# SIMULASI ANONYMOUS AND SECURE CONTINUOUS DOUBLE AUCTION SCHEME

Ronsen Purba, Anwar Utama, Poerianto

STMIK Mikroskil
Jl. Thamrin No. 122, 124, 140 Medan 20212
ronsen@mikroskil.ac.id

**Abstrak**

*Continuous Double Auction* (CDA) memungkinkan banyak pembeli dan penjual untuk penawaran pembelian dan penjualan untuk sejumlah komoditas secara terus menerus. Persyaratan sekuritas yang harus dipenuhi oleh *single auction* antara lain: *unforgeability*, *non-repudiation*, *public verifiability*, *robustness* dan *anonymity*. Persyaratan sekuritas di atas berlaku untuk *single auction*. Sementara CDA harus memiliki sejumlah tambahan yakni: *unlinkability*, *traceability*, *exculpability*, *coalition resistance*, dan *revocation* dengan menerapkan skema tanda tangan grup. Dalam penelitian ini dikembangkan sebuah simulasi untuk memperlihatkan cara kerja sistem CDA dengan memberikan pengujian terhadap adanya sejumlah kecurangan dari pihak-pihak yang terlibat. Dari pengujian yang dilakukan, diperoleh bahwa sistem CDA mampu mendeteksi kecurangan yang ada sehingga cocok diterapkan dalam dunia nyata.

**Kata Kunci:** *Continuous Double Auction, tanda tangan grup, sekuritas lelang, deteksi kecurangan, anonim*

## 1. Pendahuluan

Lelang (*auction*) adalah sebuah mekanisme pertukaran dimana banyak pembeli potensial memberikan harga penawaran untuk sebuah komoditas dan pemenangnya adalah pembeli dengan harga tertinggi. Pihak pelaksana lelang (*auctioneer*) menerima harga penawaran sebagai wakil dari penjual dan menentukan pemenang berdasarkan pada aturan lelang. Sebuah pelelangan yang hanya memiliki satu penjual dan banyak pembeli disebut sebagai pelelangan tunggal (*single auction*). Sementara, *Continuous Double Auction* (CDA) memungkinkan banyak pembeli dan penjual untuk memberikan penawaran pembelian dan penjualan dari sebuah komoditas secara terus menerus seperti dalam pasar saham . [3, 4, 5] Dalam beberapa tahun terakhir, telah bermunculan banyak perusahaan yang menawarkan pelayanan lelang secara *online* seperti eBay dan OnSale dan lain-lain. Tipe pelelangan ini memiliki kelebihan geografis dibandingkan dengan lelang tradisional, karena pembeli dan penjual tidak perlu bertemu secara fisik pada sebuah lokasi tertentu selama proses lelang. Hal ini memungkinkan dilakukannya lelang yang lebih besar yang mampu menjangkau banyak pembeli dan penjual. Namun sistem ini juga memungkinkan partisipan untuk berbuat curang. [2, 6]

Beberapa problema sekuritas utama pada lelang *online* yang sering dihadapi seperti terjadinya kolusi antar pembeli dan penjual, penyangkalan terhadap harga penawaran yang telah diberikan sebelumnya, ataupun tidak mengirimkan barang yang telah dilelang ataupun barang yang dikirimkan tidak sesuai dengan barang yang dilelang. Selain itu, *auctioneer* juga dapat bersekongkol dengan pembeli, dimana hasil lelang dapat dimenangkan oleh seorang pembeli yang bukan harga tertinggi (tidak sesuai dengan aturan). Isu lebih lanjut juga mencakup bagaimana menjaga identitas pelaksana lelang dan informasi pelelangan itu sendiri.[1,3,5,8] Salah satu protokol kriptografi yang dapat diterapkan untuk menyelesaikan

permasalahan di atas adalah skema *anonymous and secure continuous double auction* yang dikemukakan oleh Jarrod Trevathan dkk. [5]

Penelitian ini akan mengembangkan simulasi skema *anonymous and secure continuous double auction* di atas dengan menguji kemampuan untuk mendeteksi adanya kecurangan dari pihak-pihak yang terlibat dalam lelang tersebut.

## 2. Kajian Pustaka

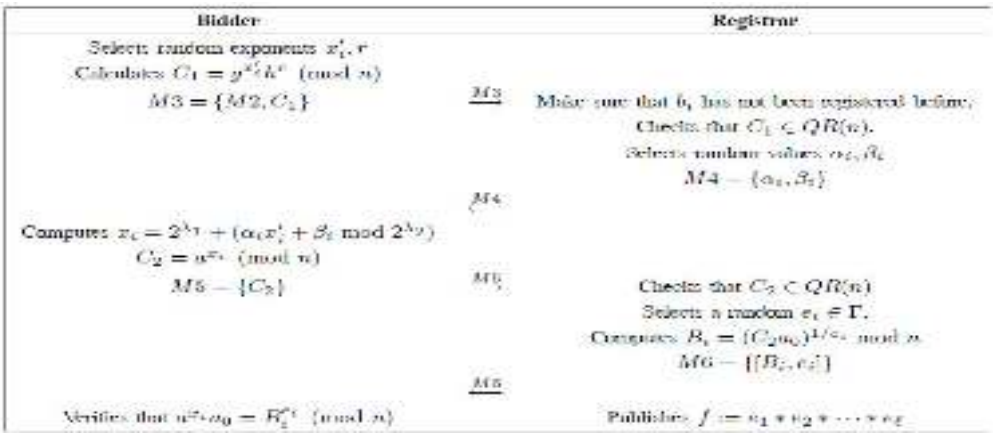
### 2.1. Persyaratan *Continuous Double Auction*

Dengan penggabungan skema tanda tangan grup, CDA memberikan karakteristik sebagai berikut: (1) *Unforgeability* – hanya *bidder* yang register yang dapat mengajukan penawaran; (2) Anonymity – identitas seorang *bidder* tetap anonim (tidak dapat menghubungkan *bidder* dengan penawaran yang dia lakukan) meskipun nilai dari penawaran dapat diketahui pihak lain; (3) *Unlinkability* – tidak ada pihak yang dapat membuat satu profil tentang strategi penawaran dari seorang *bidder* berdasarkan tawaran sebelumnya; (4) *Traceability* – apabila terajdi perselisihan atau dalam penentuan pemenang, otoritas (*Registrar*, *Auctioneer*) dengan bekerjasama tetap dapat mengidentifikasikan *bidder*; (5) *Exculpability* – tidak ada pihak – termasuk *Registrar* dan *Auctioneer*– dapat menciptakan tawaran atas nama seseorang; (6) *Coalition-resistance* – bidder yang terdaftar dan berkolusi tidak dapat menghasilkan tawaran tanpa dapat dibuktikan bahwa mereka melakukan kecurangan; (7) *Verifiability* – semua peserta lelang dapat diverifikasi bahwa mereka telah mengikuti aturan protocol dengan baik; (8) *Robustness* – tawaran yang invalid atau gagal dalam protokol tidak mempengaruhi jalannya dan hasil lelang secara keseluruhan; serta (9) *Revocation* – *bidder* dapat dengan mudah dikeluarkan dari system jika dia melakukan kecurangan.[1, 4, 5]

Skema Wang dan Leung [8] merupakan skema pertama untuk melakukan CDA yang aman dan tetap menjamin kerahasiaan (anonym) dari penawar (*bidder*). Dalam skema ini terdapat dua jenis manajer yakni Manajer Registrasi (*MR*) dan Manajer Market (*MM*). Sebelum memasuki pasar (market), setiap *bidder* harus terlebih dahulu melakukan registrasi kepada kedua manajer *MR* dan *MM*. *MR* menyimpan informasi identitas dan sertifikat dari *bidder,* sementara *MM* akan melakukan verifikasi sertifikat dan menciptakan nama samaran (*pseudonym*) untuk masing-masing bidder. [4, 7]

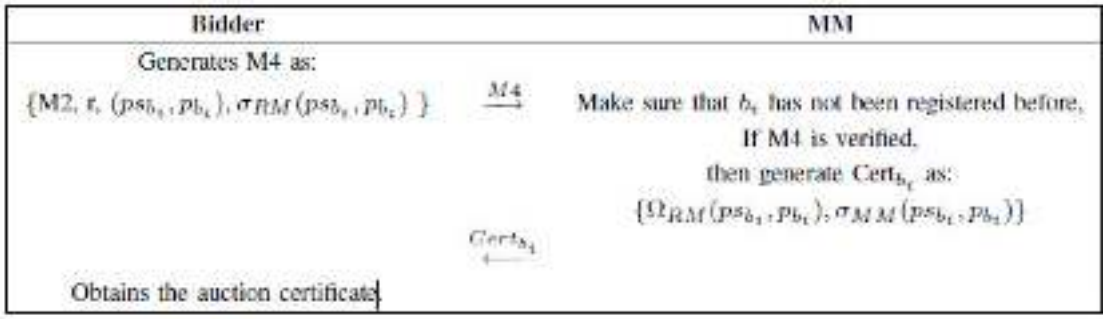
### 2.2. Analisis terhadap Skema Wang dan Leung

Skema Wang dan Leung [8] mempunyai kelemahan sebagai berikut: (1) Sewaktu pendaftaran dengan MM, *bidder* menghasilkan pesan $M_4$, yang berisi pesan $M_2$ sebagai komponen pertama. Akan tetapi, $M_2$ dibentuk dari $\Omega_{RM}$ ($ID_{bi}\|sn$) (terdiri dari identitas bidder $b_i$). Oleh karena itu, MM dengan segera menerima identitas tersebut secara benar; (2) Tawaran dapt dihubungkan dalam skema ini, sebagaimana nama samara sama digunakan untuk setiap tawaran; (3) tidak jelas bagaimana skema ini mengidentifikasikan pemenang. Setelah penawaran pertama identitas *bidder* diungkapkan sehingga tawaran berikutnya oleh orang yang sama tidak lagi anonim; (4) Ketika identitas bidder ditelusuri, skema ini mengungkapkan nilai dari tawaran terakhir. Hal ini tidak diharapkan kecuali dia dicurigai melakukan kecurangan. Skema Wang dan Leung dijelaskan sebagai berikut: Misalkan *RM* menggunakan sistem RSA dengan parameter publik $n$;$e$ sebagai kunci enkripsi. Misalkan d sebagai kunci privat dan $H(.)$ sebuah fungsi hash. Misalkan $\Omega_x(m)$ himpunan $\{m, \sigma_x(H(m))\}$ yakni pesan $m$, dan tanda tangan pihak $x$ pada $H(m)$. Selanjutnya, misalkan bidder $b_i$ mempunyai sertifikat pasangan kunci enkripsi/dekripsi. Protokol antara $b_i$ dan *RM* digambarkan seperti Gambar 1 berikut ini: [6, 8]




**Gambar 1. Protokol antara bidder $b_i$ dengan *RM***

Setelah melakukan register dengan *RM*, *bidder* harus melakukan register dengan *MM* dengan protokol seperti Gambar 2 berikut ini.




**Gambar 2. Protokol antara bidder $b_i$ dengan *MM***

Setelah mendapat sertifikat dari *MM*, *bidder* $b_i$ mengajukan penawaran dengan bentuk {*offer*, $\sigma_{bi}$ , (*offer*), $Cert_{bi}$ } dimana *offer* = {$p_{bi}$, Buy/Sell, Commodity, Value, TimeStamp}, dan $p_{bi}$ adalah kunci publik sementara $b_i$ dengan nama samaran.

### 2.3. Cara Kerja *CDA*

Tahapan yang dilakukan dalam skema *CDA* terdiri dari *Setup*, *Registration*, *Bidding*, *Winner Determination*, *Tracing*, dan *Revocation* dan dijabarkan sebagai berikut. [1, 2, 5, 8]

A. *Setup*

Kebanyakan aktivitas dari tahapan ini hanya perlu dilakukan sekali saja (untuk mempersiapkan *CDA*). *Autioneer* mengatur *CDA* dengan cara menerbitkan iklan mengenai proses pelelangan. Anggap $\lambda_1$, $\lambda_2$, $\xi_1$ dan $\xi_2$ memiliki panjang yang sama, $\Lambda$, $\Gamma$ memiliki *range* bulat tertentu dan $H(.)$ adalah sebuah fungsi *hash* bebas tabrakan. *Registrar* menentukan kunci publik grup dan kunci rahasianya dengan melakukan tahapan berikut ini:

1. Pilih dua buah bilangan prima aman p dan q, dimana p = 2p' + 1 dan q = 2q' + 1, serta p' dan q' adalah bilangan prima) dan menghitung nilai modulus RSA n = pq.
2. Pilih elemen acak a, $a_0$, g, h $\in$ QR(n).
3. Pilih sebuah elemen rahasia $x \in_R Z^*_{p'q'}$ dan menghitung nilai:
$$y = g^x \pmod n$$
4. Publikasikan kunci publik grup sebagai: Y = (a, $a_0$, g, h, n, y)

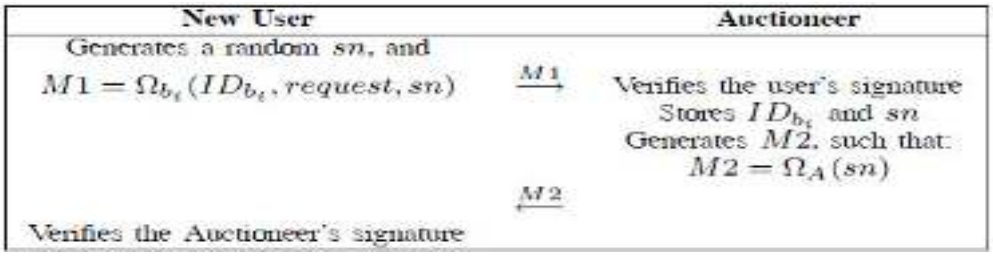
B. *Registration*

Seorang *user* memberikan sebuah permohonan kepada *auctioneer* untuk berpartisipasi dalam CDA. *Auctioneer* memverifikasi identitas dari pemohon dan memberikan sebuah token yang dapat diverifikasi oleh *registrar*. Kemudian, *user* mengambil bagian dalam sebuah protokol dengan *registrar* untuk memperoleh kunci rahasianya dan sebuah sertifikat keanggotaan dalam pelelangan. Perlu dicatat bahwa token tidak mengambil identitas asli dari *bidder*. Semua komunikasi antara *registrar* dan pemilik token diotentikasi dan disimpan untuk tujuan pelacakan.

Anggap *auctioneer* menggunakan sistem RSA dengan parameter publik *n, e* sebagai modulo RSA dan kunci enkripsi. Anggap *d* adalah kunci privatnya dalam sistem RSA dan *H*(.) adalah fungsi *hash* yang cocok. *Signature* dari pihak ke-x pada *H*(*m*), dimana m adalah pesan, dilambangkan dengan $\Omega_x(m) = \{m, \sigma_x(H(\mathrm{m}))\}$. Selain itu, anggap seorang *bidder*, $b_i$, memiliki sebuah pasangan kunci enkripsi/dekripsi yang telah disertifikasi. Protokol antara seorang *user* baru dan *auctioneer* adalah sebagai berikut:

1. *User* mengumumkan identitasnya dengan *auctioneer* dengan mengirimkan sebuah permohonan untuk berpartisipasi dalam *CDA*, identifikasi $ID_{bi}$ dan sebuah bilangan acak, sn. Data ini ditandatangani dengan menggunakan kunci privat $b_i$, $\sigma_{bi}$.
2. *Auctioneer* memverifikasi *signature user* dengan menggunakan kunci publik $b_i$. *Auctioneer* menyimpan semua informasi dan menandatangani sn dengan menggunakan kunci privat $\sigma_A$. *Auctioneer* menyimpan token $\Omega_A(m)$ secara aman dan mengirimkan sebuah duplikasi kepada $b_i$.

Tandatangan dari *auctioneer* pada identitas *user*, $M_2$, dianggap sebagai sebuah token yang dapat diberikan oleh *user* kepada *registrar*. *Registrar* mampu untuk mengecek bahwa token tersebut valid dan diberikan oleh *auctioneer* dengan menggunakan kunci publik *auctioneer*. Ringkasan prosedur kerja dari tahapan registrasi antara *user* baru dan *auctioneer* dapat dilihat pada Gambar 3 berikut ini.




**Gambar 3. Tahapan Registrasi antara *User* Baru dengan *Auctioneer***

C. *Bidding*

Dengan menggunakan sertifikat keanggotaan [$B_i$, $e_i$], seorang *bidder* dapat membangkitkan *anonymous* dan *unlinkable group signature* pada sebuah tawaran. Seorang *bidder*, $b_i$, mengirimkan sebuah tawaran yang ditandatangani, kepada *auctioneer* dengan bentuk berikut:

{*Buy/Sell*, *Commodity*, *Value*, *Timestamp*}

Dalam pasar sekuritas, tawaran secara khusus akan mencakup informasi yang berhubungan dengan kuantitas yang diinginkan (sebagai contoh seorang *bidder* menginginkan 20 unit dari komoditas dengan harga $10/unit). Sebagai tambahan, sebuah waktu jatuh tempo untuk tawaran juga harus dimasukkan untuk mengindikasikan bahwa sebuah tawaran (*bid*) adalah valid hingga waktu tertentu, setelah itu, maka akan dicabut dari pemrosesan pelelangan. Lebih lanjut lagi, pelelangan konvensional biasanya juga

memperbolehkan seorang *bidder* untuk mengirimkan hanya sebuah tawaran saja, sedangkan CDA memperbolehkan tawaran dengan jumlah tidak terhingga kali untuk dikirimkan dimana seorang *bidder* dapat membeli dan menjual komoditas yang sama, menawarkan harga yang berbeda berdasarkan pada kuantitas barang, dan sebagainya. Untuk menghasilkan sebuah *signature* m pada sebuah pesan/*bid*, m, seorang *bidder* $b_i$ melakukan langkah berikut:

1. Pilih sebuah nilai acak w dan hitunglah (menggunakan konsep ElGamal):
$$T_1 = B_i y^w \bmod n$$
$$T_2 = g^w \bmod n$$
$$T_3 = g^{ei} h^w \bmod n$$
2. Pilih $r_1, r_2, r_3, r_4$ secara acak dan hitunglah:
(a) $d_1 = T_1^{r1} / (a^{r2} y^{r3})$, $d_2 = T_2^{r1} / (g^{r3})$, $d_3 = g^{r4}$, dan $d_4 = g^{r1} h^{r4}$ (dalam modulo n)
(b) $c = H(g \parallel h \parallel y \parallel a_0 \parallel a \parallel T_1 \parallel T_2 \parallel T_3 \parallel d_1 \parallel d_2 \parallel d_3 \parallel d_4 \parallel m)$
(c) $s_1 = r_1 - c(e_i - 2^{\xi 1})$, $s_2 = r_2 - c(x_i - 2^{\lambda 1})$, $s_3 = r_3 - ce_i w$ dan $s_4 = r_4 - cw$ (dalam *Z*).
3. Pilihlah sebuah bilangan acak *win* yang akan digunakan untuk memverifikasi kepemilikan dari tawaran selama tahapan penentuan pemenang. Data ini disimpan secara aman oleh $b_i$ dan *auctioneer*.
4. Tawaran yang dikirimkan kepada *auctioneer* adalah:
$$(c, s_1, s_2, s_3, s_4, T_1, T_2, T_3, win)$$

Kemudian, *auctioneer* mengecek validitas dari *signature bidder* pada tawaran dengan menggunakan kunci publik grup Y. Sebuah tawaran dalam bentuk yang benar dimasukkan ke dalam CDA. Sebuah tawaran yang tidak valid akan dibuang. *Auctioneer* akan memverifikasi *signature* dengan melakukan beberapa langkah berikut:

1. Hitung nilai berikut: (semuanya dalam mod n)
$c' = H(g \parallel h \parallel y \parallel a_0 \parallel a \parallel T_1 \parallel T_2 \parallel T_3 \parallel (a_0^c T_1^{(s1 - c2\hat{}\xi 1)}) / (a^{s2 - c2\hat{}\lambda 1} y^{s3}) \parallel (T_2^{s1 - c2\hat{}\xi 1}) / (g^{s3}) \parallel T_2^c g^{s4} \parallel T_3^c g^{s1 - c2\hat{}\xi 1} h^{s4} \parallel m)$.
2. Terima *signature* jika dan hanya jika $c = c'$ dan parameter $s_1, s_2, s_3, s_4$ berada dalam *range* yang benar.

Ringkasan prosedur kerja dari tahapan *bidding* dapat dilihat pada Gambar 4 di bawah ini.

D. *Winner Determination*

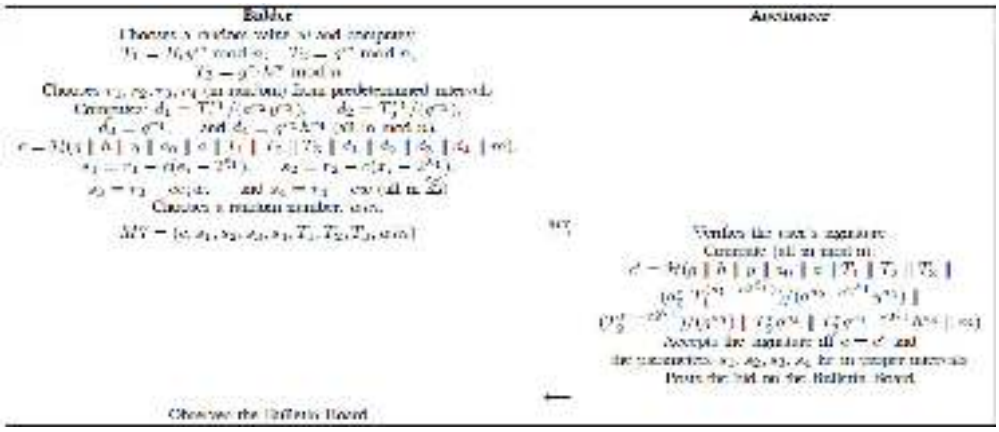
*Auctioneer* menentukan hasil pelelangan berdasarkan pada aturan CDA secara umum. Pelelangan konvensional hanya memperbolehkan satu pemenang, namun, CDA dapat memiliki banyak pemenang. Hal ini diperoleh dari aturan pelelangan yang jauh lebih rumit.

Tawaran akan dianggap *cleared* ketika nilai dari tawaran pembelian sama dengan nilai dari tawaran penjualan (sebagai contoh jika terdapat sebuah tawaran pembelian sebesar $2 dan sebuah tawaran penjualan sebesar $2, maka *auctioneer* dapat mencocokkan dan menghapus kedua tawaran ini. Pada skema ini, setelah tawaran diverifikasi, tawaran tersebut akan langsung dimasukkan ke dalam papan buletin dalam bentuk *plaintext*. Hal ini memungkinkan *auctioneer* untuk menggunakan aturan pelelangan atau algoritma penghapusan pada tawaran tersebut. Setelah sebuah tawaran dihapus, protokol penentuan pemenang diproses dengan mengikuti langkah berikut:

1. *Auctioneer* menandatangani sebuah tawaran yang dihapus dengan menggunakan kunci privatnya $\sigma_A$. Tawaran yang ditandatangani dan informasi yang berhubungan dengan perdagangan ini dimasukkan ke dalam papan buletin.
2. $b_i$ membuka papan buletin untuk melihat apakah dia memenangkan pelelangan. Jika ya, maka $b_i$ menunjukkan tawarannya dan bilangan acak win yang dipilih pada tahapan penawaran kepada *auctioneer*.

3. *Auctioneer* mengecek apakah *win* cocok dengan tawaran yang menang dan memberikan barang kepada $b_i$.

Tujuan dari *win* adalah untuk memastikan hanya pemenang saja yang diberikan barang karena tidak ada orang yang tahu hubungan antara tawaran pemenang dan *win*.



**Gambar 4. Tahapan *BiddingTracing***

E. *Tracing*

Jika terdapat perselisihan, *registrar* dapat membuka *signature* pada sebuah tawaran untuk mengungkapkan sertifikat yang diberikan kepada *bidder*. Proses ini adalah sebagai berikut:

1. Cek validitas *signature* melalui prosedur verifikasi.
2. *Recover* $B_i$ dengan menggunakan rumusan berikut:

$$B_i = T_1 / (T_2)^x \ (mod\ n)$$

Kemudian *registrar* mengecek transkrip registrasi dan menentukan token yang berhubungan dengan sertifikat ini. *Auctioneer* yang mengetahui hubungan antara token dan identitas asli, dapat menentukan identitas dari *bidder*.

F. *Revocation*

Pada kasus dimana terdapat seorang *bidder* jahat (*bidder* yang tertangkap telah melanggar aturan pelelangan), maka diperlukan sebuah peralatan efisien dan aman untuk mencabut *bidder* dari grup. Secara informal, algoritma pencabutan ini bekerja dengan menggunakan langkah berikut:

Asumsikan grup terdiri dari $l$ orang anggota dengan sertifikat $[B_1, e_1]$, …, $[B_l, e_l]$ dan nilai $f = e_1 * e_2 * \ldots * e_l$ diketahui oleh semua anggota. Anggap seorang anggota dengan eksponen ek, $(1 \le k \le l)$ perlu untuk dicabut dari sistem. *Registrar* memilih sebuah nilai acak $u \in QR(n)$ dan menghitung:

$$t = u^{1/(f/ek)} \ mod\ n$$

Kemudian, *registrar* mempublikasikan t, $e_k$ dan kunci publik baru:

$$Y = (a, a_0', g, h, n, y)$$

dimana $a_0' = a_0 * u$. Seorang *bidder* dengan eksponen $e_i$, $i \ne k$, mengubah sertifikat penandatanganan grupnya menjadi:

$$B_i' = B_i * t^{si}$$

dimana $s_i = f / (e_i * e_k)$. Jadi, sertifikat baru untuk *user* ini adalah $[B_i', e_i]$, dimana:

$$B_i' = (a^{x1} a_0')^{1/ei} \ mod\ n$$

Sekarang *bidder* k tidak dapat menghitung $B_k'$ sehingga tidak dapat menandatangani tawaran baru. [5, 6]

## 3. Metode Penelitian

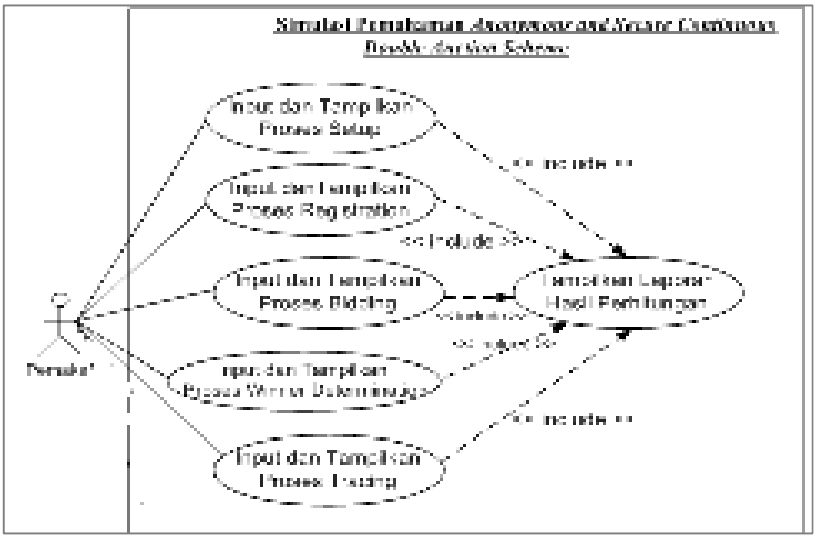
### 3.1 Analisis Proses Kerja Sistem

Skema *anonymous and secure continuous double auction* ini memiliki enam tahapan proses yang dapat dijabarkan sebagai berikut:

1. Tahapan *Setup*
   Tahapan ini hanya perlu dilakukan sekali saja, yaitu untuk mempersiapkan CDA. *Registrar* akan menggunakan tahapan *setup* ini untuk menghasilkan kunci publik grup dan kunci rahasianya.
2. Tahapan *Registration*
   Apabila *user* ingin terlibat dalam sebuah CDA, maka *user* tersebut harus melakukan tahapan *registration* ini terlebih dahulu. *User* akan menggunakan tahapan *registration* ini untuk menghasilkan kunci rahasianya dan sertifikat keanggotaan sehingga *user* dapat berubah status menjadi *bidder* terdaftar. Setelah *user* baru mendaftarkan diri kepada *auctioneer* dan menjadi *bidder*, maka tahapan selanjutnya, *user* baru (*bidder*) akan mendaftarkan dirinya kepada registrar.
3. Tahapan *Bidding*
   Pada tahapan ini, *bidder* terdaftar dapat memberikan tawaran kepada sistem *CDA*.
4. Tahapan *Winner Determination*
   Pada tahapan ini, akan ditentukan pemenang dari lelang yang sedang dilakukan.
5. Tahapan *Tracing*
   Tahapan kerja ini berfungsi untuk mengidentifikasi suatu tawaran guna mengetahui identitas asli dari *bidder* yang memberikan tawaran tersebut yang dilakukan jika terjadi perselisihan atau penyangkalan.
6. Tahapan *Revocation*
   Tahapan ini berfungsi untuk mengeluarkan seorang *bidder* dari sistem CDA, sehingga *bidder* tersebut tidak dapat memberikan tawaran lagi, karena hak aksesnya telah dicabut.

### 3.2 Pemodelan Simulasi

Sistem yang dibangun diharapkan dapat memberikan gambaran proses (tahap demi tahap) yang terdapat dalam *CDA* yang anonim dan aman sesuai dengan persyaratan yang telah ditetapkan. Simulasi proses kerja dari protokol tersebut dapat dimodelkan dalam bentuk *use case diagram* seperti terlihat pada Gambar 5 berikut ini.




**Gambar 5. *Use Case* Diagram Simulasi *CDA***

## 4. Hasil Penelitian dan Pembahasan

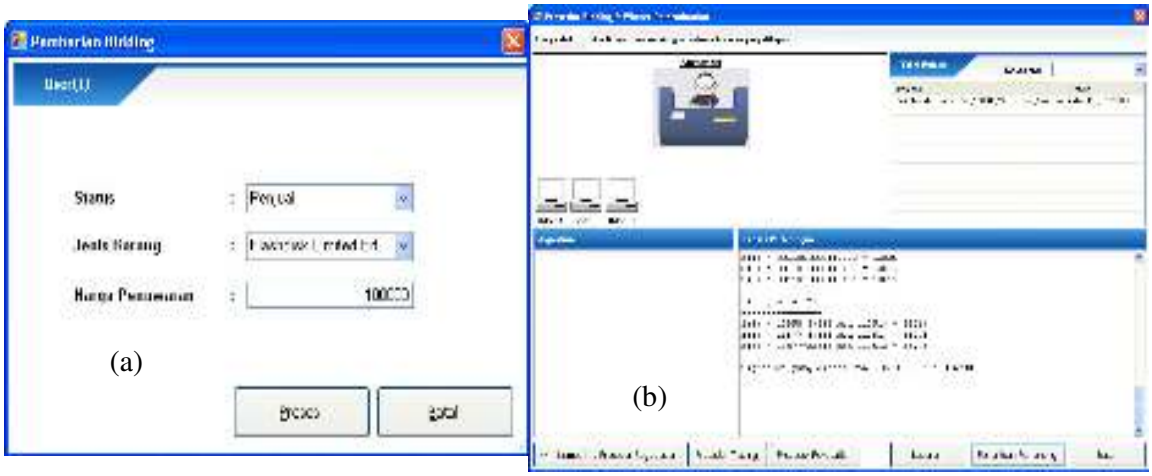
### 4.1 Hasil Penelitian

Pengujian simulasi dilakukan dengan dua skenario yakni: (1) semua proses berjalan dengan baik dan (2) apabila terjadi kecurangan. Untuk pengujian (1), maka pertama kali dilakukan adalah tahap *Setup* dengan tampilan seperti Gambar 6 dan dilanjutkan dengan tahapan registrasi dengan tampilan seperti Gambar 7 berikut ini.

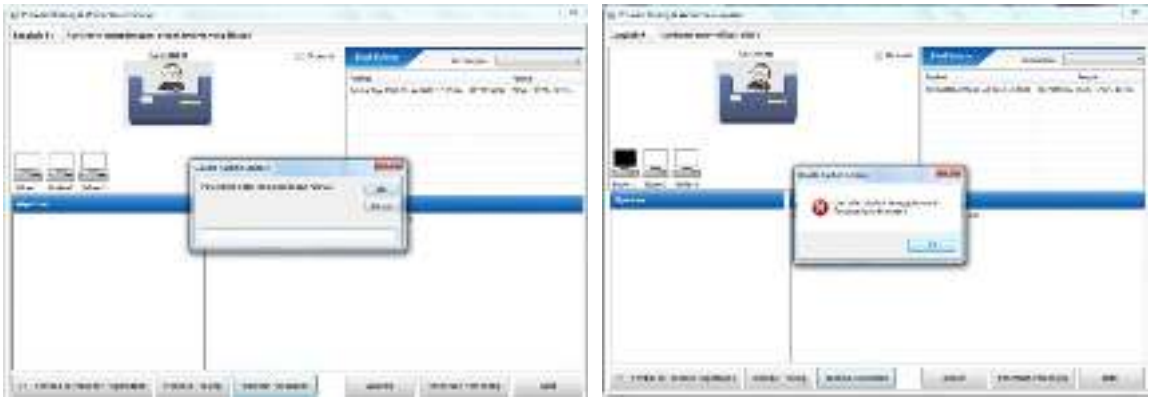
**Gambar 6. Tampilan Hasil Tahap *Setup***

**Gambar 7. Tampilan Tahapan Registrasi**

Setelah itu dilanjutkan dengan tahapan *Bidding* dan *Winner Determination* dengan tampilan seperti Gambar 8 di bawah ini. Untuk mencabut *bidder* dari sistem agar *bidder* tidak dapat lagi mengikuti proses lelang karena melakukan kecurangan dapat dilakukan dengan menjalankan prosedur *revocation,* seperti terlihat pada Gambar 9 di bawah ini.




**Gambar 8. Tampilan Proses *Bidding* (a) dan *Winner Determination* (b)**



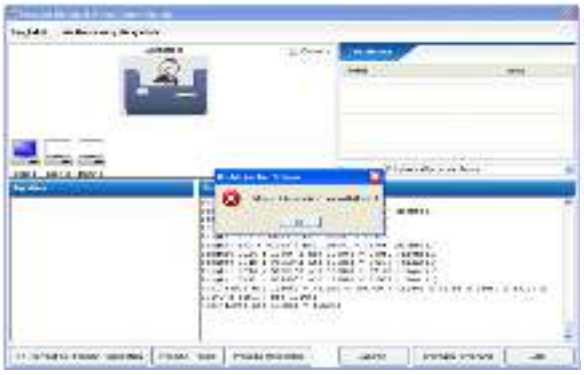
(a) (b)

**Gambar 9. Tampilan Simulasi Revocation (a) Awal (b) Akhir**

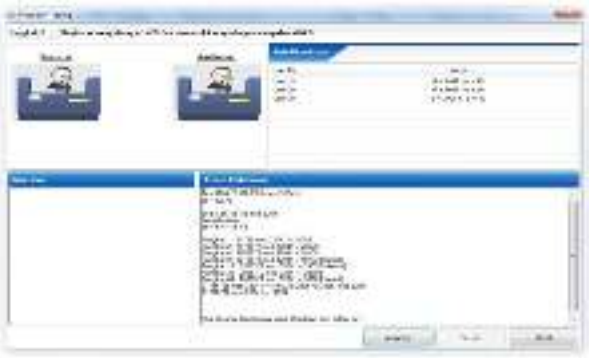
Untuk pengujian terjadinya kecurangan antara pembeli yang satu dengan pembeli lain atau antara penjual yang satu dengan penjual lainnya untuk memperdaya sistem, maka *auctioneer* dapat menjalankan protokol pembuktian seperti tampilan pada Gambar 10 di bawah ini. Sementara untuk penyelesaian jika ada perselisihan antara pembeli dengan penjual *auctioneer* dapat menjalankan protokol Tracing seperti terlihat pada Gambar 11 di bawah ini.

### 4.2 Pembahasan

Dari pengujian yang dilakukan dibuktikan bahwa protokol berjalan dengan baik tahap demi tahap, mulai dari tahap *setup*, *register*, *bidding*, dan *winner determination*. Pihak penyelenggara lelang dapat membuktikan kepemilikan tawaran yang sah jika terjadi perselisihan atau jika ada penyangkalan oleh peserta dengan melakukan protokol *tracing*. Jika peserta ditemukan melakukan kecurangan, maka peserta tersebut dapat dikeluarkan dari sistem dengan menjalankan protokol *revocation*. Penyelenggara juga dapat membuktikan jika ada konspirasi antara pembeli satu dengan pembeli lain atau antara penjual satu dengan penjual lain untuk memperdaya sistem. Dengan demikian protokol ini dapat dinyatakan memenuhi karakteristik lelang yang anonim dan aman sesuai dengan persyaratan yang ditetapkan.



**Gambar 10. *Auctioneer* Membuktikan Kecurangan**



**Gambar 11. Tampilan *Tracing***

## 5. Kesimpulan

Simulasi yang dibangun mampu menunjukkan tahapan-tahapan *CDA* dengan baik serta dapat mendeteksi adanya kecurangan untuk memenuhi syarat anonim dan aman sehingga dapat diterapkan di dunia nyata dimana pembeli dan penjual menjadi peserta lelang dalam skala besar. Perlu dilengkapi dengan deteksi kecurangan panitia lelang dengan salah satu peserta yang mencederai kejujuran dalam pelaksanaan lelang dalam dunia nyata.

## Referensi


[1] Ateniese G., Carmenisch J, Joye M. dan Tsudik G., 2000, *A Practical and Provably Secure Coalition-Resistant Group Signature Scheme*, Advances in Cryptology-Proceedings of CRYPTO 2000, Springer-Verlag, http://www.zurich.ibm.com/security/publications/2000/ACJT2000.pdf

[2] Ateniese G., Song D. dan Tsudik G., 2002, *Quasi-Efficient Revocation of Group Signatures*, Springer-Verlag, http://eprint.iacr.org/2001/101.pdf

[3] Franklin M. dan Reiter M., 1996, *The Design and Implementation of a Secure Auction Service*, IEEE Transactions on Software Engineering, vol. 22, 302–312, https://www.cs.unc.edu/~reiter/papers/1995/SP.pdf

[4] Naor M., Pinkas B., dan Sumner R., 1999, *Privacy Preserving Auctions and Mechanism Design*, in the 1st Conference on Electronic Commerce, 1999, 129–139, http://dl.acm.org/citation.cfm?id=337028

[5] Trevathan J., Ghodosi H. dan Read W., 2006, *An Anonymous and Secure Continuous Double Auction Scheme*, Hawaii International Conference on System Sciences HICSS, http://dunk2.jcu.edu.au/~jc194392/RASNew/research/cda.pdf

[6] Trevathan J., Ghodosi H. dan Read W., 2005, *Design Issues for Electronic Auctions*, in *2nd International Conference on E-Business and Telecommunication Networks,* http://eprints.jcu.edu.au/4554/

[7] Trevathan J., 2005, *Security, Anonymity and Trust in Electronic Auctions*, Association for Computing Machinery, Crossroads Student Journal, Spring Edition, vol. 11.3, 2005, http://eprints.jcu.edu.au/4961/

[8] Wang C. and Leung H., 2004, *Anonymity and Security in Continuous Double Auctions for Internet Retails Market*, 2004, in the 37th Hawaii International Conference on Systems Sciences, 2004, http://dl.acm.org/citation.cfm?id=963111