効率的な代理入札システム

田村　裕子[†]　　塩月　徹[†]　　宮地　充子[†]

Efficient Proxy-Bidding System

Yuko TAMURA[†], Toru SHIOTSUKI[†], and Atsuko MIYAJI[†]

あらまし　あらゆる電子商取引の中でも，とりわけ電子オークションは広く世界中で普及しているが，オークション参加者はオークション終了まで，他の入札を監視し入札を繰り返す必要がある．代理入札は代理人が参加者に代わって入札を行うことで，参加者がインターネットに束縛されることなく気軽に参加できることから，近年広く普及しているシステムである．しかしながら，代理入札はこれまで提案されていなかった．本論文では，効率的であり，かつ安全な代理人入札システムの構築を提案する．

キーワード　代理入札，イングリッシュオークション，第 2 価格入札，スライスビット回路

1. まえがき

現在，最も広く普及しているインターネット上のオークションはイングリッシュオークション [7], [8] である．イングリッシュオークションとは，公開される現在の落札価格より高い値を順に入札していき，最終的に最高入札額が落札額，その入札者が落札者となる価格吊上げ型のオークションである．インターネット上で開催されるイングリッシュオークションにおいて商品を落札するためには，参加者は他の入札値を随時チェックして入札を繰り返す必要がある．そのような欠点を克服した方式が代理入札（Proxy-bidding）である．代理入札では，各参加者は希望落札額を代理人に提示し，代理人が参加者に代わって入札を行うため，落札者決定までの間，参加者はインターネットに束縛される必要がない．このような代理入札は次のように行われる．例えば，開始価格が 1,000 円で，入札幅が 100 円であったとしよう．ここで，参加者 A が落札希望額として 2,000 円を秘密に代理人に提示し，外出したとする．代理人は，現在の落札価格が落札希望額より低いときに限り，入札を続ける．この場合，代理人は 1,000 円を入札し，現在の落札額は 1,000 円，現在の落札者は A となる．次に，別の参加者 B が落札希望額 2,500 円を代理人に提示した場合，B の代理人は公開されている現在の落札価格が 1,000 円なので，それより高い 1,100 円を入札する．この時点で，現在の落札額は 1,100 円，現在の落札者は B となる．一方，A の代理人はこれに対し 1,200 円を次に入札する．このように代理人による入札は繰り返され，最終的に現在の落札額は 2,100 円，現在の落札者は B となる．落札者が決定するまで，A が再度，落札希望額を変更することも可能である．

現在のインターネット上でのオークションは，代理人の役割をオークション管理者が一括して担うことで実現されている [1], [2]．この場合，オークション管理者は新たな入札（落札希望額の提示）が行われたとき，その時点での落札者の落札希望額と新たな入札者の落札希望額を比較し，低額（＋入札幅）を，現在の落札額とすればよい．つまり，上の例では，B の希望落札額である 2,500 円より低い A の希望落札価格 2,000 円に入札幅である 100 円を加算した額が現在の落札額となる．このとき，現在の落札者は B となり，次の入札が行われたときには，新たな落札希望額と 2,500 円を比較することになる．

ここで，代理入札システムの構築に必要となる性質をまとめる．

入札値の秘匿性：　オークション管理者，参加者等のすべてのエンティティに対して，すべての入札値は現在の落札額の決定（価格更新）前まで秘匿され，落札者の入札値は価格更新後も秘匿される．

[†] 北陸先端科学技術大学院大学情報科学研究科，石川県
School of Information Science, Japan Advanced Institute of Science and Technology, 1–1 Asahidai, Nomi, Tatsunokuchi, Ishikawa-ken, 923–1292 Japan

匿名性： オークション管理者，参加者等のすべてのエンティティは入札値とその入札者の関係を知ることはできず，落札者以外の入札者は秘匿される．
公開検証性： 誰もがオークションの正当性を検証することができる．
効率性： 入札，価格更新，開札における通信量，及び計算量が効率的である．

1.1 代理人入札と既存オークションの違い

オークションには，価格吊上げ型のイングリッシュオークション [7], [8]，価格吊下げ型のダッチオークション，またすべての入札値を一度に比較する第 1 価格入札 [5], [6], [9], [14]，第 2 価格入札 [4], [12], [13], [15] らがある．

イングリッシュオークションとは，参加者が順に高い値を入札していき，ほかに入札する参加者がいなくなったとき，その時点での最も高い入札額が落札額となるオークションである．これは，条件を満たす入札値が現在の落札額（公開）となるため，入札値の秘匿性は要求されない．しかし，参加者のプライバシー確保の観点から，入札値と入札者の関係，及び落札者以外の入札者を秘匿する必要がある．また，入札，価格更新はリアルタイムで行われるため，1 回の入札・価格更新にかかる通信量，計算量コストの削減が非常に重要になる．

ダッチオークションとは，商品の価格を吊り下げていき，最初に入札を決めた参加者が落札者となるオークションである．

第 1 価格入札，第 2 価格入札は，各参加者が自分の入札値を秘密にしたまま，1 度だけ入札を行うオークションであり，それぞれすべての入札値における最高入札額，2 番に高い入札額が落札額となるオークションである．よって，公平なオークションを行うためには，各入札値は秘匿されなければならず，参加者のプライバシー確保の観点からは，開札後の落札額以外の秘匿性，及び落札者以外の匿名性が必要である．

代理入札においては，参加者の入札値が現在の落札額になるとは限らないため，公平なオークションを実現するためには，すべての入札値を秘匿する必要がある．ただし，価格更新において現在の落札者の入札値と比較した後，新たな現在の落札価格はそれらの低い方の値によって設定される．つまり，価格更新前までの入札値の秘匿性と，価格更新後の高い方の値（現在の落札者の入札値）の秘匿性が必要である．また，他のオークションと同様，入札値と入札者の関係，及び落札者以外の入札者を秘匿する必要がある．

一方，価格更新に 2 入札に対する第 2 価格入札を適用することで，代理入札を実現することができる．この場合，高い方の値（最高額）を秘匿したまま，低い方の値（2 番目に高い値）のみを得ることができる．しかし，第 2 価格入札は元来，一斉入札後の処理を対象にしているため，リアルタイムでの処理が必要な代理入札には適さない．そこで，我々は金持ちの財産比べプロトコル [3], [14] を大小比較に利用する手法とスライスビット回路 [6] を利用する手法の二つを用いて，代理入札を実現する．また，面・宮地によるオークションチケットを用いた入札方式 [8] を適用することで，代理入札に匿名性をもたせる．

1.2 本論文の構成

本論文は次のように構成される．**2.** で代理入札の構築に必要となるいくつかの具体的な方法を紹介し，**3.** で代理入札方式を提案する．**4.** では，提案方式の安全性，効率性について考察する．

2. 準　　備

2.1 代 理 入 札

代理入札に必要となるエンティティ，及びオークションの流れについて述べる．

代理入札は，以下のエンティティで構築される：
登録管理者（RM）： オークションの参加者の登録・削除を行い，参加者の登録情報を知る唯一のエンティティ．
オークション管理者（AM_j）： オークションの入札・価格更新を行う n (≥ 1) 人のエンティティ．オークション管理者の代表を AM_1 とする．
参加者（B_i）： RM へ登録したオークションの参加資格をもつエンティティ．

代理入札は，以下の五つのプロトコルで構成される：
初期設定： n 人のオークション管理者は，暗号化関数とともに公開鍵を生成し，AM_1 がそれらを公開する．また，復号関数の秘密鍵は n 人のオークション管理者で分散管理する．
オークション準備： 登録管理者 RM とオークション管理者 AM_1 はオークションごとに，各参加者に必要な情報を設定し，それらを公開する．また，オークション管理者 AM_1 はそれぞれのオークションに関する，[商品，出品者情報，オークション開始価格，現在の落札額，オークション終了までの時間] などを公開する．

参加者登録： 各参加者は，オークションに参加するため，登録鍵を RM へ登録し，オークション参加に必要となる情報を取得する．
入札： 参加者 B_i は，希望落札額 $\boldsymbol{b}_i$ をオークション管理者の公開鍵暗号で暗号化し，入札値とする．
価格更新： n 人のオークション管理者は，新たな入札値と現在の落札者の入札値を比較し，低い方の入札値を出力する．価格更新ルールに従い，新たな現在の落札値を更新する．
落札者決定： オークション管理者 AM_1 は落札者に関する情報を登録管理者 RM に送り，RM はその情報から落札者を決定する．

ここで，代理入札の価格更新について述べる．新たな入札者を B_{new}，B_{new} の落札希望額を $\boldsymbol{b}_{new}$ とする．このとき，オークション管理者は暗号化された入札値 $E(\boldsymbol{b}_{new})$ と，現在の落札者 B_{high} の暗号化された入札値 $E(\boldsymbol{b}_{high})$ を比較し，高い値の入札者を現在の落札者，低い方の値 $(+\Delta)$ を現在の落札価格 $\boldsymbol{b}_{cur}$ とする．ここで Δ を入札幅とする価格更新に関するルールは以下のようになる：

1. $\boldsymbol{b}_{new} < \boldsymbol{b}_{cur} + \Delta$ ならば，$\boldsymbol{b}_{new}$ を拒否．
2. $\boldsymbol{b}_{cur} + \Delta \leq \boldsymbol{b}_{new}$ のとき，

2-1. $\boldsymbol{b}_{new} < \boldsymbol{b}_{high}$ ならば，$\boldsymbol{b}_{cur} := \boldsymbol{b}_{new} + \Delta$，$\boldsymbol{b}_{high} := \boldsymbol{b}_{high}, B_{high} := B_{high}$，

2-2. $\boldsymbol{b}_{new} = \boldsymbol{b}_{high}$ ならば，$\boldsymbol{b}_{cur} := \boldsymbol{b}_{new}$，$\boldsymbol{b}_{high} := \boldsymbol{b}_{high}, B_{high} := B_{high}$，

2-3. $\boldsymbol{b}_{high} < \boldsymbol{b}_{new}$ ならば，$\boldsymbol{b}_{cur} := \boldsymbol{b}_{high} + \Delta$，$\boldsymbol{b}_{high} := \boldsymbol{b}_{new}, B_{high} := B_{new}$．

2.2 構成要素

本節では，オークションを構築する上で必要となるいくつかのテクニックを述べる．
公開鍵暗号： E を公開鍵暗号の暗号化関数，D を復号関数，E_m を平文 m の暗号文の集合とする．また，E を以下のような準同型性質をもつものとする：

1. $E(m)^{-1} \in E_{m^{-1}}$，
2. $E(m_1)E(m_2) \in E_{m_1 m_2}$，

このような E は，ElGamal 暗号 [17] で与えることができる．ElGamal 暗号は，$q \mid p-1$ を満たす素数 p，q に対して，$g \in \mathbb{Z}_p^*$ を位数 q の元，秘密鍵 $x \in \mathbb{Z}_q^*$，公開鍵 $y = g^x \bmod p$ としたとき，平文 m の暗号文を乱数 $r \in \mathbb{Z}_q^*$ を用いて $E(m) := (g^r, my^r)$ で与える．
暗号化検証： 与えられた暗号文が平文 m の暗号文であるかどうかを検証する手法である．ElGamal 暗号 $E(m) = (e_1, e_2)$ が平文 m の暗号文であることを証明する場合，$(e_1, e_2) = (g^r, my^r)$ に対して，$SPK\{(\alpha) : e_1 = g^\alpha \wedge e_2/m = y^\alpha\}$ によってそれを示すことができる．ここで，$SPK\{(\alpha) :$ 述語 $\}$ は，述語を満たす知識 (α) のゼロ知識証明を利用した署名を表すものとする．
しきい値分散復号： n 人のプレイヤー間に復号関数 D の秘密鍵を分散し，秘密鍵を明かすことなく $t\,(\leq n)$ 人のプレイヤーが集まることによってのみ，暗号文 $E(m) = (e_1, e_2)$ の復号を行う手法である．ElGamal 暗号のしきい値分散復号の手順は以下のとおり：
Step 0. 各プレイヤーは，分散情報生成プロトコル [16] を用いて分散された復号関数 D の秘密鍵 x の分散情報 s_i を保持し，それに対応する $v_i := g^{s_i} \bmod p$ を公開しておくものとする．
Step 1. プレイヤー P_i は，$w_i := {e_1}^{s_i} \bmod p$ を公開し，$SPK\{(\alpha) : v_i = g^\alpha \wedge w_i = {e_1}^\alpha\}$ を生成する．
Step 2. t 人のプレイヤーは，ラグランジェ係数 $\lambda_j = \prod_{j \neq \ell} i_\ell/(i_\ell - i_j)$ を用いて，$\tilde{e} := \prod_{j=1}^{t} {w_{i_j}}^{\lambda_j}$ を計算する．
Step 3. $\tilde{e}/e_2 = m$ を計算することで，平文 m を得る．
分散平文等価テスト（PET）[14]： 二つの暗号文 $E(m) := (e_1, e_2), E(m') := (e_1', e_2')$ の入力に対し，$t\,(\leq n)$ 人のプレイヤーが集まることによって，暗号文を復号することなく $m = m'$ か否かのみを判定する手法である．ElGamal 暗号 E における分散平文等価テストの手順は以下のとおり：
Step 0. 各プレイヤー P_i は，分散情報生成プロトコル [16] を用いて分散された，しきい値分散復号に必要な分散情報 s_i を保持し，$v_i := g^{s_i} \bmod p$ を公開しておくものとする．
Step 1. それぞれのプレイヤー P_i は，乱数 r_i を用いて $(t_1, t_2) := (e_1 {e_1'}^{-1}, e_2 {e_2'}^{-1})$ に対する $(z_1^{(i)}, z_2^{(i)}) := ({t_1}^{r_i}, {t_2}^{r_i})$ を公開し，他のプレイヤーにそれらの正当性を $SPK\{(\alpha) : z_1^{(i)} = {t_1}^\alpha \wedge z_2^{(i)} = {t_2}^\alpha\}$ によって示す．
Step 2. プレイヤーたちは $z_1 := \prod_{i=1}^{n} z_1^{(i)}, z_2 := \prod_{i=1}^{n} z_2^{(i)}$ をしきい値分散復号し，平文 $\tilde{m}$ を手に入れる．このとき，$\tilde{m} = 1$ ならば，$m = m'$ とし，そうでないならば，$m \neq m'$ とする．
ミックスアンドマッチ [14]： $t\,(\leq n)$ 人のプレイヤーによって，0 または 1 の暗号文 $E(m_1), E(m_2)$ に対して，それらの平文の情報を知ることなく，平文同士のビット演算 G の結果の暗号文 $E(G(m_1, m_2))$ をテー

表 1 $Table_{(and)}$
Table 1 $Table_{(and)}$.

$left^{(i)}$	$right^{(i)}$
$E(1)$	$E(1)$
$E(u)$	$E(1)$
$E(u^2)$	$E(u)$

ブル $Table_{(G)}$ を用いて出力する手法である．このとき，$E(m_1)$ と $E(m_2)$ に演算を施した結果（乗算など）を入力 x としたミックスアンドマッチの出力を $Table_{(G)}(x)$ と表すことにする．また，$u \in \{0,1\}^*$ に対して，0 に対応する暗号文に $E(1)$，1 に対応する暗号文に $E(u)$ を用いることとする：

Step 1. 入力値 x の取り得る値を左列，ビット演算結果 $G(m_1, m_2)$ の暗号文を右列に対応させたテーブル $Table_{(G)}$ を作成する．また，暗号化検証によってテーブルを正しく作成したことを示す．$Table_{(and)}$ においては，平文同士の乗算結果の暗号文 $E(m_1)E(m_2)$ を左列とし，$E(m_1 \wedge m_2)$ を右列とするテーブル（表 1）を作成する．

Step 2. n 人のプレイヤーは，すべての行をシャッフルし，再暗号化を行う．再暗号化は $E(1)$ との乗算で行うことができる．ここで，i 番目の行を $(left^{(i)}, right^{(i)})$ とする．

Step 3. 次に，n 人のプレイヤーは PET を用いて，入力値と平文が等価である列 i を検索し，その正当性を示す．AND 演算の場合は $E(m_1)E(m_2) \in E_{m_1 m_2}$ との平文等価テストによって，$left^{(i)} \in E_{m_1 m_2}$ を満たす列 i を検索する．

Step 4. $right^{(i)}$ を $Table_{(G)}(x)$ として出力する．

金持ちの財産比べプロトコル [3]： 2 進数で表された k ビットの値 $\boldsymbol{b}_1, \boldsymbol{b}_2$ ($\boldsymbol{b}_i = (b_i^{(k-1)}, \ldots, b_i^{(0)})$ の大小関係の比較を行う手法である：

Step 1. $a_k = 1$ とし，$k-1 \geq j \geq 1$ に対して，

$$s_j := \begin{cases} 1 & b_1^{(j)} = b_2^{(j)} \text{のとき} \\ 0 & \text{それ以外} \end{cases}$$

$$a_j := a_{j+1} \wedge s_j$$

とする．

Step 2. $k-1 \geq j \geq 0$ に対し，

$$t_j := \begin{cases} 1 & b_1^{(j)} > b_2^{(j)} \text{のとき} \\ 0 & \text{それ以外} \end{cases}$$

$$u_j := a_{j+1} \wedge t_j$$

とする．

Step 3.

$$v := u_0 \vee \cdots \vee u_{k-1}$$

を求める．

Step 4. $v = 1$ のとき，$\boldsymbol{b}_1 < \boldsymbol{b}_2$ とし，$v = 0$ のとき，$\boldsymbol{b}_1 \geq \boldsymbol{b}_2$ とする．

ビットスライス回路 [6]： m 個の値 $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m$ ($\boldsymbol{b}_i = (b_i^{(k-1)}, \ldots, b_i^{(0)})$) から最大値 $\boldsymbol{b}_{max}$ のみを出力する手法である．ここでは，代理入札の価格更新への適用を考え，$m = 2$ として $\boldsymbol{b}_1, \boldsymbol{b}_2$ から低い方の値 $\boldsymbol{b}_{low} = (b^{(k-1)}, \ldots, b^{(0)})$ を出力する手法を述べる：

Step 1. $\boldsymbol{w} = (0,0)$ とし，$j = k-1$ から 0 まで以下を繰り返す；

Step 1-1. $\boldsymbol{w} = (w_1, w_2)$ に対して，

$$\boldsymbol{s}_j := (w_1 \vee b_1^{(j)}, w_2 \vee b_2^{(j)})$$

とする．

Step 1-2. $\boldsymbol{s}_j = (s_1, s_2)$ に対して，

$$b^{(j)} := s_1 \wedge s_2$$

とする．

Step 1-3. $b^{(j)}$ の結果を受けて，$\boldsymbol{w}$ に

$$\boldsymbol{w} := \begin{cases} \boldsymbol{w} & b^{(j)} = 1 \text{ のとき} \\ \boldsymbol{s}_j & \text{それ以外} \end{cases}$$

を代入し，$j = j-1$ とし，*Step 1-1* へ．

Step 2. $\boldsymbol{w} = (w_1, w_2)$ に対して，$w_i = 0$ を満たす $\boldsymbol{b}_i$ を $\boldsymbol{b}_i = \boldsymbol{b}_{low} = (b^{(k-1)}, \ldots, b^{(0)})$ として出力する．

3. 代理入札の提案

本章では効率的な代理入札を提案する．

3.1 初期設定

登録管理者は，参加者登録のための情報として，$q \mid p-1$ を満たす素数 p，q，生成元 $g \in \mathbb{Z}_p^*$ を公開する．オークション管理者 AM_1 は，公開鍵暗号の暗号化関数 E，及び $u \in \{0,1\}^*$ を選び，それらを公開する．また，各 AM_i は分散情報生成プロトコル [16] を用いて復号関数 D の秘密鍵の分散情報を生成し，秘密鍵に対応する公開鍵を生成する．

3.2 準　　備

オークションごとに，登録管理者 RM は，秘密の乱数 $r_{RM} \in \mathbb{Z}_q^*$ に対して $y_{RM} = g^{r_{RM}} \bmod p$ を公開する．また，オークション管理者 AM_1 も，乱数 $r_{AM} \in \mathbb{Z}_q^*$ に対して $y_{AM} = {y_{RM}}^{r_{AM}} \bmod p$ を公開し，r_{AM} を秘密に保管する．

3.3 参加者登録

各参加者 B_i は，秘密鍵 $x_i \in \mathbb{Z}_q^*$ を選択し，登録鍵として $y_i = g^{x_i} \bmod p$ を $SPK\{(\alpha) : y_i = g^{\alpha}\}$ とともに RM へ送信する．

オークションごとに RM は参加者の登録鍵 y_i に対して，$R_i := {y_i}^{r_{RM}} \bmod p$ を計算し，RM の公開掲示板 PPT_{RM} に登録者リスト $\mathcal{R} = \{R_j\}$ を掲示する．その際，各参加者が他の参加者の登録鍵 $\{y_j\}$ とリスト上の $\{R_j\}$ の対応付けができないよう，RM はすべての登録鍵をシャッフルしたリストを公開するものとする．また，RM は登録鍵 y_i と参加者の ID_i のペアを秘密に保管する．

AM_1 は，$\mathcal{R} \ni R_i$ に対して $T_i := {R_i}^{r_{AM}} \bmod p$ を計算し，オークション管理者の公開掲示板 PPT_{AM} にオークションチケットリストとして $\mathcal{T} = \{T_j\}$ を掲示する．

3.4 入　　札

参加者は $T_i = {y_{AM}}^{x_i} \bmod p$ を計算し，$\mathcal{T}$ 上にオークションチケットが発行されているかどうかを確認する．$T_i \in \mathcal{T}$ であれば，2 進数で表した k ビットの希望落札額 $\boldsymbol{b}_i = (b_i^{(k-1)}, \ldots, b_i^{(0)})$ に対して，入札値 $E(\boldsymbol{b}_i) = (e_i^{(k-1)}, \ldots, e_i^{(0)})$ を作成し，$(E(\boldsymbol{b}_i), T_i)$ を公開する．ここで，$E(\boldsymbol{b}_i)$ の各ビットを

$$e_i^{(j)} = \begin{cases} E(u) & b_i^{(j)} = 1 \text{ のとき} \\ E(1) & \text{それ以外} \end{cases}$$

とする．更に，

$$e_i^{(j)} \in E_1 \cup E_u \quad (0 \le j \le k-1)$$

の知識証明によって $E(\boldsymbol{b}_i)$ の正当性を，オークションチケットリスト $\mathcal{T} \ni T_i$ に対する $SPK\{(\alpha) : T_i = {y_{AM}}^{\alpha}\}$ によって正しい参加者であることを証明する．

3.5 価 格 更 新

n 人のオークション管理者は，新たな入札が行われたとき，**2.1** の価格更新ルールに従い，以下の手順で現在の価格 $\boldsymbol{b}_{cur}$，現在の落札者（オークションチケット）T_{high}，現在の落札者の入札値 $E(\boldsymbol{b}_{high})$ を更新する．

ここで，暗号化された二つの値の大小比較を行い，低い方の値を出力し，高い方の値に関する情報は何ら与えない関数を，

$$Compare(E(\boldsymbol{b}_1), E(\boldsymbol{b}_2)) = \begin{cases} (1, \boldsymbol{b}_1) & \boldsymbol{b}_1 \le \boldsymbol{b}_2 \text{のとき} \\ (0, \boldsymbol{b}_2) & \text{それ以外} \end{cases}$$

とする．この $Compare$ 関数については後述する．

Step 1. オークション管理者 AM_1 は現在の価格 $\boldsymbol{b}_{cur}$ に対し，$E(\boldsymbol{b}_{cur} + \Delta)$ を生成する．

Step 2. 新たな入札値 $E(\boldsymbol{b}_{new})$ に対して，オークション管理者 AM_j は協力して，$E(\boldsymbol{b}_{cur} + \Delta)$ と $E(\boldsymbol{b}_{new})$ の大小比較を行い，

$$Compare(E(\boldsymbol{b}_{cur} + \Delta), E(\boldsymbol{b}_{new})) = (0, \boldsymbol{b}_{new})$$

ならば，入札値 $E(\boldsymbol{b}_{new})$ を拒否．

Step 3. $E(\boldsymbol{b}_{new}), E(\boldsymbol{b}_{high})$ に対し，

$$Compare(E(\boldsymbol{b}_{new}), E(\boldsymbol{b}_{high})) = (1, \boldsymbol{b}_{new})$$

ならば，PET を用いて，$c = E(\boldsymbol{b}_{new})E(\boldsymbol{b}_{high})^{-1}$ に対し，

$$(\boldsymbol{b}_{cur}, T_{high}, E(\boldsymbol{b}_{high})) := \begin{cases} (\boldsymbol{b}_{new}, T_{high}, E(\boldsymbol{b}_{high})) & c \in E_1 \text{のとき} \\ (\boldsymbol{b}_{new} + \Delta, T_{high}, E(\boldsymbol{b}_{high})) & \text{それ以外} \end{cases}$$

とする．そうでないならば，

$$(\boldsymbol{b}_{cur}, T_{high}, E(\boldsymbol{b}_{high})) := (\boldsymbol{b}_{high} + \Delta, T_{new}, E(\boldsymbol{b}_{new}))$$

と更新する．

3.6 落札者決定

オークション管理者 AM_1 は，オークション終了時の $\boldsymbol{b}_{cur}, T_{high}$ をそれぞれ落札額，落札者のオークションチケットとし，$R' := {T_{high}}^{1/r_{AM}} \bmod$ を $SPK\{(\alpha) : T_h = {R'}^{\alpha}\}$ とともに公開する．

登録管理者は $y' := {R'}^{1/r_{RM}} \bmod p$ を計算し，$SPK\{(\alpha) : R' = {y'}^{\alpha}\}$ とともに $y' = y_j$ を満たす参加者を落札者として公開する．

3.7 大小比較関数

ここで，大小比較関数 $Compare$ として金持ちの財産比べプロトコル [3] にミックスアンドマッチ [14] を応用した手法 1 と，ビットスライスプロトコル [6] を

応用した手法 2 を与える．ただし，各関数への入力は k ビットの 2 進数 $\boldsymbol{b}_i = (b_i^{(k-1)}, \ldots, b_i^{(0)})$ に対して，

$$e_i^{(j)} = \begin{cases} E(u) & b_i^{(j)} = 1 \text{ のとき} \\ E(1) & \text{それ以外} \end{cases}$$

としたときの $E(\boldsymbol{b}_i) = (e_i^{(k-1)}, \ldots, e_i^{(0)})$ とする．

手法 1：

Step 1. $a_k = E(u)$ とし，ミックスアンドマッチにより，$k-1 \geq j \geq 1$ に対し，

$$s_j := Table_{(eq)}(e_1^{(j)} e_2^{(j)}),$$

$$a_j := Table_{(and)}(a_{j+1} s_j)$$

を求める．

ただし，$Table_{(eq)}$ は,左列 $e \in \{E(1), E(u), E(u^2)\}$ に対し，

$$s := \begin{cases} E(1) & e \in E_u \text{のとき} \\ E(u) & \text{それ以外} \end{cases}$$

を右列にもつテーブルであり，$Table_{(and)}$ は，

$$a := \begin{cases} E(u) & e \in E_{u^2} \text{のとき} \\ E(1) & \text{それ以外} \end{cases}$$

を右列にもつテーブルである．

Step 2. $k-1 \geq j \geq 0$ に対し，

$$t_j := Table_{(big)}(e_1^{(j)} e_2^{(j)^{-1}}),$$

$$u_j := Table_{(and)}(a_{j+1} t_j)$$

を求める．

ただし，$Table_{(big)}$ は，左列 $e \in \{E(1), E(u), E(u^{-1})\}$ に対し，

$$t := \begin{cases} E(u) & e \in E_u \text{のとき} \\ E(1) & \text{それ以外} \end{cases}$$

を右列にもつテーブルである．

Step 3. $v_0 := u_0$ とし，$1 \leq j \leq k-1$ に対し，

$$v_j := Table_{(or)}(v_{i-1} u_j)$$

を求める．

$Table_{(or)}$ は，左列 $e \in \{E(1), E(u), E(u^2)\}$ に対し，

$$v := \begin{cases} E(1) & e \in E_1 \text{のとき} \\ E(u) & \text{それ以外} \end{cases}$$

を右列にもつテーブルである．

Step 4. v_{k-1} をしきい値分散復号し，$D(v_{k-1}) = u$ ならば $E(\boldsymbol{b}_1)$ を，$D(v_{k-1}) = 1$ ならば $E(\boldsymbol{b}_2)$ をしきい値分散復号し，

$$(c, \boldsymbol{b}_{low}) := \begin{cases} (1, \boldsymbol{b}_1) & D(v_{k-1}) = u \text{ のとき} \\ (0, \boldsymbol{b}_2) & \text{それ以外} \end{cases}$$

を $Compare(E(\boldsymbol{b}_1), E(\boldsymbol{b}_2))$ の結果として出力する．

手法 2：

Step 1. $\boldsymbol{w} = (E(1), E(1))$ とし，$j = k-1$ とし，$j = 0$ まで繰り返す；

Step 1-1. $\boldsymbol{w} = (w_1, w_2)$ において，ミックスアンドマッチを用いて，

$$s_1^{(j)} := Table_{(or)}(w_1 e_1^{(j)}), s_2^{(j)} := Table_{(or)}(w_2 e_2^{(j)})$$

を求め，$\boldsymbol{s}_j = (s_1^{(j)}, s_2^{(j)})$ とする．

Step 1-2. $h_j = s_1^{(j)} s_2^{(j)}$ とし，PET を用いて，

$$b^{(j)} = \begin{cases} 1 & h_j \in E_{u^2} \text{ のとき} \\ 0 & \text{それ以外} \end{cases}$$

とする．

Step 1-3. $b^{(j)}$ の結果を受けて，$\boldsymbol{w}$ に

$$\boldsymbol{w} = \begin{cases} \boldsymbol{w} & b^{(j)} = 1 \text{ のとき} \\ \boldsymbol{s}_j & \text{それ以外} \end{cases}$$

を代入し，$j = j-1$ とし，*Step 1-1* へ．

Step 2. $\boldsymbol{w}$ をしきい値分散復号し，$\boldsymbol{b}_{low} = (b^{(k-1)}, \ldots, b^{(0)})$ に対して

$$(c, \boldsymbol{b}_{low}) := \begin{cases} (1, \boldsymbol{b}_{low}) & D(\boldsymbol{w}) = (1, u) \text{ のとき} \\ (0, \boldsymbol{b}_{low}) & \text{それ以外} \end{cases}$$

を $Compare(E(\boldsymbol{b}_1), E(\boldsymbol{b}_2))$ の結果として出力する．

4. 考　　察

4.1 安 全 性

本節では，提案する代理人入札の安全性について考察する．

入札値の秘匿性： 各参加者の入札値は，オークションシステムの暗号化関数を用いて暗号化されており，秘密鍵は n 人のオークション管理者に分散されているため，t $(\leq n)$ 人未満のオークション管理者によって復号することは不可能である．また，価格更新で用いる関数 $Compare$ は，低い方の値を出力するが，高い方の値に関する情報は何も漏らさない．

匿名性： 登録者のデータ（登録鍵，ID) は，登録管理者によって管理されている．オークション中はオークションチケットを用いて入札が行われるが，それらはオークション管理者によってランダム化されているため，登録管理者はオークション管理者 AM_1 と結託しない限り入札者と入札値の対応を知ることができない．

公開検証性： 入札においては，入札値 $E(\boldsymbol{b}_i) = (e_i^{(k-1)}, \ldots, e_i^{(0)})$ の正当性は $e_i^{(j)} \in E_1 \cup E_u$ $(0 \leq j \leq k-1)$ の知識証明によって，またオークションチケット T_i に対する $SPK\{(\alpha) : T_i = {y_{AM}}^{\alpha}\}$ の検証によって参加者の正当性を確認できる．

価格更新においては，暗号化された入札値を公開とすることによって，ミックスアンドマッチの公開検証性より，誰もが正しく価格更新が行われたことを確認することができる．

落札者決定においては，落札者のオークションチケット T_{high} に対して，オークション管理者 AM_1 によって生成された $SPK\{(\alpha) : T_{high} = {R'}^{\alpha}\}$ と，登録管理者 RM による $SPK\{(\alpha) : R' = {y'}^{\alpha}\}$ によって，確かに y' に対応する参加者が落札者であることが検証できる．

効率性： 入札，開札における計算コストについては，次節にて後述する．

4.2 効 率 性

ここで，提案方式の計算量について考察する．入札において，各参加者は k 回の暗号化と k 回の知識証明を行う．また，価格更新においては，手法 1 を用いた場合，1 回の $Compare(E(\boldsymbol{b}_1), E(\boldsymbol{b}_2))$ の計算に $5k-3$ 回のミックスアンドマッチと *Step 4* でのしきい値分散復号を必要とし，手法 2 を用いた場合は，1 回の $Compare(E(\boldsymbol{b}_1), E(\boldsymbol{b}_2))$ の計算に $2k$ 回のミックスアンドマッチと k 回の平文等価テスト（PET），そして *Step 2* でのしきい値分散復号が必要となる．

ここで，テーブル $Table_{(eq)}$, $Table_{(and)}$, $Table_{(or)}$, $Table_{(big)}$ を用いた 1 回のミックスアンドマッチには，それぞれ 1 回の暗号文乗算と 3 回の PET が必要となるため，手法 1 には $15k-9$ 回の PET と 1 回のしきい値分散復号，手法 2 では $7k$ 回の PET と 2 回のしきい値分散復号が必要となる．演算に用いる群の位数 q を 160 ビット，オークション管理者への秘密分散しきい値を $t = 2$ とし，剰余べき演算にバイナリー法を用いた場合，1 回の PET に必要な剰余乗算の回数は $29|q| = 4640$ 回であり，1 回のしきい値分散復号に必要な剰余乗算の回数が $39|q|/4 = 1560$ であることから，手法 1 と手法 2 の比較は PET の回数のみで行うことができる．このとき，ビットごとの演算が少ないプロトコルであるビットスライスを用いた手法 2 はミックスアンドマッチの回数が少ないため，任意の k に対して手法 1 より効率が良いといえる．

表 2 効率性の比較
Table 2 Efficiency.

		手法 1	手法 2	[12]
入札	暗号化	k	k	2^k
	知識証明	k	k	$2^k + 1$
価格更新	PET	$15k - 9$	$7k$	$2^{k-10} + k$

また，関数 $Compare$ の構築は第 2 価格入札を用いることができる．しかし，第 2 価格入札は，一斉入札後の処理を対象にしているため，リアルタイム処理が必要な代理入札には適さない．そこで，第 2 価格入札の一例として，阿部・鈴木による第 2 価格入札 [12] を適用した場合について考察する．この手法では，参加者はオークション管理者によって与えられた離散値リスト $List = \{price_\ell, \ldots, price_1\}$ から入札値を選択するため，k ビットの整数を表現するには 2^k ビットの入札値が必要である．よって，入札には，2^k 回の暗号化と $2^k - 1$ 回のゼロ知識証明，価格更新における 1 回の $Compare$ の計算には $2^{k+2} - 2$ 回の剰余乗算と k 回の PET が必要となる．1 回の PET に必要となる剰余乗算の回数は 4640 であることから，1 回の剰余乗算を約 2^{-12}PET と見積もると，$Compare$ の計算には $2^{k-10} + k$ 回の PET が必要であるということができる．このとき，k が 7 以上である場合，手法 2 のほうが効率が良いといえる．

これらを表 2 に，それぞれ暗号化，知識証明，PET の回数によって比較した結果をまとめる．

5. む す び

本論文では，代理入札を実現するのに必要な性質を明らかにすることで，どのようにして代理入札システムを構築するか示した．具体的な方法として，金持ちの財産比べプロトコルとビットスライスプロトコルを応用した方法は，入札値の秘匿，匿名性，公開検証性を満たし，非常に効率的である．

文 献

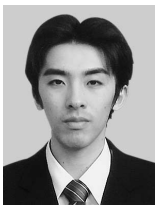
[1] http://auctions.yahoo.co.jp
[2] http://www.ebay.com
[3] A. Yao, “Protocols for secure computations (ex-

tended abstract),” Proc. FOCS’82, pp.160–164, IEEE Computer Society, 1982.
[4] H. Kikuchi, “($M+1$)st-price auction protocol,” Proc. FC2001, 2001.
[5] H. Kikuchi, M. Harkavy, and D. Tyger, “Multi-round anonymous auction protocols,” Proc. First IEEE Workshop on Dependable and Real-Time E-Commerce Systems, pp.62–69, 1998.
[6] K. Kurosawa and W. Ogata, “Bit-slice auction circuit,” Proc. ESORICS2002, vol.2502, pp.24–38, 2002.
[7] K. Omote and A. Miyaji, “A practical English auction with one-time registration,” Proc. ACISP2001, LNCS2119, pp.221–234, Springer-Verlag, 2001.
[8] K. Omote and A. Miyaji, “A practical English auction with simple revocation,” IEICE Trans. Fundamentals, vol.E85-A, no.5, pp.1054–1061, May 2002.
[9] K. Sako, “Universally verifiable auction protocol which hides losing bids,” Proc. PKC2000, pp.35–39, 2000.
[10] M. Abe, “Mix-networks on permutation networks,” Proc. ASIACRYPT’99, LNCS1716, pp.258–273, Springer-Verlag, 1999.
[11] M. Abe and F. Hoshino, “Remarks on mix-network based on permutation networks,” Proc. PKC2001, pp.317–324, 2001.
[12] M. Abe and K. Suzuki, “$M+1$-st price auction using homomorphic encryption,” Proc. PKC2002, pp.115–124, 2002.
[13] M. Harkavy, D. Tyger, and H. Kikuchi, “Electronic auctions with private bids,” Proc. Symposium on Cryptography and Inf. Security, 1998.
[14] M. Jakobsson and A. Juels, “Mix and match: Secure function evaluation via ciphertexts,” Proc. ASIACRYPT2000, pp.162–177, 2000.
[15] M. Naor, B. Pinkas, and R. Sumner, “Privacy preserving auctions and mechanism design,” Proc. ACM Conference on Electronic Commerce, pp.120–127, 1999.
[16] R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin, “Secure distributed key generation for discrete-log based cryptosystems,” Proc. EUROCRYPT’99, vol.1592, pp.295–310, 1999.
[17] T. ElGamal, “A public-key cryptosystem and a signature scheme based on discrete lofarithms,” IEEE Trans. Inf. Theory, vol.IT-31, no.4, pp.469–472, 1985.

（平成 15 年 9 月 22 日受付，16 年 1 月 9 日再受付，
2 月 20 日最終原稿受付）

田村　裕子

1997 津田塾大・学芸・数学卒．1999 北陸先端科技大学院大・情報科学研究科修士課程了．同大大学院博士課程在学中．情報セキュリティの研究に従事．



塩月　徹

2001 名大・工・機械航空工学卒．2003 北陸先端科技大学院大・情報科学研究科博士前期課程了．

宮地　充子　（正員）

1988 阪大・理・数学卒．1990 同大大学院修士課程了．同年，松下電器産業（株）入社．1998 北陸先端科技大学院大・情報科学研究科助教授．現在に至る．2002〜2003 カリフォルニア大学デービス校客員研究員．情報セキュリティの研究に従事．博士（理学）．SCIS93 若手論文賞，科学技術庁注目発明賞，坂井記念特別賞，標準化貢献賞各受賞．情報処理学会，IACR 各会員．