公開掲示板を用いた競り下げ電子オークション方式

宮崎真悟[†,☆] 櫻井幸一[†]

談合による落札価格操作を防止し，かつ応札者のプライバシを保護する電子オークション方式を提案する．本方式では落札額以外のすべての応札価格が一切露呈しない．また公開掲示板に記載された情報を用いて，すべての応札者は落札者決定の正当性を検証することができる．離散対数問題の困難性と一方向性ハッシュ関数の安全性および公開掲示版を仮定することで方式を構築することができる．

A Bulletin-board Based Electronic Auction Scheme with Bidding Down Strategy

SHINGO MIYAZAKI[†,☆] and KOUICHI SAKURAI[†]

We propose an electronic auction scheme satisfying that (i) a group of colluded bidders cannot control the contract price freely, and (ii) the privacy of each bidder can be protected. In our scheme, all prices of bidders except the winner are never revealed to anyone. Furthermore, all bidders can verify the validity of process for determining a winner via a public bulletin board. The assumptions required to our scheme are only that the discrete logarithm problem is hard and there exists a secure one-way hash function and a pullic bulletin board.

1. はじめに

1.1 背景

インターネットという世界に開かれた場を通じて，買い手が相互に競って売り手との契約者の座を勝ち取る電子オークションが様々なWebサイト[10),19)]で実施されている．だれもが売り手となり，対象物に関心を寄せる応札者をインターネットを通じて幅広い世界から募ることが魅力である．つまり，我々は電子上に空間を越えた市場を形成し，自由競争に基づき様々な契約を取り交わすことができる．買い手主導のこの仕組みを電子化しようとするとき，次の2つの問題を検討する必要がある．1つは談合による依頼者利益の保護の問題，もう1つは応札者のプライバシ保護の問題である．

1.2 談合による不正

依頼者利益の保護に関して，複数の応札者が結託し，落札価格を自由競争でなく談合で決定する問題が電子化する以前に問題[20)]となっている．特に応札者個々が他の応札者を特定できるような指名入札方式では，談合を防ぐことは技術的に難しい．しかしながら，インターネットという世界に開けた場で自由競争によるオークションを開催する状況では，比較的参加者が特定されにくい．そこで，今村らは参加者の情報が一切洩れないような仕組みを導入することで，開催時，新たな談合グループの結成機会をなくす方式[12)]を提案した．同方式では，すべての応札者がデータの送信者を特定できないような匿名通信路によって入札を行う．ここで，個人を特定する情報が一切漏れない仕組みが談合グループ結成を防止している．

ところが，今村らの方式では談合のグループを結成して応札する状況では，そのグループが落札価格を操作できる．中西らはこの不正を指摘し，談合による落札価格の操作が行えない方式[22)]を提案した．談合グループによる落札価格の操作は，入札の匿名性を悪用して最高額の入札者が名乗り出ずに，次に金額をつけた応札者が落札するという手順で行われる．よって，中西らは最高金額をつけた応札者が名乗りでない場合，その応札者を検出する仕組みを導入している．同方式において，応札者は後で否定することができない特殊な署名，否認不可署名[4)]を暗号化した応札金額と一緒に匿名通信路にて送る．つまり，この否認不可署名技

† 九州大学大学院システム情報科学研究科情報工学専攻
Graduate School of Information Science and Electrical Engineering, Kyushu University
☆ 現在，株式会社東芝情報・社会システム社SI技術開発センター
Presently with System Integration Technology Center, Information and Industrial Systems & Services Company, Toshiba Corporation

術の導入で，入札の否認を防止し談合による落札価格の操作を不可能にするという方針である．中西らの提案は入札否認を用いた不正を無効化し，談合グループと一般参加者との応札の公平性を果たしている．

1.3 応札者のプライバシ保護

オークションを電子化する際のもう1つの問題として，応札者のプライバシ保護をあげた．応札者の個人情報とその応札金額の対応関係が当事者以外に露呈することは，応札者のプライバシ侵害とされている．ただし，落札者に関しては落札後の依頼人との契約を取り交わす必要がある．よって，落札者が例外で契約を交わせるだけの個人情報と金額を主催者や依頼人に与えることはむしろ必要事項とされる．真のプライバシ保護を考えると，だれがいくらで入札したかという対応関係に加え，だれが応札したかが自分以外に知られないことが満足されるべきである．今村ら[12]と中西ら[22]の提案方式は，「発信者を特定できなような匿名通信路が存在する」という仮定の下で真のプライバシ保護を満たしている．両方式とも応札金額を公開しても個人情報を露呈しないことで，応札者のプライバシが保護される仕組みである．またKudoの方式[15]は，入札金額を管理する機関が依頼者と結託しないという仮定の下で応札者のプライバシが保護されている．

1.4 提案方式

中西らの方式[22]では，談合の問題とプライバシの問題を解決したことが示されているが，匿名通信路の存在が必要不可欠となっている．匿名通信路は具体的にCrowds[23]やOnion routing[26]といった試みがなされている．しかし，様々な匿名性評価をすべて兼ね備えた完璧な匿名通信路を考案することの難しさが議論されているように[25]，いまだ試作段階というのが現状である．よって，我々は匿名通信路や信頼できる機関の存在を必要とせず，公開掲示板と暗号論的基本技術を材料とした方式の検討を試みる．

この指針の下，本稿では談合による不正を防ぎ，かつ応札者のプライバシを保護する方式を提案する．この2つの問題を同時に解決するため，我々は否認不可署名を応札価格（平文）の暗号文と見なす手法を示す．具体的に，応札者は公開されたいくつかの金額の種類の中から1つ応札価格として選び，この価格に対する署名部分だけを公開掲示板に送付する．この際，応札価格は送信しない．落札者の決定は，用意された金額の中で一番高い金額から始め，落札者が出るまで値段を下げてゆくマイニング方式（せり下げ方式）を実施する．値段を下げてゆく過程では，その金額で入札していないことを投函した否認不可署名を用いてオークションの主催者に証明する．この手法により，落札額以外のすべての応札価格は秘匿され，応札者のプライバシ保護を満足する．また落札額までの過程で入札の否認を随時検証できることから，談合による不正を無効化できる．

提案方式の特徴は，離散対数問題の困難性や一方向性ハッシュ関数[7),24]といった暗号理論の基本的仮定と公開掲示板によりシステムを構築できることである．また離散対数問題の困難性に基づいた方式であることから，処理効率が優れた楕円曲線暗号[14),16]への移行を円滑に行うことができる．ここで公開掲示板は電子投票[5]にも適用され，実用的な道具として注目されている．

2. システム概要

2.1 モデル

本稿では2つの種類の入札を考える．1つは，ある商品に対して入札を行い，最も高値をつけた入札者を落札者とする入札で，本稿ではこれを“出品入札”と呼ぶ．一般的なオークションのモデルとして知られているものである．もう1つは，建設工事などの仕事に対し，最も低額をつけた入札者を落札者とする入札で，これを“請負入札”と呼ぶ．

提案する電子入札方式には3つの段階があり，登録プロトコル，入札プロトコル，開示・落札プロトコルに分かれている．入札プロトコルでは，参加した入札者が額を秘密にして入札を行う．ある時刻をもって入札を終了し，開示・落札プロトコルで最も高値（低値）で入札した落札者を決定する．

2.2 管理機関と参加者

提案する電子入札システムにおいて，以下の構成機関が存在する．

オークション主催者： 依頼人を集め，オークションを主催する．公開掲示板を管理し入札者からの入札情報を書き込む．また開示プロトコルにおいては，最高（低）値が決定するまで，ある周期で公開掲示板の金額を更新する．最高（低）値で入札した入札者の送付情報の正当性を検証し落札者を決定する．検証情報と送付情報すべてを公開掲示板に書き込み，参加者すべてにその正当性を公開する．

登録機関： 入札者の登録業務を行う．実際には入札者の認証を行い，送付された鍵への証明書を発行する．

依頼人： 出品入札において，芸術品やプログラムなどをオークションに出品する売り手．一番の高値

をつけた落札者に出品物を売る．または請負入札においては，工事やプログラムなどの仕事をオークションにかけ，一番低い金額をつけた落札者に依頼する．

入札者： オークションにかけられた出品物ないしは仕事に対し，購入・請負を目的とする．出品入札においては最高値，請負入札においては底値を示した人札者が落札者となる．オークション参加の際，鍵を生成して登録機関に鍵証明書を発行してもらう必要がある．

公開掲示板： だれもが記載データを参照できる．ただし，データの書き込み・消去は管理者であるオークション主催者のみ行える．主催者は登録機関の署名を基に登録を正規に行った参加者のデータのみを掲示板に記載する．

監査員： 掲示板に記載される情報がオークション主催者によって，途中で改竄されたり消去されていないかを観察する．掲示板のデータはだれでも読むことができるので，入札者各々が監査員を担うことも可能である．オークション主催者の不正やミスを検査・告知する．

2.3 要求条件

我々の提案システムは以下のすべての条件を満足する．

入札金額の秘匿性 敗者の入札金額はだれにも露呈しない．オークション主催者にも露呈しない．

入札金額の健全性 第三者が正規の登録を行った正式な秘密鍵所有者になりすまして入札することができない（正当な入札情報を作成することができない）．

落札金額の正当性 落札金額がすべての入札価格の中での最高（最低）金額である．

公平性 ある入札者が他の応札者より有利な条件で入札を行うことがない．

中西ら[22]は電子入札プロトコルが満たすべき条件を議論している．上記の条件もその選定に基づいている．ただし，入札金額の秘匿性は中西らの方式[22]では満足されていない．また，中西らの方式では否認段階において不正者が自分のIDを名乗り出ない場合，不正者を特定する場合には同グループに属する応札者のプライバシが保護されない．逆にすべての応札者のプライバシを保護しようとすると，談合による入札否認の不正が有効になる．

3. 基本プロトコル概要と問題点

提案方式での入札・開示・落札の一連の流れは以下のとおりである．

入札プロトコル 入札者はオークション主催者の用意した複数の金額値から1つを選び（w_k とする），署名 $\sigma(w_k)$ を計算する．それから一方向性関数 f を用いて計算した関数値 $Y = f(w_k \| \sigma(w_k))$ を主催者に送付する．主催者は Y を公開掲示板に書き込む．

開示・落札プロトコル オークション主催者は一番の高値（底値）から始め，入札者からの通知を受信するまで，金額のカウントダウン（アップ）をある時間周期で行う．ある時点で，自分の入札した額になったとき，その入札者は主催者に $\sigma(w_k)$ を暗号化して送る．主催者は署名 $\sigma(w_k)$ の正当性と関数値 Y との関連性を検証する．正当である場合のみ，その入札者を落札者としオークションを終了する．$\sigma(w_k)$ は公開掲示板に記載されるため，すべての入札者が落札者決定手続きの正当性を確認することができる．

入札プロトコルにおいて，一方向性関数として単にハッシュ関数を選んだ場合では入札の否認において問題が生じる．考えるのは，入札者が開示・落札段階で自分の入札を名乗り出ないという行為である．この行為を利用すると以下のような不公平な入札が行われる．

今，請負入札において A 社，B 社が結託している．この2社は最小限の金額で落札しようと考える．このとき，B 社は最低と見積もられる金額 S_{min} で，A 社は実際に落札したい金額 S_{aim} で入札する．S_{min} と S_{aim} との間に名乗り出る応札者がいない場合には，B 社は入札 S_{min} を否認して A 社が S_{aim} で落札する．このように応札者が結託することで，落札金額を操作し最小限のコストで仕事を請け負うことができる．これは落札の正当性や公平性に反すると考えられる[22]．

そこで本稿では署名者が過去に行った自分の署名を否認することができない特殊な署名方式[18]を適用して，入札の否認を防止する．ただし，従来提案されている署名の否認が不可能な署名方式では，署名の対象となる平文が明かされたうえで署名の確証・否認を行う．一方，本稿ではメッセージは署名に添付せず，署名を平文（入札価格）の暗号文と見なす応用的手法をとる．これは入札価格の秘密性と入札の否認不可性を同時に満たすためである．

4. 変換可能な否認不可署名方式

通常のディジタル署名は，署名者の検証鍵を用いれば，だれもがその署名の正当性を検証することができる．これがディジタル署名の特徴であるが，応用によっ

てはある限られた状況で発行した署名がその状況を越えて流用されるような状況が生じる．こういった「署名の1人歩き」を防止するため，Chaum と Antwerpen は署名の正当性検証に署名者本人の協力を必要とする特殊な署名方式[4]を提案した．同方式では，署名者の検証鍵を使って，署名者と対話的に署名の正当性を検証するようになっている．ただし，これでは署名の検証時，署名者が過去に行った自分の署名を不当に否認する状況が考えられる．よって，同方式では自分の署名でないことを相手に証明する否認プロトコルを設けることで，不当な署名の否認を検知できる仕組みになっている．この性質ゆえ，否認不可署名と呼ばれている．

否認不可署名は，後にゼロ知識に基づく方式[3]が提案された．しかし，これらの方式[3),4]では署名者の協力なくしては署名を検証することができない．そこで，否認不可署名をある状況で通常のディジタル署名に変換できる方式[1]が考案された．しかし，Boyar らの方式[1]は Michels ら[17]によって破られ，その改良法が示された．さらにその後，Damgard[6]や Michels ら[18]によって新たな効率的方式が提案されている．このうち，Michels らの方式は否認フェーズでの否認証明を複数回行わなくてよい分，効率が良い．また離散対数問題の困難性と一方向性ハッシュ関数の安全性に基づく方式であることから，今回適用の対象とした．

本章では，提案する電子入札で用いる Michels らの，通常の署名に変換可能な否認不可署名方式[18]を紹介する．今，(p,q,α) が公開されており，p は $p=2q+1$ を満たす大きな素数である（ただし，q は素数とする）．α は乗法群 Z_p^* での位数が q となるような生成器とする．$\mathcal{H}$ を一方向性ハッシュ関数とする．

4.1 離散対数の等価・非等価証明

以下では，$z=\beta^x \pmod p$ と $y=\alpha^x$ を満たす $x\in Z_q^*$ が存在するとき，$\log_\beta z=\log_\alpha y$ であることを証明するプロトコルを示す．これは，署名の確証プロトコルで用いられる．また逆に，否認プロトコルは $\log_\beta z\neq\log_\alpha y$ であることの証明である．以下に離散対数の等価性・非等価性を証明するプロトコルを示す．

Step.1：検証者は $u,v\in_R Z_q^*$ を選び，$a=\alpha^u y^v \pmod p$ を計算し，a を証明者に送る．

Step.2：証明者は乱数 $k,\tilde{k},w\in Z_q^*$ を生成し，$r_\alpha=\alpha^k$，$r_\beta=\beta^k$，$\tilde{r}_\alpha=\alpha^{\tilde{k}}$，$\tilde{r}_\beta=\beta^{\tilde{k}}$ を計算する．証明者は，$(r_\alpha,r_\beta,\tilde{r}_\alpha,\tilde{r}_\beta,w)$ を検証者に送る．

Step.3：検証者は (u,v) を証明者に送る．

Step.4：$a=\alpha^u y^v \pmod p$ であるときに限り，

$$s=k-(v+w)x \pmod q$$
$$\tilde{s}=\tilde{k}-(v+w)k \pmod q$$

を計算し，$(s,\tilde{s})$ を検証者に送る．

Step.5：検証者は

$$\alpha^s y^{v+w}=r_\alpha \pmod p$$
$$\alpha^{\tilde{s}} r_\alpha^{v+w}=\tilde{r}_\alpha \pmod p$$
$$\beta^{\tilde{s}} r_\beta^{v+w}=\tilde{r}_\alpha \pmod p$$

を検証し，以下を確認する．

（確証プロトコル）：$\beta^s z^{v+w}=r_\beta \pmod p$

（否認プロトコル）：$\beta^s z^{v+w}\neq r_\beta \pmod p$

4.2 署名生成と通常署名への変換

署名者である Alice が否認不可署名を生成する．検証者 Bob に対し，その署名の正当性を確証プロトコルと不当な署名を否認する否認プロトコルがある．さらに否認不可署名をだれもが検証可能な通常のディジタル署名に変換することができる．

Alice は2つの秘密鍵 $x_1,x_2\in Z_q$ を選び，$y_1=\alpha^{x_1} \pmod p$，$y_2=\alpha^{x_2} \pmod p$ を公開鍵とする．m に対する署名を生成するとき，Alice は乱数 $k\in Z_q$ を生成し，$r=\alpha^k \pmod p$ を計算する．それから以下を計算する．

$$\tilde{r}=r^{x_2} \pmod p$$
$$c=\mathcal{H}(m,\tilde{r})$$
$$s=k-cx_1 \pmod q$$

ここで，$(\tilde{r},s)$ を m への署名とする．この署名の正当性を示す際には，4.1 節で $\beta=\alpha^s y_1^{\mathcal{H}_l(m,\tilde{r})} \pmod p$，$z=\tilde{r}$，$y=y_2$ であることを証明する．不当な署名の否認は，$\log_\beta z\neq\log_\alpha y$ であることを証明する．

この否認不可署名をだれもが検証可能な通常のディジタル署名を変換するには，Alice が x_2 を公開する．これにより，$(m,\tilde{r},s,x_2)$ を入手した検証者は署名の正当性を次式で検証することができる．

$$\tilde{r}=(\alpha^s y_1^{\mathcal{H}_l(m,\tilde{r})})^{x_2} \pmod p$$

5. 電子オークション方式

5.1 初期設定

(p,q,α) がシステムパラメータとして公開されている．p，q は大きな素数で，$p=2q+1$ の関係が成り立っている．α は乗法群 Z_p^* での位数が q となるような生成器である．$\mathcal{H}_l:\{0,1\}^*\to\{0,1\}^l$ を MD5[24]や SHA-1[7]といった一方向性ハッシュ関数とする．

5.2 出品入札プロトコル

ここでは，出品入札に対するプロトコルを記す．

［登録プロトコル］

各入札者 j は作成した鍵 P_j に対し，登録機関から

証明書 $Cert_j$ を発行してもらう．

Step.1：各入札者 j は秘密鍵 $S_j \in Z_q^*$ を生成し，公開鍵 $P_j = \alpha^{S_j} \pmod p$ を定める．入札者 j は身元を明かして，登録機関に P_j を送る．

Step.2：登録機関は入札者 j にグループの番号 GID を割り当てる．1つのグループは n 人で構成される集合とする．n は入札参加人数の見積りによって決定する．それから，(P_j, GID) に対して署名 $Cert_j$ を入札者 j に送る．

［入札プロトコル］

Step.1：オークション主催者は入札金額を複数個（m 個）用意する．ここでは，$(w_1, w_2, \ldots, w_m)$ とする．ただし，表す金額の大小関係は $w_1 < w_2 < \ldots < w_m$ となっている．

Step.2：まず入札者 j は出品物に対し，入札金額 $w_k (1 \leq k \leq m)$ を選ぶ．次に，乱数 $x, k \in Z_q^*$ を選び，以下を計算する．

$$h = \alpha^x \pmod p$$
$$r = \alpha^k \pmod p$$
$$\tilde{r} = r^x \pmod p$$
$$c = \mathcal{H}_l(w_k, \tilde{r})$$
$$s = k - cS_j \pmod q$$

入札者 j は $((P_j, GID, Cert_j), (h, \tilde{r}, s))$ をオークション主催者に送る．w_k を送らないことに注意する．

Step.3：オークション主催者は証明書 $Cert_j$ の正当性を検証する．正当である場合，主催者は入札者 j に対し，$(GID, (h, \tilde{r}, s))$ を公開掲示板の該当するグループの欄に記載する．

Step.4：あらかじめ定めておいた時刻が来た段階で入札要求を締め切る．

Step.5：すべての入札者は自分の送信した入札情報が正しく掲示されているかを確認する．正しく掲示されている場合は，同じグループの n 個すべての入札情報に対し署名 $\sigma_j = Sig_j((h_1, \tilde{r}_1, s_1), \ldots, (h_n, \tilde{r}_n, s_n))$ を行う．入札者 j は $(P_j, GID, Cert_j, \sigma_j)$ を主催者に送る．

Step.6：主催者は $(P_j, GID, Cert_j, \sigma_j)$ の正当性を検証する．正当な場合にのみ，入札者 j の属するグループ欄に $(P_j, GID, Cert_j, \sigma_j)$ を記載する．

5.3 ［開示・落札プロトコル］

Step.1：オークション主催者は公開掲示板を用いて，一番高い金額 w_m をセットする．

Step.2：この金額で入札した入札者 j はオークション主催者に通知する．だれもいない場合は，否認プロトコルを行う．このとき，w_k で入札した入札者 j は，金額 w_m による入札を否認するため，以下の (y, z, β') で否認を行う（4.1 節）．

$$y = h$$
$$z = \tilde{r}$$
$$\beta' = \alpha^s P_j^{\mathcal{H}_l(w_m, \tilde{r})} \pmod p$$

w_m に対する入札者の入札否認を確認した後，次に小さい金額にセットする (w_{m-1})．その金額で入札した入札者が現れるまで，この処理を繰り返す．

Step.3：ある金額 w_k において，入札者 j が通知を行った場合は確証プロトコルにより入札の正当性を検証する．これが正しいとき，入札者 j を落札候補者とする．ここで落札候補者が1人であるとき，その入札者を落札者とする．このとき，入札者 j は x を主催者に送る．主催者は，

$$\tilde{r} = (\alpha^s P_j^{\mathcal{H}_l(w_k, \tilde{r})})^x \pmod p$$

によりその署名の正当性を検証する．主催者は $((P_j, Cert_j), (x, \tilde{r}, s))$ をを公開掲示板に記載しオークションを終了する．

Step.4：落札候補者が複数いる場合は以下を考える．

(a) 候補者の人数が少ない場合は，候補者 j は x を送り，主催者は $((P_j, Cert_j), (x, \tilde{r}, s))$ を公開掲示板に記載し候補者間での同点決勝を行う．

(b) 候補者の人数が多い場合は，$w_k \leq t \leq w_{k+1}$ の金額を複数用意し，これらの金額を用いたオークションを再度行う．

5.4 請負入札プロトコル

基本的流れは出品入札と変わらない．ただし，出品請負入札では最高値をつけた入札者が落札するのに対し，請負入札では最も低い金額をつけた入札者が落札者となる．そこで，開示・落札プロトコルでは一番低い金額から始めてのカウントアップ方式に変更する．つまり，Step.1 と Step.2 を以下のように修正する．

Step.1'：オークション主催者は公開掲示板を用いて，一番低い金額 w_1 をセットする．

Step.2'：この金額で入札した入札者 j はオークション主催者に通知する．だれもいない場

合は，ある時刻で次に小さい金額にセットする (w_2)．その金額で入札した入札者が現れるまで，この処理を繰り返す．その間の否認プロトコルは出品入札と同じように行う．

6. 考　　察

6.1 提案方式の正当性

ここでは，提案方式が電子オークション方式の条件を満足しているかを検討する．

入札金額の秘匿性　敗者の入札金額はビットコミットメントにより暗号化されているため，本人以外には分からない．

入札金額の健全性　入札当事者以外は正当な入札を行うための秘密鍵を知らないので，入札内容を改竄することはできない．また，開示・落札時における主催者による入札情報の改竄は，掲示板に記載されるグループの入札情報への署名で防ぐことができる．

落札金額の正当性　入札の否認不可性とカウントダウン（アップ）の性質から満足される．またすべての応札者は，落札額が自分の入札価格よりも高い（低い）ことを検証することができる．

公平性　入札金額は本人しか知らないことと入札の否認不可性による落札額の操作防止により，ほかより有利な条件で入札できる応札者はいない．

6.2 他方式との比較

まず，談合の問題を議論した方式の比較を行う．今村らの方式[12]は，談合集団を新たに結成する機会をなくすことで，談合の事前対策を考案している．しかしながら，いったん談合集団が結成されたり前もって結成して応札する状況では，不正な落札価格の操作が行われてしまう．この点で，中西らの方式[22]や我々の方式は，談合による不正を無効化する性質を持っており，談合の事後対策を設けている．

次に応札者のプライバシ問題に着目して比較を行う．Kudoは時間管理機関を設けた入札方式[15]を提案している．この方式では，オークション主催者は入札金額しか知ることができない．しかし，売り手と結託することによってすべての入札者と入札金額との関係を把握することができる．今村ら[12]や中西ら[22]の方式も含め，応札の匿名性により応札者のプライバシを保護する方式では，匿名通信路や信頼できる機関の存在が必要不可欠である．

これに対し，菊池ら[13]や我々の方式では，応札価格を暗号論的基本技術で秘匿して応札者のプライバシを保護する．つまり，匿名性による方式よりも想定する仮定が小さくて済む．ここで，菊池らの方式は入札者の識別情報を秘密分散により複数のオークション主催者に分散して配布する．開示・落札時には，複数の主催者により，最大金額をつけた入札者の識別情報のみが復元される仕組みになっている．よって，応札者の識別情報の組合せを計算することが容易な場合，応札額の秘匿性が失われる危険性がある．

6.3 談合とプライバシ保護

中西らの方式[22]は談合による不正な落札価格操作を防止し，応札者のプライバシ保護を実現したことを記している．しかしながら，実は以下のようにどちらかが十分に満足されない場合がある．同方式では入札否認段階において不正者を検出する際，匿名性の仮定により応札された情報から個人を特定することはできない．不正者は否認していることが知れても，自分のユーザ識別子を名乗り出ることは考えられない．よって，不正者を特定するためには，その不正者の属するグループすべての応札者に自分のユーザ識別子を提示してもらう必要がある．これにより，個人情報を管理している機関の名簿と比較して，ユーザ識別子を提示しない不正者を特定することができる．しかし，この場合，自分のユーザ識別子を提示したすべての応札者のプライバシは侵害されていることになる．つまり，談合を完全に防ぐにはある応札者のプライバシを侵害する状況に陥る．逆にすべての応札者のプライバシを保護しようとすると，不正者を特定できないので談合による不正を防げないことになる．

我々の方式は，主催者に対する匿名性はないので，こういった状況は生じない．談合による不正防止と応札者のプライバシ保護の両方を満足する．

7. おわりに

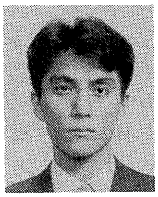
本稿では，談合による不正な落札価格の操作を防止し，応札者のプライバシを保護する実用的な電子オークション方式を示した．今後の課題として，匿名通信路や信頼できる機関を仮定とせず，だれが応札したかを暗号技術によって秘匿する手法を検討する．また，Franklin と Reiter の方式[8]のように，落札後からの決済まで盛り込んだシステム構築を目標とする．

謝　辞　電子オークションに関する貴重な議論と，参考論文などの有益な情報を提供してくださった東海大学の菊池浩明先生に深く感謝いたします．また，入札の否認不可性において貴重な助言をいただきました東芝の新保淳氏に心より感謝いたします．

参考文献

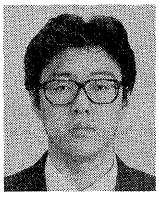
1) Boyar, J., Chaum, D. and Damgård, I.: Convertible undeniable signatures, *Advances in Cryptology – CRYPTO '90*, LNCS, Vol.537, pp.189–205 (1990).
2) Chaum, D.: Untraceable electronic mail, return addresses, and digital pseudonyms, *Comm. ACM*, Vol.24, No.2, pp.84–88 (1981).
3) Chaum, D.: Zero-knowledge undeniable signatures, *Advances in Cryptology – EUROCRYPT '90*, LNCS, Vol.473, pp.458–464 (1990).
4) Chaum, D. and van Antwerpen, H.: Undeniable Signatures, *Advances in Cryptology – CRYPTO '89*, LNCS, Vol.435, pp.212–216 (1989).
5) Cramer, R., Franklin, M., Schoenmakers, B. and Yung, M.: Multi-authority secret-ballot elections with linear work, *Advances in Cryptology – EUROCRYPT '96*, pp.72–83 (1996).
6) Damgard, I.: New convertible undeniable signature schemes, *Advances in Cryptology – EUROCRYPT '96*, LNCS, Vol.1070, pp.372–386 (1996).
7) FIPS 180-1: Secure hash standard, Federal Information Processing Standards Publication 180, U.S. Department of Commerce/N.I.S.T., National Technical Information Service (1993).
8) Franklin, M.K. and Reiter, M.K.: Verifiable signature sharing, *Advances in Cryptology – EUROCRYPT '95*, LNCS, Vol.921, pp.50–63 (1995).
9) Franklin, M.K. and Reiter, M.K.: The design and implementation of a secure auction service, *IEEE Trans. Softw. Eng.*, Vol.22, No.5, pp.302–312 (1996).
10) フリークション（電子オークションサイト），`http://jnet20.com/fleaction/index.html`
11) Gennaro, R., Krawczyk, H. and Rabin, T.: RSA-based undeniable signatures, *Advances in Cryptology – CRYPTO '97*, LNCS, Vol.1294, pp.132–149 (1997).
12) 今村幸宏，松本 勉，今井秀樹：電子匿名入札方式，1994年暗号と情報セキュリティ・シンポジウム，SCIS94-11B (1994).
13) 菊池浩明，中西祥八郎：利用者登録の不要な匿名オークション，コンピュータセキュリティシンポジウム '98, pp.243–248 (1998).
14) Koblitz, N.: Elliptic curve cryptosystems, *Mathematics of Computation*, 48, pp.203–209 (1987).
15) Kudo, M.: Secure electronic sealed-bid auction protocol with public key cryptography, *IEICE Trans. Fundamentals*, Vol.E81-A(1), pp.20–27 (Jan. 1998).
16) Miller, V.S.: Use of elliptic curves in cryptography, *Advances in Cryptology – CRYPTO '85*, LNCS, Vol.218, pp.417–426 (1985).
17) Michels, M., Petersen, H. and Horster, P.: Breaking and repairing a convertible undeniable signature scheme, *Proc. 3rd ACM Conference on Computer and Communications Security*, pp.148–152 (1996).
18) Michels, M. and Stadler, M.: Efficient convertible undeniable signature schemes, *Proc. 4th Annual Workshop on Selected Areas in Cryptography* (1997).
`http://www.geocities.com/CapeCanaveral/Lab/8983/publications.htm`
19) ネットプライス（電子オークションサイト），`http://netprice.lab.co.jp`
20) 入札制度問題研究会（編）：改訂版新公共人札・契約制度実務ハンドブック，建設省建設経済局建設業課（監修），大成出版社 (1994).
21) 中西 透，藤原 融，渡辺 創：匿名入札プロトコル，*Computer Today*, No.86, pp.24–29, サイエンス社 (1998).
22) 中西 透，渡辺 創，藤原 融，嵩 忠雄：否認不可署名を用いた匿名入札プロトコル，1995年暗号と情報セキュリティ・シンポジウム，SCIS95-B1.4 (1995).
23) Reiter, M.K. and Rubin, A.D.: Crowds: anonymity for web transactions, *ACM Trans. Information and System Security*, Vol.1, No.1 (Nov. 1998).
24) Rivest, R.L.: The MD5 message-digest algorithm, Internet Request for Comments 1321 (Apr. 1992).
25) 妹尾健史，菊池浩明，藤岡 淳，中西祥八郎：インターネット上の匿名通信路方式の評価，1998年暗号と情報セキュリティ・シンポジウム，SCIS98-3.3.E (1999).
26) Syverson, P.F., Goldschlag, D.M. and Reed, M.G.: Anonymous connections and Onion routing, *IEEE Symposium on Security and Privacy*, pp.44–54 (1997).

(平成11年1月21日受付)
(平成11年4月 1 日採録)



宮崎　真悟（正会員）

平成9年九州大学工学部情報工学科卒業．平成11年同大学院システム情報科学研究科情報工学専攻修了．同年（株）東芝入社．以来同社，SI技術開発センターにて，暗号理論，情報セキュリティの研究開発に従事．平成9年度電子情報通信学会学術奨励賞受賞．電子情報通信学会会員．



櫻井　幸一（正会員）

昭和61年九州大学理学部数学科卒業．昭和63年同大学院工学研究科応用物理専攻修了．同年三菱電機（株）入社．現在，九州大学大学院システム情報科学研究科助教授．1997年9月より1年間コロンビア大学計算機科学科客員として在籍．計算複雑性理論，暗号理論，情報セキュリティの研究に従事．「暗号理論の基礎」（1996年共立出版，監訳），「数論アルゴリズムと楕円暗号理論入門」（1997年シュプリンガー東京，訳），工学博士．電子情報通信学会，日本数学会各会員．