コンピュータセキュリティ　18−25
(2002.　7.　19)

代理入札方式を備えたイングリッシュオークションプロトコル

塩月　　徹†　　宮地　充子†

† 北陸先端科学技術大学院大学 情報科学研究科　〒923-1292 石川県能美郡辰口町旭台 1-1
E-mail: †{t-shio,miyaji}@jaist.ac.jp

あらまし　本稿では mix and match を用いて，代理入札方式を備えたイングリッシュオークションプロトコルを提案する．インターネット上で行われるイングリッシュオークションでは，入札者の利便を図るために代理入札方式が広く用いられている．本方式は，代理入札における最高入札額を秘匿しつつ，代理入札結果の公開検証が可能であるとともに，オークションマネージャーと入札者や商品提供者の結託が不可能である．

キーワード　イングリッシュオークション，代理入札方式，mix and match.

An English Auction Protocol with Proxy Bidding

Toru SHIOTSUKI† and Atsuko MIYAJI†

† School of Information Science, Japan Advanced Institute of Science and Technology, 1-1, Asahidai, Nomi, Tatsunokuchi, Ishikawa, 923-1292, JAPAN
E-mail: †{t-shio,miyaji}@jaist.ac.jp

Abstract　This paper proposes an English auction protocol with the proxy bidding system, using mix and match techniques. At the Internet English auction, the proxy bidding system is in common use because it is convenient for bidders. Our protocol protects the secrecy of the highest bids, and realizes public verifiability, while preveting collusions among auction manages, bidders, and suppliers.

Key words　English auction, proxy bidding, mix and match.

1. はじめに

イングリッシュオークションは，電子オークションで用いられる形式の中でも最も一般的なものであり，各入札者は，ある入札終了時刻まで，より高い入札値を順次入札する．そして，最終的に最も高い額の入札者が，落札者となる．この方式で各入札者がより安く落札するためには，他者の入札価格に上乗せした価格を入札し続ける必要があり，入札回数の増大につながる．また，どうしても落札したいが，入札価格をチェックし続けられないといった状況の場合，入札者は適正価格以上の価格を入札しなければならず，不便である．Yahoo! オークション[11]などでは，このような入札回数の増大を防ぎ，入札者の手間を減らすために，代理入札方式を備えたイングリッシュオークションが用いられている．

通常のイングリッシュオークションでは，公開されている現在の価格 (=最高入札額) にたいして入札が行われる．一方で，代理入札方式では現在の価格は公開されているが，最高入札額は秘匿される．各入札者が，現在の価格を参考として入札を行うところまでは，通常のイングリッシュオークションと同じであるが，この入札値の取り扱いが通常とは異なり，入札値と最高入札額が比較され，それにより最高入札額と現在の価格，そして最高入札額入札者が更新される．例えば，最高入札額に対して，入札額の方が小さい場合，その入札額があらたな現在の価格へと更新される．最高額入札者は変更されないため，この

ままオークションが終了した場合，最高額入札者は，自分の入札した最高入札額よりも小さな価格 (現在の価格) で落札が可能となる．逆に入札額の方が大きい場合，それまでの最高入札額が，現在の価格として公開され，入札額の方が最高入札額として秘匿される．そして，この入札者が最高額入札者となる．

以下に入札価格と最高入札額の大小関係による代理入札の結果を示す．

入札値 > 最高入札額

この場合，入札値が最高入札額となり，現在の価格はそれまでの最高入札額となる．

入札値 > 最高入札額

最高入札額はそのままで，現在の価格は入札値となる．

入札値 > 最高入札額

最高入札額はそのままで，入札額が現在の価格となる．

1.1 イングリッシュオークションに求められる性質

通常のイングリッシュオークションプロトコルにおいて，求められる性質として以下のようなことが挙げられている [9].

(a) **匿名性:** オークション中に入札者の identity を特定できる参加者・entity は存在しない．

(b) **追跡可能性:** 落札者は他の参加者・entity に対し入札の事実を否認することが不可能である．

(c) **偽造不可能性:** オークション管理者は単独では正当な入札者になりすますことが不可能である．

(d) **偽造不可能性**オークションの参加者は他者の入札値を偽造することが不可能である．

(e) **公平性:** 特定参加者が有利になることがなく，また AM によって他者より有利にすることも不可能である．

(f) **公開検証可能性:** 誰もが入札値に対する署名を検証可能であり，オークション参加者の正当性も検証可能である．

(g) **複数オークション間での Unlinkability を満たす:** 別々のオークション間で，入札者の対応を知られることはない．

(h) **オークション内での Linkability を満たす:** 一つのオークションの中では，入札者の対応がとられている．

(i) **入札の効率性:** 入札，検証に関しての計算量および通信量は効率的である．

(j) **容易に Revocation を行うことができる:** RM は簡単に不正な参加者を排除することが可能である．

(k) **One-time registration:** すべての参加者は，RM に一旦登録すれば複数ラウンドのオークションに参加可能である．

これらの要求を満たしつつ，代理入札方式においては，さらに以下の性質を満たす必要がある．

(l) **最高入札額の秘匿:** 入札時に最高額入札者以外は最高額入札額を知り得ない．

(m) **頑強性:** 不正な入札値を除去可能

代理入札では，入札者は最高入札額以下の価格で落札することが可能であるが，不正行為によってこの最高入札額が知られることとなれば，商品提供者は落札価格の吊り上げを図ることとなる．したがって，最高入札額を秘匿することが最も重要な要件である．これは，入札者同士の結託および，商品提供者 (入札者) とオークション管理者 (AM) の結託に対しても，満たされる必要がある．

また，頑強性は入札値が秘匿された形であるため，不正な入札値により，オークションシステムの運営の妨げとなることを防ぐためである．

2. 既存方式

既存のイングリッシュオークションに関する研究としては，[5], [6], [7], [8], [9], [10] などが挙げられるが，いずれも実際のイングリッシュオークションでは，広く使われている代理入札方式を備えていない．

面らはイングリッシュオークションプロトコルとして，上記の (a)～(k) を満たすプロトコルを提案しており [9]，本稿では，これに代理入札の機能を追加している．

この方式では，2 種類のオークション管理者が存在し，Registration Manager(RM) が入札者 Bidder $\mathcal{A}_i$ ($i \in \{1, \ldots, I\}$) の登録，削除を担当し，Auction Manager(AM) が実際にオークションを開催し，オークションごとに入札者にオークションチケットを発行する．

また，RM と AM は掲示板を持っており，それらは 所持する管理者のみ書き込み可能であり，誰からでも参照できる．

この公開掲示板と，いくつかの知識の証明 ([2] 参照) をもとに，上述の性質を満たしたイングリッシュオークションプロトコルを実現している．

2.1 Procedure

Initialization: RM は $q|p-1$ となる大きな素数と，乗法群 $\mathbf{Z}_p$ の位数 q の原始元 g を公開する．

Registration: 入札者 $\mathcal{A}_i$ ($i \in \{1, \ldots, I\}$) は以下のように公開鍵を登録する．入札者 $\mathcal{A}_i$ は秘密鍵 x_i を選び，公開鍵 $y_i = g^{x_i} \pmod p$ を計算する．次に y_i を RM に送り，y_i の底 g における離散対数 x_i の知識の証明を以下のように公開する．

$$V_{1i} = PK[(\alpha) : y_i = g^{\alpha}](m_R),$$

ここで，m_R は RM の発行するメッセージである．RM は V_{1i} を確認した後，オークション参加者の名前と共に y_i をそれぞれ公開する．

Auction Setup: オークションが開催されるとき，RM は $y_i^r \pmod p$ ($i = 1, \ldots, I$) を g^r と共に RM の掲示板に公開する．ここで RM は $\{y_i^r\}$ の順序をシャッフルして公開し，全入札者との対応を秘密とする．ただし，各入札者は $y_i^r \stackrel{?}{=} (g^r)^{x_i}$ を調べることにより，登録されていることを確認できる．

Round setup: AM は $s \in_R \mathbf{Z}_q$ となる乱数 s を生成

し $g^{rs} \pmod p$ を g^r を用いて計算する．同様に $T_i = (y_i{}^r)^s \pmod p$ を y_i^r を用いて計算し，A_i のオークションチケットとする．この g^{rs} と $T_i = (y_i{}^r)^s \pmod p$ $(i = 1, \ldots, I)$ を AM の掲示板に公開する．

Bidding: 入札者は，以下の (ID_{T_i}, m_i, V_{2i}) を入札情報として AM に送り，AM はこれを掲示板に公開する．

- the identity ID_{T_i} of auction key T_i
- 入札値 m_i $(m_i = \text{auction identity}||\text{bid value})$
- $V_{2i} = PK[(\alpha) : T_i = (g^{rs})^{\alpha}](m_i)$

各入札者は $(g^{rs})^{x_i}$ を計算することができるため自らのオークションチケット T_i を計算することができる．また，V_{2i} は $\mathcal{A}_i$ が $\alpha = x_i$ の値を知っていることの証明である．AM はこの V_{2i} $(i, \ldots, I)$ をすべて確認することにより，各入札者の正当性を確かめる．

Winner Decision: 今 (ID_{T_j}, m_j, V_{2j}) が Winning bid となったとする．AM は落札者を決定するために，RM に T_j が $y_j{}^r$ と一致することを証明する必要がある．そこで AM は知識の証明 V_{3j} を以下のように生成する

$$V_{3j} = PK[(\alpha) : T_j = (y_j{}^r)^{\alpha})](m_R),$$

V_{3j} および $(T_j, y_j{}^r, m_j, V_{2j})$ を公開することにより，落札者の正当性を誰でも確認することが可能である．また，この時点で初めて RM は落札者を特定することが可能である．

Winner Announcement: Winner Decision procedure の後，RM のみが落札者を特定することが可能となる．また，乱数 (r, s) はオークションごとに変更されるため，オークション間の入札者の対応を調べることは不可能である．

3. 提案方式

3.1 Entities

本方式での entity はオークションマネージャー (AM1, AM2)，入札者 (A) からなる．既存方式と違い，2 つの AM の果たす役割に差異が小さいためこのように表記している．

- **AM1:**
  - オークションの開催を準備する．
  - 代理入札を行う．
  - 登録機関として入札者の管理を行う．
  - AM2 落札者の特定を行う．
- **AM2:**
  - オークションの開催を準備する．
  - オークションを行う．
  - 現在の価格を保持する
- **入札者 (A):**
  - オークションの参加者．

3.2 記　　号

以下のように記号を定義する:

p, q	:	$(q \mid p-1)$ となるような大きな素数;
g	:	位数 q となる $g \in \mathbf{Z}_p$ 上の原始元 ;
I	:	入札者の数;
i	:	入札者の index $(i = 1, \cdots, I)$;
$\mathcal{A}_i$	:	bidder i;
B_i	:	bidder i の入札値ベクトル;
K	:	入札値ベクトルのビット数;
k	:	入札値ベクトルの index;
x_i	:	$\mathcal{A}_i$ の秘密鍵 $(x_i \in_R \mathbf{Z}_q)$;
y_i	:	$\mathcal{A}_i$ の公開鍵 $(y_i = g^{x_i} \pmod p)$;
r	:	AM1 の秘密の乱数 $(r \in_R \mathbf{Z}_q)$;
s	:	AM2 の秘密の乱数 $(s \in_R \mathbf{Z}_q)$;
T_i	:	$\mathcal{A}_i$ のオークションチケット;
X	:	AM1, 2 の秘密鍵 $(X \in_R \mathbf{Z}_q)$ 秘密分散法を用いて AM1, AM2 により保持される．;
Y	:	AM の公開鍵 $(Z \in_R \mathbf{Z}_q)$;
Cp	:	現在の価格;
Hp	:	最高入札額;
$E_y()$	:	公開鍵 y による ElGamal encryption $E_y(m) = (G = g^r, M = my^r)$

3.3 Building blocks

本方式では ElGamal 暗号をもとにプロトコルを組み立てている．入札時に入札額を秘匿するため，bit ごとの暗号化を施す．入札値ベクトル $B = v_1, \ldots, v_k$ を bit ごとに暗号化するにあたり，各 bit の取る値は

$$v_i = \begin{cases} v_k = 1 & (v_k = 1) \\ v_k = z & (v_k = 0) \end{cases} \quad (z(\neq 1) : \text{public})$$

とする．また，この暗号化された入札値ベクトルを以下のように表現するものとする．

$$E_Y(B) = (E_Y(v_1), \ldots, E_Y(v_K))$$

これにより，入札値は 2^K 個の bidding point を持つことができる．

3.3.1 公開掲示板

AM1, AM2 がそれぞれ管理所有し，誰でも読むことができ，それぞれの管理者のみ書き込むことが可能である．

- AM1 の掲示板: $\{p, q, g, Y\}$, 各入札者に対応する公開鍵 $\{y_i\}$, $\{y_i^r\}$ $(i = 1, \ldots, I)$
- AM2 の掲示板: g^{rs}, $\{y_i^{rs}\}$ $(i = 1, \ldots, I)$, 現在の価格. 暗号化された最高入札額.

3.3.2 離散対数の知識の証明

離散対数の知識の証明に基づく署名として以下の 2 つを用いている [2].

(1) $PK[(\alpha) : y_1 = g_1^{\alpha} \wedge y_2 = g_2^{\alpha}](m)$
離散対数の等価証明

(2) $PK[(\alpha, \beta) : y_1 = g_1^{\alpha} \vee y_2 = g_2^{\beta}](m)$
2 つの離散対数のどちらかを知っていることの証明

3.3.3 Verifiable ElGamal Encryption

暗号文 $E_y(m) = (G = g^r, M = my^r)$ が，正当な手続きにしたがって m を暗号化したものであることを，$PK[(\alpha) : G = g^\alpha \wedge M/m = y^\alpha](m)$ を示すことにより，秘密情報 r を明かすことなく示すことができる．

3.3.4 Destributed decryption for ElGamal

ElGamal 暗号の特性として，閾値秘密分散法を用いて分散された秘密鍵を，公開することなく，容易に復号を行うことができることが挙げられる．(t, n) 閾値秘密情報分散プロトコルで鍵 X が x_i $(i = 1, \ldots, n)$ に分散され[3]，それぞれ Player P_i が x_i を持つものとする．ここで，暗号文 (α, β) を復号するには以下のようにする．まず，各 P_i は β_i^x を計算し．正しく計算を行ったことの証明，$PK[x_i : y_i = g^{x_i} \wedge \beta_i = \beta^{x_i}](m)$ と共に公開する．そして，各 Player が正しい share による β_i を用いて，$\beta^x = \prod_{i=1}^{t} \beta_{a_i}^{\lambda_{a_i}}$ を計算することにより，β^x を求めることができ，x_i を公開することなく復号することができる．ここで，λ_{a_i} は a_i 番目の share の LaGrange の係数である．

3.3.5 Mix and match [4]

代理入札を行う際に入札値と最高入札額の大小比較のために用いる．これを用いることにより，bit 単位で暗号化された入力を，平文を明らかにすることなく大小比較が可能である．

最初に秘密分散法により秘密鍵 X を AM1， AM2 が分散保持する．大小比較関数 f を以下のように定義する．

$$f(B_i, B_j) = (t_0, t_1) = \begin{cases} (1, z) & x > y \text{ のとき} \\ (z, 1) & x < y \text{ のとき} \\ (z, z) & x = y \text{ のとき} \end{cases}$$

入力は入札値ベクトルの bit 単位であり，このすべての入札値ベクトルの場合に対応した Table を作成する．これを検証可能な形で行単位に re-encrypt と mix を行う [1]．入出力を暗号化された形で最終的な出力 $(E_Y(t_0), E_Y(t_1))$ のみ求める．最後の出力を Destributed decryption により復号する．この Mix and match での演算は全て検証可能である．

3.4 Protocol

Initialization: AM1 は p, q, g を公開する．AM1， AM2 は秘密分散法を用い，秘密鍵 X を分散保持し，暗号化鍵 Y を公開する．

Registration: 入札者 $\mathcal{A}_i$ $(i \in \{1, \ldots, I\})$ は以下のように登録を行う．

（1） 入札者 $\mathcal{A}_i$ は秘密鍵 x_i を選び，公開鍵 $y_i = g^{x_i} \pmod p$ を計算する．

（2） y_i を AM1 に送り，y_i の底 g における離散対数 x_i の知識の証明 V_{1i} :

$$V_{1i} = PK[(\alpha) : y_i = g^\alpha](m_R),$$

を公開する．

（3） AM1 は V_{1i} を確認した後，オークション参加者の名前と共に y_i をそれぞれ公開する．

Auction Setup: オークションが開催されるとき，AM1 は $y_i^r \pmod p$ $(i = 1, \ldots, I)$ を g^r と共に AM1 の掲示板に公開する．ここで AM1 は $\{y_i^r\}$ の順序をシャッフルして公開し，全入札者との対応を秘密とする．ただし，各入札者は $y_i^r \stackrel{?}{=} (g^r)^{x_i}$ を調べることにより，登録されていることを確認できる．

Round setup:

（1） AM2 は bidding point K を公開し，初期価格を公開．それに対応した大小比較 Table を構成して AM1 に送る．

（2） AM1 は送られてきた大小比較 Table に mix and match テクニックに沿って mix と re-encrypt を施し， AM2 に送る．

（3） AM2 は同様に mix と re-encrypt を施す．

（4） AM2 は，$s \in_R \mathbf{Z}_q$ となる乱数 s を生成し $g^{r_s} \pmod p$ を g^r を用いて計算する．同様に $T_i = (y_i{}^r)^s \pmod p$ を y_i^r を用いて計算し，A_i のオークションチケットとする．この g^{rs} と $T_i = (y_i{}^r)^s \pmod p$ $(i = 1, \ldots, I)$ を AM2 の掲示板に公開する．

Bidding: 入札者 A_i は，入札値ベクトルを暗号化 $E_Y(B_i)$ し，正しく暗号化したということの証明

$$V_i = PK[(\alpha) : G = g^\alpha \wedge M/m = y^\alpha](m)$$

を計算する．$(ID_{T_i}, E(B_i), V_i, , V_{2i}), (k = 1, \ldots, K)$ を入札情報として AM2 に送り，AM2 はこれを掲示板に公開する．各入札者は $(g^{rs})^{x_i}$ を計算することができるため自らのオークションチケット T_i を計算することができる．また，V_{2i} は $\mathcal{A}_i$ が $\alpha = x_i$ の値を知っていることの証明である．AM2 はこの V_{2i} $(i, \ldots, I)$ をすべて確認することにより，各入札者の正当性を確かめる．

公開価格の決定: 入札価格とそれまでの最高入札額を比較することにより，公開価格と，秘匿された次の最高入札額，および最高入札額入札者を決定する．AM1， AM2 はそれまでの最高入札値 $H_p = E_Y(B_{i'})$ と，入札値 $E_Y(B_i)$ を Mix and match による大小比較を行い，その結果 (t_0, t_1) により復号する入札値を決定する．

$$(Cp, Hp) = \begin{cases} (B_{i'}, E_Y(B_i)) & (t_0, t_1) = (1, z) \text{ のとき} \\ (B_i, E_Y(B_{i'})) & (t_0, t_1) = (z, 1) \text{ のとき} \\ (B_{i'}, E_Y(B_i)) & (t_0, t_1) = (z, z) \text{ のとき} \end{cases}$$

AM1， AM2 は Distributed ElGamal decryption により，復号することが決まった方のみを復号して公開する．

Winner Decision: 今 $(ID_{T_i}, E(B_i), V_i, V_{2i})$ が Winning bid となったとする．AM2 は落札者を決定するために，AM1 に T_j が $y_j{}^r$ と一致することを証明する必要がある．そこで AM2 は知識の署名 V_{3j} を以下のように生成する

$$V_{3j} = PK[(\alpha) : T_j = (y_j{}^r)^\alpha)](m_R),$$

V_{3j} および $(T_j, y_j{}^r, Cp, V_{2j})$ を公開することにより，落札者の正当性を誰でも確認することが可能である．また，この時点で初めて AM1 は落札者を特定することが可能である．

Winner Announcement: 落札者決定の後，AM1 のみが落札者を特定することが可能である．また，乱数 (r,s) はオークションごとに変更されるため，オークション間の入札者の対応を調べることは不可能である．

3.5 最高入札額の秘匿

最高入札額は，ElGamal 暗号化により秘匿され，AM1，AM2 の結託がないならば，どの entity も最高入札額についての情報を得ることができない．ただし，入札額と最高入札額が等しい場合 $((s,t)=(z,z))$，その入札者は，自らの入札額と最高入札額が等しいことがわかる．ただし，これは代理入札方式の基本的なルールによるものであり，問題とはならない．

3.6 公開検証可能性

代理入札の結果の判定は，全面的に mix and match テクニックにより行われる．ここでの演算はすべて公開検証可能であり，誰でも検証することが可能である．

3.7 頑 強 性

入札者が不正な値を入札した場合，mix and match の Table にマッチする行が見つからないため，これを検出することができ，頑強性は満たされる．

3.8 その他の要求条件について

イングリッシュオークションにおいて求められる要件として挙げた (a)～(k) のうち，(i) 入札の効率性以外の項目では，面らの方式[9] の性質をそのまま受け継ぐことができる．したがって，本方式でも AM1，AM2 の結託がない限り，(a)～(k) の要求を満たすことができる．

3.9 効 率 性

イングリッシュオークションの効率性において重要なものは，入札者の計算量と通信量を減らすことである．そのため，本方式では入札者の通信，計算量を減らすために入札値の bit 列の長さ K に対し，2^K 個の bidding point を取るようにしている．入札者の一度の入札あたりの通信量は，$O(K)$ であり，計算量も $O(K)$ である．ただし，bidding point の数を考えれば十分であると言える．また，AM の通信，計算量であるが，通信量は $O(K)$ であり，計算量は $O(2^K)$ となる．ただし，オークションに必要となる bidding point は多くて 2^{20} 程度である．

4. ま と め

本稿では，Mix and match テクニックを用いて，代理入札方式を備えたイングリッシュオークションプロトコルを提案した．提案方式では，イングリッシュオークションに求められる特性を維持しつつ，最高入札額の秘匿，および頑強性を満たしている．また，入札の効率性に関しては，入札者の通信，計算量を低く抑えることができた．

今後の課題としては，AM の計算量と，知識の証明を減らすことが必要である．

文 献

[1] M. Abe. "Mix-Networks on Permutation Networks". In *Advances in Cryptology - ASIACRYPT '99,* LNCS 1716, Springer-Verlag, pages 317–324, 1999.

[2] J. Camenisch and M. Stadler. "Efficient Group Signature Schemes for Large Groups". In *Advances in Cryptology - CRYPTO '97,* LNCS 1294, Springer-Verlag, pages 410–424, 1997.

[3] R. Canetti, R.Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin. "The (in)security of distributed key generation in dlog-based cryptosystems". In *Advances in Cryptology - EUROCRYPT '99,* LNCS 1403, Springer-Verlag, pages 295–310, 1999.

[4] M. Jakobsson and A. Juels. "Mix and Match: Secure Function Evaluation via Ciphertexts". In *Advances in Cryptology - ASIACRYPT 2000,* LNCS 1976, Springer-Verlag, pages 162–177, 2000.

[5] M. Kumar and S. Feldman. "Internet Auctions". In *Proceedings of the Third USENIX Workshop on Electronic Commerce*, pages 49–60, 1998.

[6] T. Mullen and M.Wellman. "The auction manager: Market middleware for large-scale electronic commerce". In *Proceedings of the Third USENIX Workshop on Electronic Commerce*, pages 49–60, 1998.

[7] K. Nguyen and J. Traoré. "An Online Public Auction Protocol Protecting Bidder Privacy". In *Proceedings of the 5th Australasian Conference on Information and Privacy (ACISP 2000),* LNCS 1841, Springer-Verlag, pages 427–442, 2000.

[8] K. Omote and A. Miyaji. "A Practical English Auction with One-time Registration". In *Proceedings of the 6th Australasian Conference on Information and Privacy (ACISP 2001),* LNCS 2119, Springer-Verlag, pages 221–234, 2001.

[9] K. Omote and A. Miyaji. "A Practical English Auction with Simple Revocation". *IEICE Trans. Fundamentals*, Vol.E85-A,No.5:1054–1061, 2002.

[10] Stuart G. Stubblebine and Paul F. Syverson. "Fair On-line Auctions Without Special Trusted Parties". In *Proceedings of the Third International Financial Cryptography (FC '99),* LNCS 1648, Springer-Verlag, pages 230–240, 1999.

[11] Yahoo. "http://auctions.yahoo.com".