if a bidder wins and does not want to pay, they might deny that they submitted the winning bid. In this event the identity of the bidder who submitted the bid in question can be revealed.

Revocation - Malicious bidders can be easily revoked from all future auctions.

English auctions are open bid and the timely nature of the auction process therefore raises several further concerns. Due to the flexibility of closing rules for English auctions this introduces the following unique requirements:

Unskewability - The Auctioneer must not be able to alter the auction timing. For example, speed up its clock in an attempt to close the auction early, or slow the auction down to keep the bidding process active beyond the official timeout.

Unblockability - The Auctioneer cannot selectively block bids based on bid amount or the identity of the bidder.

Conditional bid cancellation - In online auctions using an expiration time, it is common for the auction to continue for days or weeks. In this situation a bidder might be reluctant to make such an open ended bid. Therefore depending on the closing rule and the stage of the auction it is desirable to allow bidders to conditionally cancel bids. Note that bidders should not be able to cancel bids when an auction is in a timeout stage and cancellation must only be done in strict accordance with the Auctioneer's bid cancellation policy.

2 Existing English Auction Schemes

Discussions regarding security for English auctions can be found in [8,16]. Several "secure" English auction schemes have been proposed by [9,11,12,13]. The first scheme is due to [13]. This scheme requires bidders to register with the Auctioneer. The Auctioneer must periodically timestamp the auction proceedings with a *Notary* to prove to bidders that it is not skewing its clock. Bidders submit bids using a reverse hash chain and secret bid commitments. This is done to ensure that the Auctioneer cannot block bids, and that bidders are not able to repudiate bids. The auction proceedings are recorded on a public bulletin board that is readable by everyone, but can only be written to by the Auctioneer.

We have identified the following problems with this scheme:

1. There is no anonymity for the bidders.
2. Bids are linkable, meaning that the Auctioneer can create profiles about individual bidders and their bidding strategies.
3. All parties must trust the Notary. (i.e., to ensure the correct timing is maintained.)

[12] refine a scheme by [11] that uses a form of modified group signature [1,5,6]. This scheme allows a bidder to register once and participate in any number of auctions held by the Auctioneer. Bids are claimed to be unlinkable between different auctions, but linkable within a particular auction. This is achieved by requiring the bidder to calculate a new signature generation key prior to each auction.

In this scheme there are two managers responsible for conducting the auction. The *Registration Manager* (RM) secretly knows the correspondence of the bidder's identity and registration key. RM works as an identity escrow agency. The *Auction Manager* (AM) hosts the auction and prepares bidder's auction keys in each round.

We have identified the following problems with this scheme:

1. All bidders must update their keys between each round of auctioning, which is essentially equivalent to re-registering. Therefore, this negates the author's claims that registration is a one-off procedure.
2. AM can skew its clock and/or selectively block bids.
3. Revoking a bidder is inefficient as it requires AM to reissue new keys to all of the existing bidders.
4. [9] describe a flaw in this scheme during the winner announcement stage. Here AM is able to erroneously inform any bidder that they have won without being publicly verifiable. Lee *et al.* propose a solution. However, this introduces several more bulletin boards and requires computations that are an order of magnitude slower.
5. Bids are linkable within a current auction, but unlinkable between plural auctions. The motivation for this is stated as the auction participants gain utility in terms of entertainment from viewing the auction. For example, when there is a rally between two particular bidders, observers enjoy knowing how many bids a bidder has submitted.

With regard to the last point, it is our opinion, that in an anonymous auction scheme all bids (whether in the same auction or not) must be totally unlinkable. Observers can still see a rally, however, there is no need to know exactly whom the bids are coming from. Our scheme described in the next section, does not allow bids to be linked within the same auction or between plural auctions.

3 Components of Our Scheme

The auction has four parties:

A *Bidder*, who is interested in buying an item from a seller in an English auction.

An *Auction Manager* (AM), who organises the auction proceedings, accepts bids and determines the winner according to whoever has submitted the highest bid. To participate in an auction, a bidder presents his/her real identity to AM. AM issues the bidder with a token that allows him/her to register.

A *Registration Manager* (RM), who takes part in the protocol in order to complete the registration of a bidder, once a token has been obtained from AM. At the end of the protocol, the bidder obtains a secret key that enables him/her to generate signed bids in a proper format.

An *Auction Helper* (AH), who aids AM in accepting bids and determining the winner. AH is owned by a separate company and is tasked with ensuring that AM does not alter its clock or block bids.

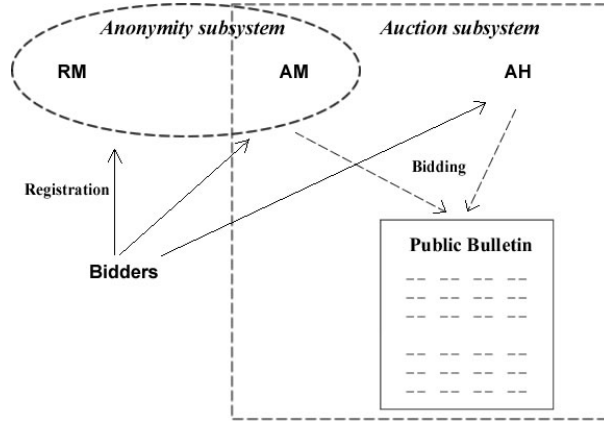


Fig. 1. The Auction Model

The scheme uses a two-server trust approach that can be broken down into two subsystems: the *anonymity subsystem* and the *auction subsystem* (see Figure 1). The anonymity subsystem protects the anonymity of the bidders provided the AM and RM do not collude. The auction subsystem ensures the correct outcome of the auction as long as AM and AH do not collude. There is no trust assumed between RM and AH.

Each bidder, AM and AH are connected to a common broadcast medium with the property that messages sent to the channel instantly reach every party connected to it. The broadcast channel is public so that everybody can listen to all information communicated via the channel, but cannot modify it. It is also assumed that there are private channels between RM and any potential bidders (who wish to join the auction proceedings).

3.1 Group Signatures

To join an auction, a bidder must first register with RM (who plays the role of a group manager in a group signature scheme). Once registered, a bidder can participate in the auction by signing bids using the group signature. Bids are submitted to an independent AM who runs the auction (with the help of AH which is explained later). AM (and AH) post the auction results on a publicly verifiable bulletin board.

One of the most efficient and popular proposals for group signature schemes is due to [1]. This is the group signature scheme that is used for the basis of our auction protocol. The [1] group signature scheme informally works as follows:

Let $n = pq$ be an RSA modulus, where p and q are two safe primes (i.e., $p = 2p' + 1$, $q = 2q' + 1$, and p' , q' are also prime numbers). Denote by $QR(n)$, the set of quadratic residues - a cyclic group generated by an element of order $p'q'$. The group public key is $\mathcal{Y} = (n, a, a_0, y = g^x, g, h)$, where a, a_0, g, h are randomly selected elements from $QR(n)$. The secret key of the group manager is x .

To join the group, a user (bidder i) must engage in a protocol with the group manager (i.e., RM and AM) and receive a group certificate $[B_i, e_i]$ where $B_i = (a^{x_i}, a_0)^{1/e_i} \text{ mod } n$

n with e_i and x_i chosen from two integral ranges as defined in [1]. (x_i is only known to the user/bidder).

In order to sign a message/bid, m , the user/bidder has to prove possession of his member certificate $[B_i, e_i]$ without revealing the certificate itself. More precisely, the user/bidder computes:

$$T_1 = B_i y^w \bmod n, T_2 = g^w \bmod n,$$

$$T_3 = g^{e_i} h^w \bmod n SK(m)$$

where the value $SK(m)$, computed over a message m , indicates a signature of knowledge of the secret key x_i and the e_i th root of the first part of the representation of T_3 (in the implementation of our scheme, the exact signature generation and verification procedures will be presented).

In the case of a dispute, the group manager can open a signature that reveals the identity of the signer. This is due to the fact that the pair (T_1, T_2) is an ElGamal encryption of the user's certificate (using the public key of the group manager). That is, the group manager can compute B_i , using $B_i = T_1 / (T_2)^x$.

In certain circumstances users must be revoked from the group. For example, a membership expires or a user misbehaves. Reissuing keys to all existing group members is unwieldy and inefficient for a large group. Using a certificate revocation list to blacklist malicious bidders requires the verifier of the signature to check a list that is linear in the number of revoked users.

[4] propose a scheme based on a dynamic accumulator that requires a member to prove that they have not been revoked. Informally, an *accumulator* is a method to combine a set of values into one short accumulator such that there is a short witness that a given value was incorporated into the accumulator. It is infeasible to find a witness for a value that is not in the accumulator. A *dynamic accumulator* allows values to be added and deleted from the accumulator at unit cost. By incorporating dynamic accumulators into a group signature scheme, revocation can easily be performed by deleting a member's value from the accumulator.

A user must check the accumulator prior to signing. This requires an online link between the group manager and the users. In terms of an auction, a bidder must check the accumulator each time they submit a bid. This is reasonable for English auctions, as there is a real-time communication link between the Auctioneer and bidders anyway.

The [4] dynamic accumulator scheme can be defined as follows: A dynamic accumulator for a family of inputs $\{\mathcal{X}_1\}$ is a family of families of functions $\{\mathcal{F}_1\}$ with the following properties:

Efficient generation: *There is an efficient probabilistic algorithm \mathcal{G} that on input 1^k produces a random element f of \mathcal{F}_k . Moreover, along with f , \mathcal{G} also outputs some auxiliary information about f , denoted aux_f .*

Efficient evaluation: *$f \in \mathcal{F}_k$ is a polynomial-size circuit that, on input $(u, k) \in \mathcal{U}_f \times \mathcal{X}_k$, outputs a value $v \in \mathcal{U}_f$, where \mathcal{U}_f is an efficiently-samplable input domain for the function f ; and \mathcal{X}_k is the intended input domain whose elements are to be accumulated.*

Quasi-commutative: For all k , for all $f \in \mathcal{F}_k$ for all $u \in \mathcal{U}_f$ for all $x_1, x_2 \in \mathcal{X}_k$, $f(f(u, x_1), x_2) = f(f(u, x_2), x_1)$. If $\mathcal{X} = \{x_1, \dots, x_m\} \subset \mathcal{X}_k$, then by $f(u, \mathcal{X})$ we denote $f(f(\dots(f(u, x_1), \dots), x_m))$.

Witness: Let $v \in \mathcal{U}_f$ and $x \in \mathcal{X}_k$. A value $w \in \mathcal{U}_f$ is called a witness for x in v under f if $v = f(w, x)$.

Addition: Let $f \in \mathcal{F}_1$, and $v = f(u, \mathcal{X})$ be the accumulator so far. There is an efficient algorithm A to accumulate a given value $x' \in \mathcal{X}_1$. The algorithm outputs:

1. $\mathcal{X}' = \mathcal{X} \cup \{x'\}$ and $v' = f(v, x') = f(u, \mathcal{X}')$;
2. w' which is the witness for $x \in \mathcal{X}$ in v' .

Deletion: Let $f \in \mathcal{F}_1$, and $v = f(u, \mathcal{X})$ be the accumulator so far. There exist efficient algorithms \mathcal{D}, \mathcal{W} to delete an accumulated value $x' \in \mathcal{X}$. The functionality of the algorithms includes:

1. $\mathcal{D}(aux_f, v, x') = v'$ such that $v' = f(u, \mathcal{X} \setminus \{x'\})$, and
2. $\mathcal{W}(w, x, x', v, v') = v'$ such that $f(w', x) = v'$, where $x \in \mathcal{X}$ and $f(w, x) = v$.

The [4] dynamic accumulator scheme is based on the strong RSA assumption and accumulates prime numbers (i.e., the primes used for the membership certificates in [1] group signature scheme). The scheme also provides a proof that a committed value was accumulated (we will omit these details). The construction of a dynamic accumulator where the domain of accumulated values consists of prime numbers, is as follows:

- F_k is the family of functions that correspond to exponentiating modulo-safe prime products drawn from the integers of length k . Choosing $f \in F_k$ amounts to choosing a random modulus $n = pq$ of length k , where $p = 2p' + 1$, $q = 2q' + 1$, and p, p', q, q' are all prime. We will denote f corresponding to modulus n and domain $\mathcal{X}_{A,B}$ by $f_{n,A,B}$.
- $\mathcal{X}_{A,B}$ is the set $\{e \in \text{primes} : e \neq p', q' \wedge A \leq e \leq B\}$, where A and B can be chosen with arbitrary polynomial dependence on the security parameter k , as long as $2 < A$ and $B < A^2$. $\mathcal{X}'_{A,B}$ is (any subset of) of the set of integers from $[2, A^2 - 1]$ such that $\mathcal{X}_{A,B} \subseteq \mathcal{X}'_{A,B}$.
- For $f = f_n$, the auxiliary information aux_f is the factorisation of n .
- For $f = f_n$, $\mathcal{U}_f = \{u \in QR_n : u \neq 1\}$ and $\mathcal{U}'_f = \mathbb{Z}_n^*$.
- For $f = f_n$, $f(u, x) = u^x \bmod n$. Note that $f(f(u, x_1), x_2) = f(u(x_1, x_2)) = u^{x_1 x_2} \bmod n$.
- Update of the accumulator value. Adding a value \tilde{x} to the accumulator value v can be done as $v' = f(v, \tilde{x}) = v^{\tilde{x}} \bmod n$. Deleting a value \tilde{x} from the accumulator is as follows: $\mathcal{D}((p, q), v, \tilde{x}) = v^{\tilde{x}-1 \bmod (p-1)(q-1)} \bmod n$.
- Update of a witness. Updating a witness u after \tilde{x} has been added can be done by $u' = f(u, \tilde{x}) = u^{\tilde{x}}$. In case, $\tilde{x} \neq x \in \mathcal{X}_k$ has been deleted from the accumulator, the witness u can be updated as follows. By the extended GCD algorithm, one can compute the integers a, b such that $ax + b\tilde{x} = 1 \bmod n$ and then $u' = \mathcal{W}(u, x, \tilde{x}, v, v') = u^b v'^a$.

4 The Auction Protocol

This section describes the auction protocol. A high level view of the protocol is given in Figure 2. Lines depict communication between parties while the dashed circles indicate

stages in the protocol. Lines that pass through the dashed circles are communications that are performed during the particular stage.

4.1 Setup

Most activities of this stage need to be performed only once (in order to establish the auction proceedings). Let $\lambda_1, \lambda_2, \gamma_1$, and γ_2 be some lengths, Λ, Γ be some integral ranges, and $\mathcal{H}(\cdot)$ be a collision-resistant hash function. RM sets up the group public key and his secret key by performing the following steps:

1. Chooses two safe primes p and q (i.e., $p = 2p' + 1$ and $q = 2q' + 1$, where p' and q' are prime numbers) and sets the RSA modulus $n = pq$
2. Chooses random elements $a, a_0, g, h \in QR(n)$
3. Chooses a secret element $x \in_R \mathbb{Z}_{p'q'}^*$ and sets $y = g^x \pmod n$
4. Publishes the group public key as $\mathcal{Y} = (n, a, a_0, y, g, h)$
5. Creates the public modulus n for the accumulator, chooses a random $u \in QR_n$ and publishes (n, u)
6. Set up (empty for now) public archives E_{add} for storing values that correspond to added users and E_{delete} for storing values that correspond to deleted users

4.2 Registration

A user submits a request to AM to participate in the auction proceedings. AM verifies the identity of the requestor, and issues a token that is verifiable by RM. The user then takes part in a protocol with RM, in order to obtain his/her secret key and a certificate of membership in the auction proceedings. Note that the token does not carry the real identity of the bidder. All communication between RM and the owner of a token is authenticated and recorded. The protocol between a new bidder i , and RM is as follows (checks in which values are chosen from proper intervals, the user knows discrete logarithms of values, etc. are omitted):

1. Bidder i selects random exponents x'_i, r and sends $C_1 = g^{x'_i} h^r \pmod n$ to the RM
2. RM checks that $C_1 \in QR(n)$. If this is the case, RM selects random values α_i, β_i and sends them to bidder i
3. Bidder i computes $x_i = 2^{\lambda_1} + (\alpha_i x'_i + \beta_i \pmod{2^{\lambda_2}})$ and sends to RM the value $C_2 = a^{x_i} \pmod n$
4. RM checks that $C_2 \in QR(n)$. If this is the case, RM selects a random $e_i \in \Gamma$ and computes $B_i = (C_2 a_0)^{1/e_i} \pmod n$ then sends the membership certificate $[B_i, e_i]$ to bidder i (note that $B_i = (a^{x_i} a_0)^{1/e_i} \pmod n$)
5. Bidder i verifies that $a^{x_i} a_0 = B_i^{e_i} \pmod n$
6. Add the current u to the bidder's membership certificate. Update $u: u = f_n(u, e_i)$. Update E_{add} : store e_i there
7. Verify that $f_n(u_i, e_i) = u_i^{e_i} = u$

RM creates a new entry in the membership table and stores bidder i 's membership certificate $[B_i, e_i]$ and a transcript of the registration process in this location.

4.3 Setup - Before Each Auction

AM organises the auction (i.e., advertising and calls for auction). AM posts information to the bulletin board regarding the auction including the auction id (which uniquely identifies the auction), the reserve price (minimum winning price that will be accepted), the auction starting time and the auction closing rules.

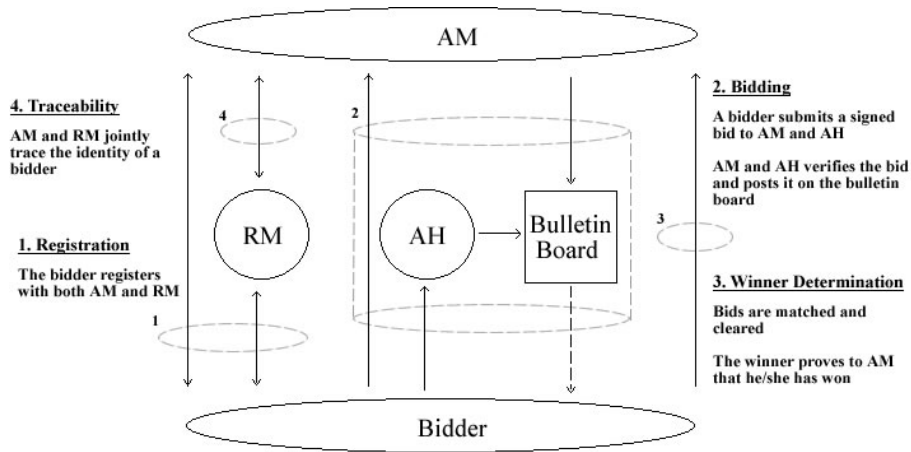


Fig. 2. The Auction Protocol

4.4 Bidding

Using a membership certificate $[B_i, e_i]$, a bidder can generate anonymous and unlinkable group signatures on a bid m . m contains the auction id and the amount of the bid (i.e., $m = id \parallel \text{bid value}$). Bidder i submits a bid m to both AM and AH signed using his/her secret key.

Update Membership - Prior to submitting a bid, a bidder must check if there have been any changes to the group (i.e., new bidders have been added, or other bidders have been revoked). If this is the case, a bidder must perform a membership update. This is done as follows:

An entry in the archive is called “new” if it was entered after the last time bidder i performed an update.

1. Let y denote the old value of u
2. For all new $e_j \in E_{add}$, $u_i = f(u_i, \prod e_j) = u_i^{\prod e_j}$ and $y = y^{\prod e_j}$
3. For all new $e_j \in E_{delete}$, $u_i = W(u_i, e_i, \prod e_j, y, u)$ (Note that as a result $u = f(u_i, e_i)$)

Sign Bid - In order to generate a signature on a message/bid, m , bidder i performs the following:

1. Chooses a random value w and computes:

$$T_1 = B_i y^w \bmod n, \quad T_2 = g^w \bmod n,$$

$$T_3 = g^{e_i} h^w \bmod n$$

2. Chooses r_1, r_2, r_3, r_4 (randomly) from predetermined intervals and computes:

- (a) $d_1 = T_1^{r_1}/(a^{r_2} y^{r_3})$, $d_2 = T_2^{r_1}/(g^{r_3})$, $d_3 = g^{r_4}$, and $d_4 = g^{r_1} h^{r_4}$ (all in mod n),
- (b) $c = \mathcal{H}(g \parallel h \parallel y \parallel a_0 \parallel a \parallel T_1 \parallel T_2 \parallel T_3 \parallel d_1 \parallel d_2 \parallel d_3 \parallel d_4 \parallel m)$,
- (c) $s_1 = r_1 - c(e_i - 2^{\xi_1})$, $s_2 = r_2 - c(x_i - 2^{\lambda_1})$, $s_3 = r_3 - ce_i w$, and $s_4 = r_4 - cw$ (all in \mathbb{Z}).

3. In addition to T_1, T_2 , and T_3 the bidder computes the values $C_e = g^e h^{r_1}$, $C_u = u h^{r_2}$, and $C_r = g^{r_2} h^{r_3}$ and sends them to AM, with random choices $r_1, r_2, r_3 \in_R \mathbb{Z}_{[n/4]}$

4. The output is

$$(c, s_1, s_2, s_3, s_4, r_1, r_2, r_3, r_4, T_1, T_2, T_3, C_e, C_u, C_r)$$

Prove Membership/Verify Bid - AM and AH check the validity of the bidder's signature using the group's public key \mathcal{Y} . A bid of the correct form is considered to be valid and is included in the auction (i.e., posted on the bulletin board). An invalid bid is discarded. There are two copies of the bid on the bulletin, one posted by AM and the other posted by AH. AM and AH verify the signature on the bid as follows:

1. Compute (all in mod n):

$$c' = \mathcal{H}(g \parallel h \parallel y \parallel a_0 \parallel a \parallel T_1 \parallel T_2 \parallel T_3 \parallel (a_0^c T_1^{(s_1 - c2^{\xi_1})}) / (a^{s_2 - c2^{\lambda_1}} y^{s_3}) \parallel (T_2^{s_1 - c2^{\xi_1}}) / (g^{s_3}) \parallel T_2^c g^{s_4} \parallel T_3^c g^{s_1 - c2^{\xi_1}} h^{s_4} \parallel m)$$

2. AM, AH and the bidder engage in a protocol to prove membership (see [4] for details)
3. Accept the signature if and only if $c = c'$, and the parameters s_1, s_2, s_3, s_4 lie in the proper intervals

Bid Cancellation - If a bidder desires to cancel a bid, they must send a copy of the bid they wish to cancel and a CANCEL message signed using his/her group key to both AM and AH. Upon receiving the CANCEL message, AM and AH check the bidder's signature on the message using the group's public key \mathcal{Y} . If the signature is valid, AM and AH then check what stage the auction is in. If the auction close rule is currently in an expiration time stage, AM and AH each post a message to the bulletin stating that the particular bid has been cancelled. If the auction is currently in a timeout stage, the CANCEL message is discarded and the bid remains in effect.

4.5 Winner Determination

Once the auction has closed, AM and AH then determine the auction outcome according to which bidder has made the highest bid. The winning bidder can produce a copy of the signed bid as evidence that they have won.

4.6 Traceability

In the event of a dispute, RM (with the help of AM) can open the signature on a bid to reveal which bidder is the original signer. This process is as follows:

1. Check the signature's validity via the verification procedure
2. Recover B_i (and thus the identity of bidder i) as $B_i = T_1/T_2^x \bmod n$

RM then checks the registration transcripts, and determines the token associated with this certificate. AM, who knows the relation between tokens and real identities, can determine the identity of the bidder. Note that in our scheme, revealing the identity of a bidder does not reveal any information about his/her past bids.

4.7 Revocation

When a bidder has been caught breaking the auction rules, they can be permanently revoked from the auction proceedings by cancelling the bidder's ability to sign future bids. To achieve this, the bidder's prime number used in his/her membership certificate is not included when the dynamic accumulator is updated. This can be done as follows: Retrieve e_i which is the prime number corresponding to the bidder's membership certificate. Update u : $u = \mathcal{D}(\psi(n), u, e_i)$. Update E_{delete} : store e_i there.

5 Security

This section provides an informal security analysis of the online English auction scheme presented in this paper based on the characteristics described in Section 1.2.

Unforgeability - Only bidders that are members of the group are able to sign messages on behalf of the group. This is due to the unforgeability of the underlying group signature.

Anonymity - Given a valid signature $(c, s_1, s_2, s_3, s_4, T_1, T_2, T_3)$ identifying the actual signer is computationally difficult. Determining which bidder with certificate $[B_i, e_i]$ has signed a bid, requires deciding whether the three discrete logarithms $\log_y T_1/B_i$, $\log_g T_2$, and $\log_g T_3/g^{e_i}$ are equal. This is assumed to be infeasible under the decisional Diffie-Hellman assumption, and thus anonymity is guaranteed. Note that in our auction, RM can figure out the certificate associated with each signature, but cannot determine the identity of the bidder associated with this certificate.

Table 1. Comparison of English auction schemes

	SS99	OM001	Our Scheme	TX03
Registration	1 exp.	480 mul.	30 exp.	2 exp.
Signing	1 exp.	240 mul.	25 exp.	17 exp.
Verification	1 exp.	320 mul.	21 exp.	16 exp.
Revocation	N/A	$O(\ell)$	$O(1)$	$O(1)$

Unlinkability - Deciding if two signatures $(c, s_1, s_2, s_3, s_4, T_1, T_2, T_3)$ and $(\tilde{c}, \tilde{s}_1, \tilde{s}_2, \tilde{s}_3, \tilde{s}_4, \tilde{T}_1, \tilde{T}_2, \tilde{T}_3)$ were computed by the same bidder is computationally hard (with the same argument as for anonymity).

Exculpability - Neither a bidder nor AM, AH and/or RM can sign on behalf of another bidder. This is because the secret key x_i , associated to user i is computationally hidden from RM. RM, at most, can learn $a^{x_i} \bmod n$, which cannot help him to learn the exponent x_i (since the discrete logarithm over the safe composite modulo n , is difficult).

Coalition-resistance - This is due to the following theorem: [1] Under the strong RSA assumption, a group certificate $[B_i = (a^{x_i} a_0)^{1/e_i} \bmod n, e_i]$ with $x_i \in \Lambda$ and $e_i \in \Gamma$ can be generated only by the group manager provided that the number K of certificates the group manager issues is polynomially bounded.

Verifiability - All bids (including signatures) are posted to the public bulletin, therefore all parties can verify the auction outcome.

Robustness - Invalid bids will not be posted to the bulletin board. Moreover, malicious bidders will be revoked from the system, and thus cannot affect the auction outcome.

Traceability - RM is always able to open a valid signature and, with the help of AM, identify the signer of the bid.

Revocation - Bidders can be easily revoked from the future auctions if they have broken the auction rules. See theorem 2 in [4].

One-time registration - Once a bidder has received a signature generation key, they are free to participate in future auctions.

Unskewability - AH observes AM's clock (and vice versa) therefore any clock skews will not go unnoticed. AM's clock can be trusted as long as both AM and AH do not collude.

Unblockability - A bidder must submit his/her bids to both AM and AH, who post the bid on the bulletin board. If either tries to block a bid, then only one confirmation of the bid will be posted to the bulletin board which will indicate that one of the parties has blocked a bid. Bids cannot be blocked unless AM and AH collude.

Conditional bid cancellation - Bidders can conditionally cancel bids by sending a CANCEL message to AM and AH as long as the auction is not in a timeout stage.

6 Efficiency

This section discusses the efficiency considerations of the new scheme. We contrast our approach with the existing English auction schemes. Table 1 shows the amount of work performed during each major stage of the auction in terms of the number of modular exponentiations (exp) or multiplications (mul) required. The schemes compared include: [13] (SS99), [12] (OM01), our scheme, and [14] (TX03). ([14] is an alternate implementation of our approach.)

The registration, signing and verification procedures for SS99 are relatively efficient. However, SS99 do not protect a bidder's identity, nor do they discuss revocation issues. To incorporate revocation into this scheme, it is likely that the registration procedure would have to be repeated between auctions. Furthermore, SS99 do not address the issue of one-time registration. Once again bidders would have to repeat the registration process for each auction they want to participate in.

OM01 is significantly less efficient than SS99. OM01 does not address bid cancellation whereas SS99 does. Furthermore, OM01 does not prevent the Auctioneer from skewing its clock. However, OM01 protects a bidders identity and addresses one-time registration. The cost of one-time registration in OM01 is issuing new keys to bidders between auctions, which is essentially equivalent to re-registering. The revocation method in OM01 is tied in with the one-time registration mechanism and therefore must also be repeated between each auction. To revoke a bidder requires the Auctioneer to perform work proportional to $O(\ell)$ where ℓ is the number of bidders.

In contrast, our scheme has the most practical one-time registration procedure. That is, once a bidder has registered, there is no work required to retain membership other than regularly checking the accumulator. We address bid cancellation, clock-skewing and privacy concerns. To revoke a bidder, the Auctioneer only has to update the accumulator. Bidders must check the accumulator value prior to each bid which is a constant operation. Our auction scheme can also be implemented using TX03 which has significant efficiency gains.

The efficiency of our scheme is comparable to the existing proposals. First of all our scheme has an enhanced set of security requirements that are much more comprehensive. Furthermore, our scheme clearly has the most efficient revocation method. In addition, we have the most practical one-time registration procedure.

7 Conclusions

This paper presented a scheme for conducting secure and anonymous online English auctions. Such a scheme is vital for protecting the security and anonymity of participants who engage in online auctioning. The timeliness of information and verifiability of the Auctioneer's actions is critical in an online English auction. We have shown that the existing "secure" English auction schemes are inadequate for the task. The scheme by [13] does not provide anonymity for the bidders and requires all parties to trust a public Notary. The scheme by [12] does not prevent an Auctioneer from skewing his/her clock or from blocking bids.

In direct contrast, our scheme solves all of the problems of the existing schemes and has a more comprehensive set of security requirements. We use a group signature to provide verification of bids and to protect the identities of bidders. The group signature is modified so that the identity of a bidder is divided among two separate parties (i.e., the anonymity subsystem). The role of the Auctioneer is also divided among two parties to prevent clock-skewing and bid-blocking (i.e., the auction subsystem). The scheme has comparable efficiency to the existing proposal for its enhanced security and privacy characteristics. The efficiency and security of the scheme rests with the underlying group signature scheme used. Our approach offers the client flexibility in choosing from any group signature scheme. The scheme offers efficient one-time registration and revocation procedures that are clearly better suited to handling multiple auctions than existing proposals.

References

1. Ateniese, G., Camenisch, J., Joye, M., Tsudik, G.: A Practical and Provably Secure Coalition-Resistant Group Signature Scheme. In: Bellare, M. (ed.) CRYPTO 2000. LNCS, vol. 1880, pp. 255–270. Springer, Heidelberg (2000)
2. Ateniese, G., Song, D., Tsudik, G.: Quasi-Efficient Revocation of Group Signatures. In: FC 2002. LNCS, vol. 2357, pp. 183–197. Springer-Verlag, Heidelberg (2002)
3. Boyd, C., Mao, W.: Security Issues for Electronic Auctions, Technical Report, Hewlett Packard, TR-HPL-2000-90 (2000)
4. Camenisch, J., Lysyanskaya, A.: Dynamic Accumulators and Application to Efficient Revocation of Anonymous Credentials. In: Yung, M. (ed.) CRYPTO 2002. LNCS, vol. 2442, pp. 61–76. Springer, Heidelberg (2002)
5. Camenisch, J., Stadler, M.: Efficient Group Signature Schemes for Large Groups. In: Kaliski Jr., B.S. (ed.) CRYPTO 1997. LNCS, vol. 1294, pp. 410–424. Springer, Heidelberg (1997)
6. Chaum, D., van Heyst, E.: Group Signatures. In: Davies, D.W. (ed.) EUROCRYPT 1991. LNCS, vol. 547, pp. 257–265. Springer, Heidelberg (1991)
7. Franklin, M., Reiter, M.: The Design and Implementation of a Secure Auction Service. IEEE Transactions on Software Engineering 22, 302–312 (1996)
8. Kumar, M., Feldman, S.: Internet Auctions. In: Proceedings of the Third USENIX Workshop on Electronic Commerce, pp. 49–60 (1998)
9. Lee, B., Kim, K., Ma, J.: Efficient Public Auction with One-Time Registration and Public Verifiability. In: Pandu Rangan, C., Ding, C. (eds.) INDOCRYPT 2001. LNCS, vol. 2247, pp. 162–174. Springer, Heidelberg (2001)
10. Naor, M., Pinkas, B., Sumner, R.: Privacy Preserving Auctions and Mechanism Design. In: The 1st ACM Conference on Electronic Commerce, pp. 129–139 (1999)
11. Nguyen, K., Traore, J.: An On-line Public Auction Protocol Protecting Bidder Privacy. In: Clark, A., Boyd, C., Dawson, E.P. (eds.) ACISP 2000. LNCS, vol. 1841, pp. 427–442. Springer, Heidelberg (2000)
12. Omote, K., Miyaji, A.: A Practical English Auction with One-Time Registration. In: Varadharajan, V., Mu, Y. (eds.) ACISP 2001. LNCS, vol. 2119, pp. 221–234. Springer, Heidelberg (2001)
13. Stubblebine, S., Syverson, P.: Fair On-Line Auctions without Special Trusted Parties. In: Franklin, M.K. (ed.) FC 1999. LNCS, vol. 1648, pp. 230–240. Springer, Heidelberg (1999)
14. Tsudik, G., Xu, S.: Accumulating Composites and Improved Group Signing. In: Lai, C.-S. (ed.) ASIACRYPT 2003. LNCS, vol. 2894, pp. 269–286. Springer, Heidelberg (2003)
15. Trevathan, J.: Security, Anonymity and Trust in Electronic Auctions. Association for Computing Machinery Crossroads, Spring Edition, 11(3), 3–9 (2005)
16. Trevathan, J., Ghodosi, H., Read, W.: Design Issues for Electronic Auctions. In: 2nd International Conference on E-Business and Telecommunication Networks, pp. 340–347 (2005)
17. Trevathan, J., Ghodosi, H., Read, W.: An Anonymous and Secure Continuous Double Auction Scheme. In: 39th International Hawaii Conference on System Sciences, vol. 125, pp. 1–12 (2006)
18. Viswanathan, K., Boyd, C., Dawson, E.: A Three Phased Schema for Sealed Bid Auction System Design. In: Clark, A., Boyd, C., Dawson, E.P. (eds.) ACISP 2000. LNCS, vol. 1841, pp. 412–426. Springer, Heidelberg (2000)