An Anonymous and Secure Continuous Double Auction Scheme

Jarrod Trevathan
*School of Mathematical and
 Physical Sciences*
James Cook University
 Email: jarrod.trevathan@jcu.edu.au

Hossien Ghodosi
School of Information Technology
James Cook University
 Email: hossein@cs.jcu.edu.au

Wayne Read
*School of Mathematical and
 Physical Sciences*
James Cook University
 Email: wayne.read@jcu.edu.au

Abstract

A Continuous Double Auction (CDA) allows many buyers and sellers to continuously submit bids for the purchase and sale of a commodity (e.g., online share trading). Protocols protecting privacy in this type of powerful market mechanism are essential. However, until recently the security of CDAs has been given limited coverage. This paper describes a new scheme for conducting an anonymous and secure CDA. We show that any existing secure group signature scheme can be used to implement a CDA which has the following characteristics: unforgeability, anonymity, unlinkability, exculpability, coalition-resistance, verifiability, robustness and traceability. Furthermore, bidders can be added to and removed from the auction without affecting the process of the auction. Our scheme is more flexible than the only existing secure CDA scheme, which in contrast provides only a limited subset of these characteristics.

I. Introduction

An auction is an exchange mechanism where many potential buyers submit bids for a commodity, which is usually awarded to the highest bidder. The Auctioneer accepts bids on behalf of the seller of the commodity and determines the winner according to the auction rules.

An auction that has only one seller and many buyers is referred to as a *single* auction. A *Continuous Double Auction (CDA)* allows for many buyers and sellers to continuously submit bids for the purchase and sale of a commodity. The most well known use for CDAs is in share markets.

In recent years, several companies have emerged that offer auctioning services via an online network such as eBay¹ and OnSale². These types of auctions have geographical advantages over traditional auctions, as sellers and buyers need not be physically present at a central location during the auction proceedings. This allows for larger and more elaborate auctions, which reach many more bidders than traditional auctions. However, it also allows the participants to cheat.

It is well documented that major security problems in online auctions exist (e.g., see [7], [17], [18], [20]). For example, buyers and sellers might be in collusion, repudiate bids, or not pay for/deliver the item bid upon. Alternately, the Auctioneer might be corrupt and award the auction to someone other than the legitimate winner. A further significant issue is how to protect a bidder's identity and bidding information.

An emerging aspect of electronic auctions is the ability to trade shares on the Internet. This is done using a brokerage

site such as Commsec³. A broker submits buy and sell bids to the Auctioneer running a CDA. Present brokers only offer trivial security measures such as issuing a client with a user name and password, and encrypting trading sessions. During this process much information about a client's identity and bidding pattern is released to the public. In terms of a share market, certain information is required by law to be available to authorised parties. Beyond this, it is the right of the bidder to have his/her anonymity protected.

Privacy is a desirable requirement in online trading for numerous reasons. Firstly, it prevents the Auctioneer from selectively blocking bids, based on the identity of a bidder. Secondly, many banking institutions tend to sell client's information to advertising agencies. Finally, share trading can be much more controversial than normal auctioning. For example, there may be legal/industrial disputes, bankruptcies, criminal behaviour (insider trading), etc. In such cases, there must be measures to protect an individual's anonymity (or revoke it when required).

Coverage exists regarding different CDA models (see e.g., [8], [9]) and bidding strategies (see e.g., [10], [16]). However, security and anonymity in CDAs has been given limited attention. Wang and Leung's scheme [21], to our knowledge, is the only auction scheme proposed that specifically addresses CDA security. In their CDA scheme, trust is divided amongst two separate servers in order to protect a bidder's anonymity. However, we have discovered that this scheme allows the identity of a bidder to be revealed immediately after his/her first bid. Furthermore, it allows profiles to be created about a bidder's trading behaviour, as bids are linkable. In this paper, we propose a secure CDA scheme to fix these problems.

This paper is organised as follows: In the remainder of this section we describe the fundamentals of electronic auctions, general electronic auction security and our contribution to CDA security. In Section II, we will review Wang and Leung's scheme, and describe issues specific to CDAs. In Section III, we will discuss the components of our new CDA scheme including the communication model, parties involved in the system, and cryptographic building blocks employed in our scheme. Section IV outlines the protocol for our CDA. In Section V, we will discuss security issues for the proposed CDA. Section VI gives an efficiency comparison of Wang and Leung's scheme to several different implementations of our

¹<http://www.ebay.com>

²<http://www.onsale.com>

³<http://www.commsec.com.au>

scheme.

A. Electronic Auction Fundamentals and Security Issues

The main activities fundamental to any electronic auction are:

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. This ensures that only valid bids are made, and that bidders can be identified for payment purposes.

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. It is desirable that the determination of the auction winner can be publicly verified.

The security requirements for an electronic auction are numerous. In general, core requirements include that the Auctioneer must determine the correct winner according to the auction rules; the winner must receive the item from the Seller; the Seller must receive payment in full from the winning bidder; and no bidder should have more information than any other to determine his/her bid. The final requirement is especially true in CDAs, where insider trading is considered an offence. Discussions regarding auction security can be found in [3], [7], [13], [20]. The following outlines the general security goals for electronic auctions:

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

Non-Repudiation – Once a bidder has submitted a bid, they must not be able to repudiate having made the relevant bid. Otherwise, if a bidder wins and does not want to pay they might deny that they submitted the winning bid.

Public 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.

Robustness – The auction process must not be affected by invalid bids nor 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.

Auctions can be classified according to whether the bids are *sealed* or *open*. In a sealed bid auction, bidders submit their bids during a bidding round. The bid values remain sealed (i.e., no one else knows what the bid values are) until a winner determination round. Open bid auctions on the other hand allow everyone to know the value of everyone else's bids. Sealed bid auctions introduce their own unique security concerns which have been well-documented in existing literature (see [7], [13], [20]). However, CDAs are open bid, therefore no one gains any advantage by knowing the values of other people's bids. In

fact it is essential for CDAs to provide information regarding market depth (i.e., list of buy/sell bids and their values) to the participants, in order to facilitate the bidding process.

B. New CDA Results and our Contribution

In this paper we present a new proposal for conducting anonymous and secure CDAs. We show that the CDA scheme by Wang and Leung is inadequate and describe several concerns regarding its security and anonymity claims. Furthermore, we explain how any existing secure group signature scheme can be used to provide anonymity and security for a CDA.

Chaum and van Heyst [6] introduced the concept of group signatures. 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 their identity. Signatures can be verified with respect to a single group public key, while hiding the identity of the signer. Only a designated group manager is able to open signatures, and thus reveal the signer's identity.

Since its invention, group signatures have been the subject of investigation by many authors. Camenisch and Stadler [5] present the first efficient group signature scheme, where the size of the group's public key, and the signatures, are independent from the number of group members. Furthermore, the group's public key remains unchanged if a new member is added to the group. Group signatures have desirable properties which makes them ideal for use in electronic auctions.

By incorporating a group signature scheme, our CDA provides the following characteristics:

Unforgeability – Only registered bidders can issue a bid.

Anonymity – The identity of a bidder remains anonymous (i.e., a bidder cannot be associated with the bid s/he has submitted). However, the value of the bid is still available to others (i.e., open bid).

Unlinkability – No party can form a profile about a bidder's bidding strategy based on past bids.

Traceability – In case of dispute and/or to determine the winner of the auction, the authorities (e.g., the Registrar and Auctioneer, cooperatively) are always able to identify the bidder.

Exculpability – No party—even the Registrar and Auctioneer—can issue a bid on behalf of any other bidder.

Coalition-resistance – A colluding subset of registered bidders cannot issue a bid that cannot be linked back to one of the colluding bidders.

Verifiability – All auction participants can be verified as having followed the protocol correctly.

Robustness – Invalid bids or failures in following the protocol does not affect the overall auction outcome.

Revocation – Bidders can be easily revoked from the CDA if they have broken the rules.

Note that our CDA scheme has more security characteristics than those outlined in Section I-A (i.e., unlinkability, traceability, exculpability, coalition-resistance and revocation). CDAs are quite unique compared to more conventional types

of auctions and the reasons for these additional security requirements will become apparent once we examine an existing secure CDA proposal.

II. Existing CDA Scheme

Wang and Leung's scheme [21] is the first attempt to conduct secure CDAs while preserving the anonymity of bidders. In Wang and Leung's CDA, there are two authorities, the Registration Manager (RM) and the Market Manager (MM). Before entering the CDA market, each bidder must register with both RM and MM. RM holds the corresponding relation of the identity and the certificate of bidders. MM verifies the certificate and issues a pseudonym for the bidder.

Registration with RM in [21] -

Suppose RM uses the RSA system with public parameters n, e as the RSA modulo and the encryption key, respectively. Let d be the corresponding private key in the RSA system and $H(\cdot)$ be an appropriate hash function. Denote by $\Omega_x(m)$ the set $\{m, \sigma_x(H(m))\}$, that is a message, m , and the signature of party x on $H(m)$. Also, let a bidder, b_i , possess a certified encryption/decryption key pair. The registration protocol between b_i and RM is shown in Table I (note that $\|$ denotes concatenation).

After registration with RM, the bidder must register with MM. Table II illustrates the protocol between MM and bidders.

Upon obtaining the certificate from MM, the bidder b_i submits their bid in the form $\{\text{offer}, \sigma_{b_i}(\text{offer}), \text{Cert}_{b_i}\}$, where $\text{offer} = \{p_{b_i}, \text{Buy/Sell}, \text{Commodity}, \text{Value}, \text{Timestamp}\}$, and p_{b_i} is a temporary public-key (or the pseudonym) associated with bidder b_i .

A. Analysis of Wang-Leung's Scheme

- 1) During registration with MM, the bidder forms the message M_4 , which contains the message M_2 as the first component. However, M_2 is formed as $\Omega_{RM}(ID_{b_i} \| sn)$ (i.e., it contains the identity of bidder b_i). Therefore, MM immediately learns the true identity of b_i .
- 2) Bids are linkable in this scheme, as the same pseudonym is used for each bid. This allows profiles to be created about bidders.
- 3) It is unclear how this scheme identifies winners. After the first trade (i.e., the first time a bidder wins) the identity of the bidder (associated with its pseudonym) is disclosed, and thus, later bids issued by this bidder are not anonymous.
- 4) When a bidder's identity has been traced, this scheme reveals the values of all past bids they have made. This is undesirable if there is no reason to doubt the validity of the guilty bidder's previous bids.

B. Further Problems - Procrastinating Attack

Even if the protocol by Wang and Leung is fixed, anonymity cannot be achieved in this model. In this section we will propose a procrastinating attack that can be used to immediately reveal a bidder's true identity after registration.

However, before we outline the attack, we must first examine the basic components of an auction. In a traditional auction model, there are two parties (excluding the Seller):

- 1) The Auctioneer, who organises the auction, accepts the bids on behalf of the seller of the commodity, and determines the winner according to the auction's rules.
- 2) The Bidder, who computes his/her bid and submits it to the Auctioneer, attempting to win the commodity according to the auction's rule.

This simple model works based on the assumption that the Auctioneer is trustworthy. However, the major problem in electronic auction protocols is to protect bidders from a corrupt Auctioneer. Franklin and Reiter [7] suggest distributing the role of Auctioneer amongst ℓ servers. The auction can be considered secure/fair unless a threshold t , $1 \leq t \leq \ell$ of the servers collude. However, these types of schemes have a high communication overhead and cannot be trusted when the same company owns all the servers.

An alternative approach is to split trust among two servers owned by separate entities (see [11]–[13]). The auction is considered secure as long as the two parties do not collude. Let S_1 and S_2 denote the two servers/parties. This model essentially works as follows;

- 1) Bidders present their identification to S_1 and obtain a token that does not carry their ID.
- 2) Bidders submit the token (without revealing their ID) to S_2 , which issues a pseudonym associated with the token.

In this way, neither S_1 nor S_2 know the relationship between any real ID and the pseudonyms. The bidder then submits his/her bid using the pseudonym. In case of dispute, however, S_1 and S_2 (cooperatively) can determine the real ID associated with each pseudonym. This technique works properly for single auctions, in which the registration phase is separate from the bidding phase. However, in CDAs, the registration and bidding phases overlap and this protocol is not secure. The following scenario explains our attack:

The Attack – A bidder provides identification to S_1 and obtains a token. Using this token, it gets a pseudonym from S_2 that can be used for bidding. If there is no separation between the registration and bidding phases, S_1 can act in a procrastinating manner by halting all new registrations until the recently registered bidder submits his/her bid. This enables S_1 to learn the mapping between the bidder's identity and his/her pseudonym. As a result, Wang and Leung's CDA [21] scheme is susceptible to this attack.

Note that Wang and Leung's scheme is given in the context of Internet retail markets whereas our scheme is designed specifically for share market applications. There are differing security and anonymity requirements between these two types of CDA. For example, a share market offers identical intangible goods and the valuation (i.e., the price) is calculated in a different manner (i.e., there is no "wear and tear" to depreciate its value, instead the value is calculated using a company's

TABLE I
THE REGISTRATION PROTOCOL BETWEEN b_i AND RM

Bidder		RM
Generates a random sn , and $M1 = \Omega_{b_i}(ID_{b_i}, request, sn)$	$\xrightarrow{M1}$	Verifies b_i 's signature Generates $M2$, such that: $M2 = \Omega_{RM}(ID_{b_i} sn)$
	$\xleftarrow{M2}$	
Verifies RM's signature Generates random numbers r Computes pseudonym $ps_{b_i} = H(H(ID_{b_i} sn r))$ Generates a pair of temporary private/public keys sb_i, pb_i		
	$\xleftrightarrow{\text{Cut-and-Choose Protocol}}$	
Obtains $\sigma_{RM}(ps_{b_i}, pb_i)$		

TABLE II
THE REGISTRATION PROTOCOL BETWEEN b_i AND MM

Bidder		MM
Generates M4 as: $\{M2, r, (ps_{b_i}, pb_i), \sigma_{RM}(ps_{b_i}, pb_i)\}$	$\xrightarrow{M4}$	Make sure that b_i has not been registered before, If M4 is verified, then generate $Cert_{b_i}$ as: $\{\Omega_{RM}(ps_{b_i}, pb_i), \sigma_{MM}(ps_{b_i}, pb_i)\}$
	$\xleftarrow{Cert_{b_i}}$	
Obtains the auction certificate.		

expected profit). Furthermore, the location of the seller in a share market has not effect on the cost of shipping the item as occurs in auctions with more conventional items. Finally, it is unclear to the authors exactly what an Internet retail market is as eBay (and similar online auction sites) do not actually list this as an auction type that buyers/sellers can use. Share markets on the other hand are the best known example of a CDA.

III. Components of our CDA Scheme

The scheme we present in this paper uses the additional security characteristics of unlinkability and revocation to fix the problems of the existing scheme. As our CDA is based on a group signature, coalition resistance and exculpability are included to ensure that neither group members nor those involved in issuing a member's group certificate can forge an innocent bidder's signature. Note that non-repudiation is referred to as "traceability" in our CDA scheme.

A. Parties in The System

Figure 1 illustrates the major parties, stages and information flow of our CDA scheme. The auction has three parties:

- 1) A Bidder, who is interested in buying and/or selling commodities in a CDA.
- 2) An Auctioneer, who organises the auction, accepts the bids and determines the winner according to the auction

rules. The Auctioneer also holds the corresponding relation of the identity and a token associated with each bidder.

- 3) A Registrar, who takes part in a protocol in order to complete the registration of a bidder who has obtained a token from the Auctioneer. At the end of the protocol, the bidder obtains a secret key that enables him/her to generate signed bids in a proper format.

The arrows in Figure 1 represent the messages sent between parties. Dashed circles surrounding messages indicate that the enclosed messages are sent during a particular stage of the auction protocol. Each stage of the protocol is explained in Section IV.

B. Communication Channel

Each bidder and the Auctioneer are connected to a common broadcast medium (or public Bulletin Board) with the property that messages sent to the channel instantly reach every party connected to it. We assume that the broadcast channel is public, that is, everybody can listen to all information communicated via the channel, but cannot modify it. We further assume that there are also private channels between the Registrar and any potential bidders (who wish to join the CDA). Nobody is able to listen to, or modify, the messages

Fig. 1. System Dynamics of the CDA Scheme

sent via these private channels ⁴.

C. Group Signatures

For the CDA construction presented in the paper, we employ a group signature scheme invented by Ateniese *et al.* [1], which is provably secure. To join a CDA, a bidder must first register with a Registrar (who jointly plays the role of a group manager with the Auctioneer in a group signature scheme). Once registered, a bidder can participate in the CDA by signing bids using the group signature. Bids are submitted to an independent Auctioneer who runs the CDA. The auction results are posted on a publicly verifiable bulletin board by the Auctioneer. The Ateniese *et al.* [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 b_i) must engage in a protocol with the group manager (Registrar) to receive a group certificate $[B_i, e_i]$, where $B_i = (a^{x_i} a_0)^{1/e_i} \bmod n$ 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:

$$T_1 = B_i y^w \bmod n, \quad T_2 = g^w \bmod n, \\ T_3 = g^{e_i} h^w \bmod n, \quad SK(m)$$

⁴This assumption can be realised by using cryptographic tools that provide authenticated communication.

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 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 $B_i = T_1 / (T_2)^x$.

IV. CDA Protocol

In this section we present the protocol for our CDA scheme. Note that unlike single auctions, CDAs do not consist of various separate phases, as the auction runs continuously and thus all phases overlap. Some bidders are in the process of buying/selling while others may concurrently be in the process of registration. However, from the point of view of an individual bidder and/or the nature of activities in the auction, our scheme consists of the stages below.

A. Setup

Most activities of this stage need to be performed only once (in order to establish a CDA). The Auctioneer organises the CDA (i.e., advertising and calls for auction). Let $\lambda_1, \lambda_2, \xi_1$, and ξ_2 be some lengths, Λ, Γ be some integral ranges, and $\mathcal{H}(\cdot)$ be a collision-resistant hash function. The Registrar 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', 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's public key as

$$\mathcal{Y} = (a, a_0, g, h, n, y)$$

B. Registration

A user submits a request to the Auctioneer to participate in the CDA. The Auctioneer verifies the identity of the requestor, and issues a token that is verifiable by the Registrar. The user then takes part in a protocol with the Registrar to obtain his secret key and a certificate of membership in the auction. Note that the token does not carry the real identity of the bidder. All communication between the Registrar and the owner of a token is authenticated and kept for tracing purposes (i.e., revealing the identity of user associated with the token).

Suppose the Auctioneer uses the RSA system with public parameters n, e as the RSA modulo and the encryption key, respectively. Let d be the corresponding private key in the RSA system and $H(\cdot)$ be an appropriate hash function. Denote by $\Omega_x(m)$ the set $\{m, \sigma_x(H(m))\}$, that is a message, m , and the signature of party x on $H(m)$. Also, let a bidder, b_i , possess a certified encryption/decryption key pair. The protocol between a new user and the Auctioneer is as follows:

- 1) The user establishes his/her identity with the Auctioning by sending a *request* to participate in the CDA, identification, ID_{b_i} , and a random number, sn . This is signed using b_i 's private key, σ_{b_i} .
- 2) The Auctioneer verifies the user's signature using b_i 's public key. The Auctioneer stores all of the information and signs sn using the private key σ_A . The Auctioneer stores the token, $\Omega_A(m)$, securely and forwards a copy to b_i .

This process is shown in Table III. The Auctioneer's signature on the user's identity, $M2$ (see Table III), serves as a token that the user can present to the Registrar. The Registrar is able to check that it is a valid token issued by the Auctioneer by using the Auctioneer's public key.

The protocol between a new bidder, b_i , and the Registrar is as follows (checks in which the values are chosen from proper intervals, the user knows discrete logarithms of values, etc. are omitted):

- 1) b_i selects random exponents x'_i, r and sends

$$C_1 = g^{x'_i} h^r \pmod{n}$$

to the Registrar.

- 2) The Registrar checks that $C_1 \in QR(n)$. If this is the case, the Registrar selects random values

$$\alpha_i, \beta_i$$

and sends them to b_i .

- 3) b_i computes

$$x_i = 2^{\lambda_1} + (\alpha_i x'_i + \beta_i \pmod{2^{\lambda_2}})$$

and sends to the Registrar the value

$$C_2 = a^{x_i} \pmod{n}$$

- 4) The Registrar checks that $C_2 \in QR(n)$. If this is the case, the Registrar selects a random $e_i \in \Gamma$ and computes

$$B_i = (C_2 a_0)^{1/e_i} \pmod{n}$$

and sends to b_i the membership certificate

$$[B_i, e_i]$$

(note that $B_i = (a^{x_i} a_0)^{1/e_i} \pmod{n}$).

- 5) b_i verifies that

$$a^{x_i} a_0 = B_i^{e_i} \pmod{n}$$

- 6) The Registrar publishes value f , where

$$f := e_1 * e_2 * \dots * e_\ell$$

(e_i s, $1 \leq i \leq \ell$, are the exponents of current group members).

The Registrar then creates a new entry in the membership table and stores b_i 's membership certificate $[B_i, e_i]$ and a transcript of the registration process in this location.

C. Bidding

Using a membership certificate $[B_i, e_i]$, a bidder can generate anonymous and unlinkable group signatures on a bid. A bidder b_i , submits a signed bid, to the Auctioneer of the form:

$$\{Buy/Sell, Commodity, Value, Timestamp, etc.\}$$

In securities markets, it is typical for a bid to also contain information regarding the quantity being bid for (e.g., a bidder desires 20 units of commodity at a price of \$10 per unit). In addition, an expiration time for the bid might also be included indicating that a bid is valid until a particular date, after which it should be discarded from the auction proceedings. Furthermore, conventional auctions usually allow a bidder to submit only one bid, whereas CDAs allow an indefinite number of bids to be submitted (e.g., a bidder may buy and sell the same commodity, offering different prices based on the quantity of the goods, etc.) In order to generate a signature on a message/bid, m , a bidder b_i performs the following:

- 1) Chooses a random value w and computes:

$$T_1 = B_i y^w \pmod{n}, \quad T_2 = g^w \pmod{n},$$

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

- 2) Chooses r_1, r_2, r_3, r_4 (in random) from predetermined intervals and computes:

$$(a) \quad d_1 = T_1^{r_1} / (a^{r_2} y^{r_3}), \quad d_2 = T_2^{r_1} / (g^{r_3}), \quad d_3 = g^{r_4},$$

$$\text{and } d_4 = g^{r_1} h^{r_4} \text{ (all in mod } n),$$

$$(b) \quad c = \mathcal{H}(g \parallel h \parallel y \parallel a_0 \parallel a \parallel T_1 \parallel T_2 \parallel T_3 \parallel d_1 \parallel d_2 \parallel d_3 \parallel d_4 \parallel m),$$

$$(c) \quad s_1 = r_1 - c(e_i - 2^{\xi_1}), \quad s_2 = r_2 - c(x_i - 2^{\lambda_1}),$$

$$s_3 = r_3 - c e_i w, \quad \text{and } s_4 = r_4 - c w \text{ (all in } \mathbb{Z}).$$

- 3) Chooses a random number, win , which is used to verify ownership of the bid during the winner determination stage. This is kept secret by both b_i and the Auctioneer.

TABLE III
THE REGISTRATION PROTOCOL BETWEEN A NEW USER AND THE AUCTIONEER

New User	Auctioneer
Generates a random sn , and $M1 = \Omega_{b_i}(ID_{b_i}, request, sn)$	$\xrightarrow{M1}$ Verifies the user's signature Stores ID_{b_i} and sn Generates $M2$, such that: $M2 = \Omega_A(sn)$
$\xleftarrow{M2}$ Verifies the Auctioneer's signature	

TABLE IV
THE REGISTRATION PROTOCOL BETWEEN b_i AND THE REGISTRAR

Bidder	Registrar
Selects random exponents x'_i, r Calculates $C_1 = g^{x'_i} h^r \pmod n$ $M3 = \{M2, C_1\}$	$\xrightarrow{M3}$ Make sure that b_i has not been registered before, Checks that $C_1 \in QR(n)$, Selects random values α_i, β_i $M4 = \{\alpha_i, \beta_i\}$
$\xleftarrow{M4}$ Computes $x_i = 2^{\lambda_1} + (\alpha_i x'_i + \beta_i \pmod{2^{\lambda_2}})$ $C_2 = a^{x_i} \pmod n$ $M5 = \{C_2\}$	$\xrightarrow{M5}$ Checks that $C_2 \in QR(n)$ Selects a random $e_i \in \Gamma$, Computes $B_i = (C_2 a_0)^{1/e_i} \pmod n$ $M6 = \{[B_i, e_i]\}$
$\xleftarrow{M6}$ Verifies that $a^{x_i} a_0 = B_i^{e_i} \pmod n$	Publishes $f := e_1 * e_2 * \dots * e_\ell$

TABLE V
THE BIDDING PROTOCOL BETWEEN b_i AND THE AUCTIONEER

Bidder	Auctioneer
Chooses a random value w and computes: $T_1 = B_i y^w \pmod n$, $T_2 = g^w \pmod n$, $T_3 = g^{e_i} h^w \pmod n$ Chooses r_1, r_2, r_3, r_4 (in random) from predetermined intervals Computes: $d_1 = T_1^{r_1} / (a^{r_2} y^{r_3})$, $d_2 = T_2^{r_1} / (g^{r_3})$, $d_3 = g^{r_4}$, and $d_4 = g^{r_1} h^{r_4}$ (all in mod n), $c = \mathcal{H}(g \parallel h \parallel y \parallel a_0 \parallel a \parallel T_1 \parallel T_2 \parallel T_3 \parallel d_1 \parallel d_2 \parallel d_3 \parallel d_4 \parallel m)$, $s_1 = r_1 - c(e_i - 2^{\xi_1})$, $s_2 = r_2 - c(x_i - 2^{\lambda_1})$, $s_3 = r_3 - c e_i w$, and $s_4 = r_4 - c w$ (all in $\mathbb{Z}_n$) Chooses a random number, win . $M7 = (c, s_1, s_2, s_3, s_4, T_1, T_2, T_3, win)$	$\xrightarrow{M7}$ Verifies the user's signature Compute (all in mod n): $c' = \mathcal{H}(g \parallel h \parallel y \parallel a_0 \parallel a \parallel T_1 \parallel T_2 \parallel T_3 \parallel$ $(a_0^c T_1^{(s_1 - c 2^{\xi_1})}) / (a^{s_2 - c 2^{\lambda_1}} y^{s_3}) \parallel$ $(T_2^{s_1 - c 2^{\xi_1}}) / (g^{s_3}) \parallel T_2^c g^{s_4} \parallel T_3^c g^{s_1 - c 2^{\xi_1}} h^{s_4} \parallel m)$ Accepts the signature iff $c = c'$ and the parameters s_1, s_2, s_3, s_4 lie in proper intervals Posts the bid on the Bulletin Board
Observes the Bulletin Board	$\leftarrow$

4) The bid submitted to the Auctioneer is

$$(c, s_1, s_2, s_3, s_4, T_1, T_2, T_3, win)$$

The Auctioneer then checks the validity of the bidder's signature on bid, using the group's public key $\mathcal{Y}$. A bid of

the correct form is included in the CDA (i.e., posted on the bulletin board). An invalid bid is discarded. The Auctioneer verifies the signature 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) Accept the signature iff $c = c'$ and the parameters s_1, s_2, s_3, s_4 lie in proper intervals.

D. Winner Determination

The Auctioneer determines the auction outcome according to general CDA rules. Conventional auctions only allow for one (or few) winner(s), however, CDAs can have multiple winners. This results in more complicated auction rules.

Bids are referred to as *cleared* when the value of a buy bid equals the value of a sell bid (e.g., if there is a buy bid of \$2 and a sell bid of \$2, then the Auctioneer can match and clear these two bids). The Australian Stock Exchange⁵ clears bids in a strictly time based manner. No priority is given to bids based on amount. Matching buy and sell bids are cleared. In the situation where a buy bid exceeds a sell bid, the surplus (i.e., the difference between the buy and sell price) is awarded to the seller.

Sandholm *et al.* [15] examines various techniques for performing online market clearing. They show that the Auctioneer can increase the market volume (number of cleared bids) by retaining the proceeds of surplus trades. Surplus revenue can then be used to subsidise loss-making trades.

Wurman *et al* present an academic auction server referred to as “AuctionBot” in [22]. The purpose of this server is to allow researchers to explore the design space of auctions. In [23] Wurman and Wellman describe several CDA clearing algorithms that have been tested on AuctionBot.

In our scheme, as soon as bids have been verified, they are posted to the bulletin board in plaintext. This allows the Auctioneer to employ any auction rules or clearing algorithm to the bids. This method has been used by Viswanathan *et al* [20], and Wang and Leung [21] to provide verifiability of the matching process. A full description of clearing strategies is orthogonal to our discussion on CDA security.

Once a bid has been cleared, the winner determination protocol proceeds as follows:

- 1) The Auctioneer signs a cleared bid using its private key σ_A . The signed bid and associated information regarding the trade is posted on the bulletin board.
- 2) b_i views the bulletin board to see if he/she has won. b_i presents the winning bid and the random number *win* chosen during the bidding stage to the Auctioneer.
- 3) The Auctioneer checks that *win* matches the winning bid and awards the goods to b_i .

The purpose of *win* is to ensure only the winner is awarded the goods as no one else knows the correspondence between the winning bid and *win*.

⁵<http://www.asx.com.au>

E. Traceability

In the event of a dispute, the Registrar can open the signature on a bid to reveal the certificate assigned to the bidder. This process is as follows:

- 1) Check the signature’s validity via the verification procedure.
- 2) Recover B_i as

$$B_i = T_1/(T_2)^x \pmod{n}$$

The Registrar then checks the registration transcripts, and determines the token associated with this certificate. The Auctioneer, 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.

F. Revocation

In the case of a malicious bidder (i.e., a bidder that has been caught breaking the auction rules) we would like an efficient and secure means of revoking the bidder from the group. In our scheme we employ a technique presented in Ateniese, Song and Tsudik [2], which considers the revocation problem in Ateniese *et al* [1]. The revocation algorithm informally works as follows:

Assume the group consists of ℓ members with associated certificates $[B_1, e_1], \dots, [B_\ell, e_\ell]$ and the value $f = e_1 * e_2 * \dots * e_\ell$ is known to all members. Suppose a member with exponent $e_k, (1 \leq k \leq \ell)$ needs to be revoked from the system. The Registrar chooses a random value $u \in QR(n)$ and computes

$$t = u^{1/(f/e_k)} \pmod{n}$$

Then the Registrar publishes t, e_k and the new public key

$$\mathcal{Y} = (a, a'_0, g, h, n, y)$$

where $a'_0 = a_0 * u$. A bidder with exponent $e_i, i \neq k$, updates his group signing certificate as

$$B'_i = B_i * t^{s_i}$$

where $s_i = f/(e_i * e_k)$. So the new certificate for this user is $[B'_i, e_i]$, where

$$B'_i = (a^{x_i} a'_0)^{1/e_i} \pmod{n}$$

Now bidder k , cannot compute the corresponding B'_k and thus cannot sign/issue any new bid.

V. Security

In this section we will discuss how our scheme has addressed the security criteria we proposed for CDAs in the introductory section.

Unforgeability – Only bidders that are members of the group are able to generate a group signature, and thus issue a bid. This is due to the unforgeability of the underlying group signature. Furthermore, each bid contains a timestamp that

serves as a freshness indicator. If an opponent attempts to replay a bid with an outdated timestamp, it will be rejected.

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 Problem, and thus anonymity is guaranteed. Note that in our CDA, the Registrar can figure out the certificate associated with each signature, but cannot determine the identity of the bidder associated with this certificate.

Unlinkability – Given two signatures $(c, s_1, s_2, s_3, s_4, T_1, T_2, T_3)$ and $(c', s'_1, s'_2, s'_3, s'_4, T'_1, T'_2, T'_3)$, deciding if they are computed by the same bidder is computationally difficult (with the same argument as anonymity).

Exculpability – Neither a bidder nor the Auctioneer and/or Registrar (individually or cooperatively) can sign a message/bid on behalf of another bidder. This is because the secret key of x_i , associated to user i is computationally hidden from the Registrar. The Registrar, at most, can learn $a^{x_i} \bmod n$, which cannot help him/her 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.

Theorem 1: [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/signatures are posted to the public bulletin, therefore all parties can verify the auction outcome. A bid can be verified using the group's public key $\mathcal{Y}$. The winning bidder can present *win* as proof that he/she won.

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

Traceability – The Registrar is always able to open a valid signature and, with the help of Auctioneer, identify the signer of the bid.

Revocation – Bidders can be easily revoked from the CDA if they have broken the auction rules. This is done by updating the group's public key and each remaining bidder's certificate.

A. Procrastinating Attack

Our scheme is not susceptible to the procrastinating attack described in Section II-B. To see how let the Auctioneer be S_1 and the Registrar S_2 . S_1 attempts to learn the identity of b_i by delaying all new registrations until b_i submits his/her first bid. In our scheme S_1 cannot learn any information about b_i as bids are not linkable (due to the properties of the group signature). When b_i submits a bid, S_1 cannot be certain if the signature belongs to b_i , or if the bid was submitted by an existing bidder.

TABLE VI
COMPARISON OF CDA SCHEMES

	WL04	ACJT00	CL02	TX03
Registration	$L \times 3 + 2$ exp.	30 exp.	30 exp.	2 exp.
Signing	1 exp.	25 exp.	25 exp.	17 exp.
Verification	3 exp.	21 exp.	21 exp.	16 exp.
Revocation	Unclear	$O(\ell)$	$O(1)$	$O(1)$

VI. Efficiency

In this section, we provide a comparison of Wang and Leung's CDA scheme to several implementations of our CDA approach based on group signatures. Table VI shows the amount of work performed during each major stage of the CDA in terms of the number of modular exponentiations. The schemes compared include: Wang and Leung [21] (WL04), Ateniese *et al.* [1] (ACJT00), Camenisch and Lysyankaya [4] (CL02), and Tsudik and Xu [19] (TX03).

The notation L in Table VI denotes the number of times the cut-and-choose protocol is run in Wang and Leung's scheme. Small values of L increase the chances of cheating, whereas higher values decrease the system efficiency. Wang and Leung suggest L should be at least 20, which requires an average of 60 modular exponentiations for registration. The group signature scheme by Tsudik and Xu is clearly the most efficient in terms of registration.

While Wang and Leung's scheme is more efficient for signing and verification, it suffers from the security drawbacks stated in sections II-A and II-B. Furthermore, Wang and Leung require the Auctioneer to store a public key for each bidder, whereas our scheme only requires one public key for verification (i.e., the group public key $\mathcal{Y}$).

Revocation is measured as the work that must be performed in terms of the number of revoked bidders, or the number of remaining bidders ℓ . It is unclear how Wang and Leung's scheme deals with revoked bidders. Ateniese, Song and Tsudik [2] revoke bidders in the ACTJT group signature scheme using a Certificate Revocation List. The Auctioneer must check each bid against the list, which is linear in size of the number of revoked bidders. Alternatively, Camenisch and Lysyankaya, and Tsudik and Xu use a method based on dynamic accumulators where the cost of checking if a bidder has been revoked is constant. With this approach the burden of checking for revocation rests with the bidder.

A. Other Approaches

Instead of using a group signature scheme, we compare some alternate approaches to preventing linkability of bids.

The first approach is to use a *one-time pseudonym*. This means that once a bidder has submitted a bid, he/she must re-register to obtain a new pseudonym. Continuously running the registration protocol of Wang and Leung is more inefficient than using a group signature scheme. It would make the procrastinating attack harder, but would not eliminate it if a bidder were to bid immediately.

Another approach is to issue *multiple pseudonyms* during registration. This prevents a bidder from being profiled, and eliminates the need to run the registration protocol for each bid submitted. However, this method requires the bidder to store a large number of pseudonyms, whereas the group signature approach only requires a single size certificate. Furthermore, this complicates the revocation as now the Auctioneer has to check a large number of pseudonyms for a single bidder.

VII. Conclusion

In this paper we proposed a new scheme for conducting secure and anonymous CDAs. Such a scheme is vital for protecting the security and anonymity of participants who engage in share trading via online brokerage firms. We showed that the only existing CDA proposal by Wang and Leung is inadequate for the task. First of all, its security can be readily subverted by a procrastinating attack. Secondly, their scheme allows bids to be linked and profiles can be created about individual bidders. Finally it is inefficient in the following three areas: registration, bid verification, and bidder revocation. 1) Registration is inefficient due to the reliance on the cut-and-choose protocol; 2) Bid verification requires the Auctioneer to hold a large number of keys (i.e., proportional to the number of bidders); 3) Once a bidder has been traced, it is unclear how the bidder can be revoked.

In direct contrast, our scheme is more flexible and solves all of these problems by utilising any existing secure group signature scheme. The procrastinating attack is ineffective due to the properties of the group signature scheme. Bids cannot be linked to a particular bidder as every signature is different each time a bid is signed, therefore bidders cannot be profiled. While our scheme is slower for bidding and verification, it is efficient in the following respects: 1) Registration does not require expensive cut-and-choose operations; 2) The Auctioneer only requires one key for verifying bids; 3) The cost of revocation can be reduced to a constant. Furthermore, we provide a more comprehensive set of security requirements which are provably secure. The efficiency and security of our CDA scheme rests with the underlying group signature scheme used, and our approach offers the client flexibility in choosing from any group signature scheme.

Clearly much work is required on improving the efficiency of group signature schemes.

References

- [1] Ateniese G., Camenisch J., Joye M. and Tsudik G., "A Practical and Provably Secure Coalition-Resistant Group Signature Scheme," in *Advances in Cryptology - Proceedings of CRYPTO 2000* (M. Bellare, ed.), vol. 1880 of *Lecture Notes in Computer Science*, Springer-Verlag, 2000, 255–270.
- [2] Ateniese G., Song D. and Tsudik G., "Quasi-Efficient Revocation of Group Signatures," in *Proceedings of Financial Cryptography*, (M. Blaze, ed.), vol. 2357 of *Lecture Notes in Computer Science*, Springer-Verlag, 2002, 183–197.
- [3] Boyd C. and Mao W., "Security Issues for Electronic Auctions," Technical Report, Hewlett Packard TR-HPL-2000, 2000.
- [4] Camenisch J. and Lysyanskaya A., "Dynamic Accumulators and Application to Efficient Revocation of Anonymous Credentials," in *Advances in Cryptology - Proceedings of CRYPTO 2002* (M. Yung, ed.), vol. 2442 of *Lecture Notes in Computer Science*, Springer-Verlag, 2002, 61–76.
- [5] Camenisch J. and Stadler M., "Efficient Group Signature Scheme for Large Groups," in *Advances in Cryptology - Proceedings of CRYPTO '97* (S. Burton and J. Kaliski, eds.), vol. 1294 of *Lecture Notes in Computer Science*, Springer-Verlag, 1997, 410–424.
- [6] Chaum D. and van Heyst E., "Group Signatures," in *Advances in Cryptology - Proceedings of EUROCRYPT '91* (D. Davies, ed.), vol. 547 of *Lecture Notes in Computer Science*, Springer-Verlag, 1991, 257–265.
- [7] Franklin M. and Reiter M., "The Design and Implementation of a Secure Auction Service," *IEEE Transactions on Software Engineering*, vol. 22, May 1996, 302–312.
- [8] Friedman D. and Rust J., *The Double auction Market: Institutions, Theories, and Evidence*. Addison-Wesley, 1992.
- [9] Gjrestad S. and Dickhaut J., "Price Formation in Double Auctions," *Games and Economic Behaviour*, vol. 22, 1998, 1–29.
- [10] He M. and Leung H., "An Agent Bidding Strategy Based on Fuzzy Logic in a Continuous Double Auction," in *Proceedings of the fifth International Conference on Autonomous Agents*, 2001, 61–62.
- [11] Jakobsson M. and Juels A., "Mix and Match: Secure Function Evaluation via Ciphertexts," in *Advances in Cryptology - Proceedings of ASIACRYPT 2000* (T. Okamoto, ed.), vol. 1976 of *Lecture Notes in Computer Science*, Springer-Verlag, 2000, 162–177.
- [12] Juels A. and Szydlo M., "A Two-Server, Sealed-Bid Auction Protocol," in *Proceedings of Financial Cryptography*, vol. 2357 of *Lecture Notes in Computer Science*, Springer-Verlag, 2002, 72–86.
- [13] Naor M., Pinkas B., and Sumner R., "Privacy Preserving Auctions and Mechanism Design," in *The 1st Conference on Electronic Commerce*, 1999, 129–139.
- [14] Nguyen K. and Traoré J., "An Online Public Auction Protocol Protecting Bidder Privacy," in *Proceedings of ACISP 2000 – Australasian Conference on Information Security and Privacy* (E. Dawson, A. Clark, and C. Boyd, eds.), vol. 1841 of *Lecture Notes in Computer Science*, Springer-Verlag (Berlin), 2000, 427–442.
- [15] Sandholm T., Blum A., and Zinkevich M., "On-line Algorithms for Market Clearing," in *Proceedings of the 13th SIAM Symposium on Discrete Algorithms (SODA)*, 2002.
- [16] Tesauro C. and Bredin J., "Strategic Sequential Bidding in Auctions using Dynamic Programming," in *Proceedings of the First International Joint Conference on Autonomous Agents and Multi-Agent Systems (AAMAS'02)*, 2002, 591–598.
- [17] Trevathan J., "Security, Anonymity and Trust in Electronic Auctions," *Association for Computing Machinery, Crossroads Student Journal*, Spring Edition, vol. 11.3, 2005.
- [18] Trevathan J., Ghodsi H. and Read W., "Design Issues for Electronic Auctions," in *2nd International Conference on E-Business and Telecommunication Networks*, 2005 (to appear).
- [19] Tsudik G. and Xu S., "Accumulating Composites and Improved Group Signing," in *Advances in Cryptology - Proceedings of ASIACRYPT 2003* (C. Lai ed.), vol. 2894 of *Lecture Notes in Computer Science*, Springer-Verlag, 2003, 269–286.
- [20] Viswanathan K., Boyd C., and Dawson E., "A Three Phased Schema for Sealed Bid Auction System Design," in *Proceedings of ACISP 2000 – Australasian Conference on Information Security and Privacy* (E. Dawson, A. Clark, and C. Boyd, eds.), vol. 1841 of *Lecture Notes in Computer Science*, Springer-Verlag (Berlin), 2000, 412–426.
- [21] Wang C. and Leung H., "Anonymity and Security in Continuous Double Auctions for Internet Retail Market," in *the 37th Hawaii International Conference on Systems Sciences*, 2004.
- [22] Wellman M., Wurman P., and Walsh W., "The Michigan Internet AuctionBot: A Configurable Auction Server for Human and Software Agents," in *Second International Conference on Autonomous Agents (AGENTS)*, May 1998, 301–308.
- [23] Wellman M., Wurman P., and Walsh W., "A Parametrization of the Auction Design Space," in *Games and Economic Behavior*, 35(1-2), 2001, 304–338.