# 変換可能なグループ署名を用いた電子入札方式

宮崎真悟[†] 櫻井幸一[††]

本稿の目的は，入札における競争原理を高めることである．そこで，個人に特化した情報をいっさい公開しない検証可能な電子入札方式を提案する．個人に特化した情報の効果として，低い価格で落札を続けている応札者の情報が応札時に明らかになることで，他の応札希望者の参加意欲が失われることがある．また逆に，各応札者を識別する情報が公開されない場合，談合を行う寄合からの抜けがけが起こりやすくなる．以上より，個人に特化した情報を公開しない仕組みは，目的達成の1つの解決方法となる．本稿では，変換可能なグループ署名を提案し，これに基づく電子入札方式を構築する．

# An Electronic Sealed-bid Auction Scheme Based on a New Convertible Group Signature Scheme

Shingo Miyazaki[†] and Kouichi Sakurai[††]

In this paper, we discuss how to enhance the motivation for rivalry in the electronic sealed-bid auction. The existence of person, who often becomes the successful bidder with the low price, can dampen another incentive to participate in the sealed-bid auction. On the contrary, if the information identifying each bidder is never published, a member of group for bid rigging has a chance of sellout. So, we propose a verifiable sealed-bid auction scheme without publishing the information related to the identity of each bidder, based on a new convertible group signature scheme.

## 1. はじめに

### 1.1 匿名性と談合の問題

入札では，競り手の一般競争により落札価格が決定する．それゆえ，競争原理が機能しなくなると，競り手側で価格を自由に操作することが可能となる．指名競争入札がその良い例で，業者が談合により落札者と落札価格を決め，形式的な競争を行う．実際に談合疑惑に関する様々な事件[1)]が起こっているが，ここに競争はなく，寄合により落札価格と落札者が決定される．

このような背景には，入札時に他の応札者が分かることの事前要因と，また誰が落札したかを誰もが把握できることの事後要因がある．特に前者においては，井上ら[9)]による次のような状況も指摘されている．談合グループは不当に低い値段で落札を続けていく．これを繰り返し根強く行ってゆくことで，他の参加希望者の応札意欲を失わせる．徐々にグループ以外の参加人数を減らし，市場を独占することにより，対象物を自分たちの思うがままの値段で落札することができる．この指摘は，応札時の応札者に関する情報公開をいわば印籠のように扱うことで，参加意欲を操作するものである．

今村ら[10)]や井上ら[9)]では，次回入札への影響をなくすため，匿名応札方式を取り入れている．また中西ら[21)]は応札者のプライバシ保護という目的も含めて匿名性を満たす方式を提案している．ただし，これらの方式では主催者に対しても匿名であるので，落札時，自分の名前を名乗り出ない応札者や不正者を検出しにくいといった反面もある．

### 1.2 本稿の目的

本稿では，個人に特化した情報を主催者以外に公開しない仕組みで競争原理を円滑に働かせ，かつ不正者・脱落者を正確に把握できる方式を検討する．具体的に変換可能なグループ署名を提案し，これに基づく競り下げ電子入札方式[16)]の改良を試みる．

指針として，個人に特化した情報を公開する必要なく，かつ他応札者が落札の正当性を検証できるような仕組みを考える．これにより，次回入札への影響をな

† 株式会社東芝 SI 技術開発センター
System Integration Technology Center, Toshiba Corporation
†† 九州大学大学院システム情報科学研究院情報工学部門
Graduate School of Information Science and Electrical Engineering, Kyushu University

くし，事前効果による市場独占を防止する．また事後効果に関しては，グループ鍵で検証する落札情報だけが公開されるので，実際に誰が落札したかを主催者（落札者）以外が公開情報より知ることができない．これにより談合を行うグループから抜けがけを起こりやすくし，結果，入札を寄合のない競争状態へ導くことができる．

本稿では，個人に特化した情報を公開する際の問題点を述べ，これを解決する電子入札方式を検討する．その解決方法として，変換可能なグループ署名を提案する．本手法は否認不可署名からディジタル署名への変換時の変数公開をグループ署名にも適用したものである．効果として，検証者に応じて与える情報量を段階的に制御することができる．つまり，主催者には何らかの個人に特化した情報を与えるのに対し，他の応札者にはそういった特化情報を公開しない．それでもなお，落札者決定までの処理の正当性を証明および検証することができる．さらに，応札価格の秘匿性について議論し，提案方式の同性質を向上させる改良法もあわせて提案する．

## 2. 問題点と解決へのアプローチ

従来方式[16]では，公開掲示板に記載される情報として個人の署名検証用の公開鍵があった．よって，公開鍵と応札者の関係を知っている第三者は誰が落札したか，誰の入札であるかを，公開情報より把握することが可能である．

朝日新聞に記載された記事[1]を例にして考えてみる．譲り合いで落札している約 20 社でなる大手 A 級業者の中に，1 社談合に加わらない業者が他の業者の談合疑惑を証言したという事件である．この業者が加わる入札では競争原理が働き，落札価格が予想価格を大きく下回るが，一方の参加しない入札ではほぼ予想価格で落札されるという．この事件を観察すると，ある業者による寄合からの抜けがけが市場に競争原理を働かせていることが分かる．

ここで，一般的な入札で考えてみると，公開情報より応札者を識別する情報がなくなれば，談合を行う寄合からの抜けがけは起こりやすくなる．これにより，譲り合いによる落札形態が崩れ，自由競争による本来の入札形態を促すことができる．つまり，応札の匿名性を強め，入札の証拠を残さない方式は，談合による不正な価格操作を防止する効果を生み出す．

また，連続して入札が行われる場合，従来方式[16]では，公開情報より前回の落札者や応札者を見分けることができる．ここで次の状況が問題となってくる．ある応札グループはそれぞれ固定の公開鍵を用いて入札に参加し，高値をつけて繰り返し落札を続ける．これにより，このグループの公開鍵の存在が次第に他の参加意欲を損失させる働きを持ってくる．すると，この応札グループは市場を独占し，自分たちの思うがままの値段で落札することが可能となってくる．逆に，応札者の特質を確定づけるような情報が公開されなければ，掲示板の公開情報より参加意欲を奪う状況はなくなる．つまり，各入札での自由な価格競争が行われる．

このように個人に特化した情報を応札情報として与えないことは，入札に自由競争を働かせる 1 つの手段となる．ここでは，主催者以外の第三者に対して個人の特化情報を与えなければ十分である．従来方式[16]で用いた仮名の概念では，問題の解決になっていないことに注意する．毎回使いつづければ，仮名に応札者の特質をすり込むことができるからである．

そこで，本稿では応札者の特質を表す情報を主催者以外にいっさい公開しない入札方式を考える．その解決手段として，変換可能なグループ署名を提案する．

## 3. 変換可能なグループ署名

### 3.1 グループ署名

通常のディジタル署名では，個人の署名の検証には個人の検証鍵が用いられる．これは，入札の正当性を示すために通常のディジタル署名を使うと，おのずと個人に特化した情報を使わざるをえないことを意味する．つまり，通常のディジタル署名では 2 章に述べた問題点を解決できない．

そこで，我々は Chaum らによって提案されたグループ署名[5]の概念に注目する．グループ署名とは，構成メンバがグループを代表する署名を行い，同署名はそのグループの 1 つの検証鍵で正当性を検証できる署名方式である．ここで大事な性質は，生成された署名から実際に署名を行ったグループのメンバを特定できないことである☆．つまり，確かにグループを代表する署名であるが，実際の署名者を特定づけるような情報が存在しないのである．

この性質は，個人に特化した情報を用いないという解決手段に適合するものである．そこで本提案ではグループ署名の概念を適用する．

### 3.2 検証可能な署名への変換

ディジタル署名でもグループ署名でも署名対象となる文書が存在する．ここで，入札における署名すべき

☆ 厳密には，グループの管理者だけは署名を行ったメンバを特定できるが，ここでは一般の検証者を対象とした表記を行う．

対象とは応札価格である．入札を応札価格に対する署名送付とすると，この時点で自分の応札金額を主催者に通知するないしは一般に公開することになる．

後者の場合，応札締切ぎりぎりまで待った応札者はそれまでの応札価格をすべて把握して入札できる．ここで，入札時刻による応札の不公平が生じる．前者の場合でも，主催者が一部応札者にそれまでの応札価格を垂れ流す危険を問題としなければならない．そこで，従来の電子入札ないしは電子オークション方式では同問題が議論され，秘密分散共有法[12),23)]や，役割に応じた機関分散[13)]といった手法で対策がとられている．

本提案方式が今回基盤とする方式[16)]では，否認不可署名を用いることで，応札価格への署名と署名文書の暗号化という二面性を利用している．落札時に秘密情報の一部を検証者に渡すことで，暗号化の効果が解け，誰でも検証可能なディジタル署名に変換するという仕組みである．

よって本稿ではこの仕組みを 3.1 節で議論したグループ署名に適用し，落札時にのみ検証可能つまり落札価格が公開される手法を提案する．これを変換可能なグループ署名とする．

具体的に，否認不可署名のディジタル署名への変換時に解放される秘密情報が，同時にグループ署名をも検証可能にする．逆に同情報の解放なしには，グループ署名は署名者以外に検証できない．

本方式では，応札情報は否認不可署名部分とグループ署名部分で成る．否認不可署名部分は暗号化した応札価格と提示された価格との非等価性を証明・検証する手段として，一方のグループ署名部分は落札価格の正当性を証明・検証する手段として用いられる．

### 3.3 離散対数問題に基づく提案方式

検証時に署名者が必要となる否認不可署名を通常のディジタル署名に変換する落し戸を，同時にグループ署名に適用する．つまり，否認不可署名から通常のディジタル署名変換時に，その署名限定の秘密情報が解放された時点で，対をなすグループ署名が検証可能となる．同手法を離散対数問題に基づいて設計した方式を以下に示す．

署名者 Alice は 2 つの秘密署名鍵 $x_1, x_2 \in Z_q^*$ を選び，$y_1 = \alpha^{x_1} \pmod p$ と $y_2 = \alpha^{x_2} \pmod p$ をそれぞれに対応する検証鍵とする．仕様上，$(x_1, y_1)$ が長期使用の署名・検証鍵で，$(x_2, y_2)$ が使い捨て署名・検証鍵と考える．

また独立して，Alice は自分の属するグループの秘密鍵 $x_G$ を持ち，対応する公開鍵 $P_G = \alpha^{x_G} \pmod p$ が公開されている．今，Bob だけが Alice の長期使用の検証鍵 $y_1$ を知っているものとする．

文書 $m$ に対する否認不可署名とグループ署名の対を生成するとき，Alice は以下を行う．まず Alice は乱数 $k, \mu \in Z_q^*$ を生成し，

$$r = \alpha^k \pmod p$$
$$\lambda = \alpha^\mu \pmod p$$

を計算する．それから以下を計算する．$\mathcal{H}(\cdot)$ は無衝突一方向性ハッシュ関数とする．

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

さらにグループ署名部分を計算する．

$$t = \frac{\tilde{r}\mu + rk}{x_G + \mathcal{H}(m, \tilde{r}, \lambda)} \pmod q$$

ここで，文書 $m$ に対し，$(\tilde{r}, s, \lambda, \tilde{\lambda})$ を否認不可署名，$(\tilde{r}, t, \lambda)$ をグループ署名とする．ここで，Alice 以外は $r$ を知らないので，Bob を含めた他のエンティティは Alice なしでは両署名を検証することができない．

Alice が使い捨ての秘密鍵 $x_2$ を Bob に解放すると，否認不可署名は下記のように $y_1$ を知る Bob が検証可能なディジタル署名に変換される．

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

またこのとき，Bob（または Alice 本人）が $r = \tilde{r}^{x_2^{-1}}$ を公開することで，グループ署名は下記のように誰にでも検証可能なディジタル署名に変換される．

$$\lambda^{\tilde{r}} r^r = (P_G \alpha^{\mathcal{H}(m, \tilde{r}, \lambda)})^t \pmod p$$

## 4. 提案する電子入札方式

本章では，個人に特化した情報をいっさい公開しない電子入札方式を提案する．

### 4.1 モデル

本方式では，以下の構成機関が存在する．

**主催者：** 開示プロトコルにおいては，応札者内の最低入札価格が決定するまで，ある周期で公開掲示板の金額を更新する．最低価格で入札した応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：** 応札者の登録業務を行う．応札者の認証を行い，送付された鍵への証明書を発行する．

**依頼人：** 工事やプログラム作成などの仕事を提示し，

一番低い価格をつけた落札者にその仕事を依頼する．

**応札者：** 依頼人が提示した仕事に対し，購入・請負を目的とする．応札時に，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：** 誰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主催者のみ行える．

### 4.2 要求条件

本提案方式は以下のすべての条件を満足する．

**応札価格の秘匿性：** 敗者の応札価格は主催者も含め誰にも露呈しない．

**応札価格の健全性：** 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）．

**落札価格の正当性：** 落札価格がすべての応札価格の中での最低価格である．

**公平性：** ある応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．

**無証拠性：** 公開情報から ID や個人検証鍵といった各応札者に特化した情報は露呈しない．関連して，落札者決定処理の正当性を検証する際に，各応札者に特化した情報を必要としない．

### 4.3 プロトコル

**［初期設定］**

システムパラメータ $(p, q, \alpha)$ が公開されている．$p$, $q$ は大きな素数で，$p = 2q + 1$ の関係が成り立っている．$\alpha$ は乗法群 $Z_p^*$ での位数が $q$ となるような生成器である．$\mathcal{H}$ を無衝突一方向性ハッシュ関数とする．

**［登録プロトコル］**

主催者は応札者をいくつかのグループに分け，各グループ $j$ の署名用秘密鍵 $S_{Gj}$ を登録時に秘密裡に送付する．簡単のため，グループ $j$ に属する応札者 $A$ が応札する場合を考え，属するグループの秘密鍵を $S_G$，公開鍵を $P_G = \alpha^{S_G} \pmod p$ とする．また応札者 $A$ の常用の秘密鍵を $S_A$，公開鍵を $P_A = \alpha^{S_A} \pmod p$，対応する鍵証明書を $Cert_A$ とする．

**［応札プロトコル］**

Step.1：主催者は入札金額を $m$ 種類用意する．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：応札者 $A$ は出品物に対し，準備された価格集合：$\{w_1, w_2, \ldots, w_m\}$ の中から，応札金額 $w_k$ $(1 \le k \le m)$ を 1 つ選ぶ．次に，乱数 $x, k, \mu \in Z_q^*$ を選び，以下を計算する．

$$h = \alpha^x \pmod p$$
$$r = \alpha^k \pmod p$$
$$\tilde{r} = r^x \pmod p$$
$$\lambda = \alpha^\mu \pmod p$$
$$\tilde{\lambda} = \lambda^x \pmod p$$
$$c = \mathcal{H}(w_k, \tilde{r}, \lambda, \tilde{\lambda})$$
$$\sigma = k - cS_A \pmod q$$

さらに，グループ署名を計算する．

$$t = \frac{\tilde{r}\mu + rk}{S_G + \mathcal{H}(w_k, \tilde{r}, \lambda)} \pmod q$$

応札者は $(P_A, Cert_A, h, \tilde{r}, \lambda, \tilde{\lambda}, \sigma, t)$ を主催者に送る．

Step.3：主催者は証明書 $Cert_A$ の正当性を検証する．正当である場合，$(h, \tilde{r}, \sigma, t)$ を公開掲示板の該当するグループ欄に記載する．

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．

**［開示・落札プロトコル］**

Step.1：主催者は公開掲示板の現在価格 $W$ に一番低い金額 $w_1$ を設定する．

Step.2：現在価格 $W$ で入札した応札者 $j$ は主催者にその旨通知し，応札の確証プロトコルを用いて，応札の正当性と価格の一致性を証明する（付録にある $\log_\beta z = \log_\alpha y$ の証明．ただし，$z = \tilde{r}$，$y = h$，$\beta = \alpha^\sigma P_A^{\mathcal{H}(w_i, \tilde{r}, \lambda, \tilde{\lambda})}$ とする）．誰もいない場合は，各応札者は自分の入札金額が現在価格でないことを否認プロトコルを用いて証明する（付録にある $\log_\beta z \neq \log_\alpha y$ の証明☆）．

主催者は $W$ に対する入札否認の正当性を確認した後，次に高い金額 $w_2$ を設定する．$W$ で入札した応札者が現れるまで，この処理を繰り返す．

Step.3：ある金額 $w_k$ において，応札者 $A$ が通知を行った場合は以下のようにして入札の正当性を検証する．

3a： まず応札者 $A$ は $x$ を主催者に送付する．

3b： 主催者は $(\tilde{r}, \sigma, x, w_k, \lambda, \tilde{\lambda})$ と公開鍵 $P_A$ を用いて署名を検証する．

$$\tilde{r} = (\alpha^\sigma P_A^{\mathcal{H}(w_k, \tilde{r}, \lambda, \tilde{\lambda})})^x \pmod p$$

☆ 適用する Michels-Stadler 否認不可署名方式[15]では，$P_A$ を公開しなくても，離散対数の等価・非等価を検証できる．

**表 1** 主催者への情報と公開情報
Table 1 Knowledge only known to the auctioneer and public data.

| | 応札時データ | 否認時新規データ | 落札時新規データ |
|---|---|---|---|
| 主催者 | $P_G, (P_A, Cert_A, h, \tilde{r}, \lambda, \tilde{\lambda}, \sigma, t)$ | — | $x$ |
| 公開掲示板 | $P_G, (h, \tilde{r}, \sigma, t)$ | $\beta$ | $\lambda, r$ |

次に $\tilde{\lambda} = \lambda^x \pmod p$ の一致性を確認する．これが正当であれば，$r = \tilde{r}^{x^{-1}} \pmod p$ を計算し，グループ署名を検証する．

$$\tilde{\lambda}^{\tilde{r}}\tilde{r}^{r} = (P_G \alpha^{\mathcal{H}(w_k, \tilde{r}, \lambda)})^{tx} \pmod p$$

個人署名とグループ署名双方が正当であるならば，$(r, \lambda)$ を公開する．一般応札者は，$(\lambda, r, \tilde{r}, t, w_k, P_G)$ を用いて，落札価格の正当性を確認する．

$$\lambda^{\tilde{r}} r^{r} = (P_G \alpha^{\mathcal{H}(w_k, \tilde{r}, \lambda)})^{t} \pmod p$$

## 5. 応札価格の秘匿性に関する問題点と改良

### 5.1 問 題 点

選択する応札価格の種類が少ない場合，すべての応札価格 $w_i \in W = \{w_1, w_2, \ldots, w_m\}$ を検証式に代入して一致性を検証することで，任意の応札者の応札価格 $w_k \in W$ を探り出すことができる．具体的な検出アルゴリズムを次に示す．

主催者はすべての応札価格 $w_i \in W$ に対して，以下の検証を行う．

(1) ある $w_i$ に対し，与えられた応札情報から以下を計算する．

$$\begin{aligned} R(w_i) &= \alpha^{\sigma} P_A^{c(w_i)} \pmod p \\ &= r P_A^{-c(w_k)} P_A^{c(w_i)} \pmod p \end{aligned}$$

ここで，$w_i = w_k$ の場合，$R(w_i) = r$ となる．

(2) (1) で計算した $R(w_i)$ に対し，以下の検証式の一致性を検証する．

$$(P_G \alpha^{\mathcal{H}(w_k, \tilde{r}, \lambda)})^{t} \stackrel{?}{=} \lambda^{\tilde{r}} R(w_i)^{R(w_i)} \pmod p$$

一致しない場合は，別の $w_j$ $(j \neq i)$ で，(1) からやり直す．一致するとき，$w_i = w_k$ であり，主催者は応札価格 $w_k$ を知ることができる．

上記アルゴリズムは，“Polynomially Secure” の議論に精通するところがある．つまり，『メッセージ空間 $M = \{m_1, m_2\}$ と暗号化関数 $Enc$ があるとき，暗号化データ $Enc(m_1)$ が与えられてこれが $m_1$ の暗号文であることを 1/2 以上の確率で識別できないとき，$Enc$ は “Polynomially Secure” である』という議論[18]である．

応札価格がある暗号化関数で暗号化されているが，そのメッセージ空間（応札価格の集合）の大小によって識別の手間が変わる．メッセージ空間を大きくすれば，応札価格の秘匿性は高まるが，落札者決定の処理効率が悪くなる．逆に小さいと処理効率は高まるが，上記アルゴリズムによる応札価格の識別が容易になる．

よって，次節では，発見的であるが，“Polynomially Secure” 方式に変形する改良プロトコルを示す．

### 5.2 改良プロトコル

モデルや初期設定，登録プロトコルは 4 章と同じである．問題点を解決するため，応札/開示・落札プロトコルを以下のように改良する．

**[改良応札プロトコル]**

Step.1：主催者は入札金額を $m$ 種類用意する．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：応札者 $A$ は出品物に対し，準備された価格集合：$\{w_1, w_2, \ldots, w_m\}$ の中から，応札金額 $w_k$ $(1 \leq k \leq m)$ を 1 つ選ぶ．次に，乱数 $x, k, \mu \in Z_q^*$ を選び，以下を計算する．

$h = \alpha^x \pmod p$
$r = \alpha^k \pmod p$
$\tilde{r} = (r^r)^x \pmod p$
$\lambda = \alpha^{\mu} \pmod p$
$\tilde{\lambda} = \lambda^x \pmod p$
$c = \mathcal{H}(w_k, \tilde{r}, \lambda, \tilde{\lambda})$
$\sigma = rk - cS_A \pmod q$

さらに，グループ署名を計算する．

$$t = \frac{\tilde{r}\mu + rk}{S_G + \mathcal{H}(w_k, \tilde{r}, r, \lambda)} \pmod q$$

応札者は $(P_A, Cert_A, h, \tilde{r}, \lambda, \tilde{\lambda}, \sigma, t)$ を主催者に送る．

Step.3：主催者は証明書 $Cert_A$ の正当性を検証する．正当である場合，$(h, \tilde{r}, \sigma, t)$ を公開掲示板の該当するグループ欄に記載する．

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．

**[改良開示・落札プロトコル]**

Step.1：主催者は公開掲示板の現在価格 $W$ に一

番低い金額 $w_1$ を設定する．

Step.2：現在価格 $W$ で入札した応札者 $j$ は主催者にその旨通知し，応札の確証プロトコルを用いて，応札の正当性と価格の一致性を証明する（付録にある $\log_\beta z = \log_\alpha y$ の証明．ただし，$z = \tilde{r}$，$y = h$，$\beta = \alpha^\sigma P_A^{\mathcal{H}(w_i,\tilde{r},\lambda,\tilde{\lambda})}$ とする）．誰もいない場合は，各応札者は自分の入札金額が現在価格でないことを否認プロトコルを用いて証明する（付録にある $\log_\beta z \neq \log_\alpha y$ の証明☆）．

主催者は $W$ に対する入札否認の正当性を確認した後，次に高い金額 $w_2$ を設定する．$W$ で入札した応札者が現れるまで，この処理を繰り返す．

Step.3：ある金額 $w_k$ において，応札者 $A$ が通知を行った場合は以下のようにして入札の正当性を検証する．

3a： まず応札者 $A$ は $(x, r)$ を主催者に送付する．

3b： 主催者は $(\tilde{r}, \sigma, x, w_k, \lambda, \tilde{\lambda})$ と公開鍵 $P_A$ を用いて署名を検証する．

$$\tilde{r} = (r^r)^x \pmod p$$
$$\tilde{r} = (\alpha^\sigma P_A^{\mathcal{H}(w_k,\tilde{r},\lambda,\tilde{\lambda})})^x \pmod p$$

次に $\tilde{\lambda} = \lambda^x \pmod p$ の一致性を確認する．これが正当であれば，グループ署名を検証する．

$$\tilde{\lambda}^{\tilde{r}}\tilde{r}^r = (P_G\alpha^{\mathcal{H}(w_k,\tilde{r},r,\lambda)})^{tx} \pmod p$$

個人署名とグループ署名双方が正当であるならば，$(r, \lambda)$ を公開する．一般応札者は，$(\lambda, r, \tilde{r}, t, w_k, P_G)$ を用いて，落札価格の正当性を確認する．

$$\lambda^{\tilde{r}} r^r = (P_G\alpha^{\mathcal{H}(w_k,\tilde{r},r,\lambda)})^t \pmod p$$

## 6. 考　　察

### 6.1 提案方式の正当性

改良を加えた提案方式が要求条件を満たしているかを議論する．

**応札価格の秘匿性：** 敗者の応札価格は，入札終了まで暗号化されたままであるため，$(x, r)$ を持つ本人以外は復号できない

**応札価格の健全性：** 入札当事者以外は正当な入札を行うための個人秘密鍵 $S_A$ を知らないので，入札内容を改竄することはできない．

**落札価格の正当性：** 入札の否認不可性と選択範囲にある最小価格から値を上げてゆく手法の性質から満足される．またすべての応札者は，落札価格が自分の入札価格よりも低いことを検証することができる．

**公平性：** すべての応札価格は落札時まで本人しか知らないことと，落札価格を操作する不正を防止する仕組みにより，他より有利な条件で入札できる応札者はいない．

**無証拠性：** 各応札者について，公開される情報はランダムな要素を含む暗号化された応札価格と，その応札者の属するグループの検証鍵である．よって応札者の特質を表現できる変数はなく，また落札価格決定に至るまでの否認証明は，各応札者の個人情報を用いて主催者が計算する情報で他の応札者はその正当性を検証することができる．同情報はランダムな変数との関数値のため，応札者に特質を帯びた情報は露呈しない．

### 6.2 敗者の応札価格を秘匿する方式

敗者の応札価格を秘匿する方式についての比較を行う．我々のほかに，井上・松本方式[9]や佐古方式[23]が提案されている．井上・松本方式[9]や我々の方式では，入札内容や購入意思を開示することは応札者自身にしかできない．これに対し，佐古方式では主催するセンター群の公開鍵で暗号化されているので，応札内容の秘密性はセンター群の信頼性に依存している．ただし，逆に佐古方式では入札後は応札者との通信は必要なく，センター群で復号化処理を行うだけである．この点において，入札後の通信を必要とする井上・松本方式や我々の方式よりも効率的である．

井上方式は，匿名型ネットワークの存在を仮定していることや，応札の否認に対する対処を行っていない点で我々と異なる．

### 6.3 否認の同時性

井上・松本方式[9]や小林・森田方式[11]，本提案方式のように購入意思や否認証明を一定の期間に送る方式では，送付順序と開示処理への配慮が必要である．つまり，中西ら[21]が議論している，入札否認による談合グループの不正な応札価格操作を適用できるからである．特に井上・松本方式では，主催者が応札者を特定できない匿名性を悪用して，次のように不正を行うことが可能である．

今，井上・松本方式の競争段階において，ある金額

☆ 適用する Michels-Stadler 否認不可署名方式[15]では，$P_A$ を公開しなくても，離散対数の等価・非等価を検証できる．

**表 2** 改良方式における主催者への情報と公開情報
Table 2 Knowledge only known to the auctioneer and public data in the improved scheme.

| | 応札時データ | 否認時新規データ | 落札時新規データ |
|---|---|---|---|
| 主催者 | $P_G, (P_A, Cert_A, h, \tilde{r}, \lambda, \tilde{\lambda}, \sigma, t)$ | — | $r, x$ |
| 公開掲示板 | $P_G, (h, \tilde{r}, \sigma, t)$ | $\beta$ | $\lambda, r$ |

に対する暗号化された請負意志を開示する状況を考える．ここで，談合グループはできるだけ高い価格で，しかも必ず落札したい（仕事を請け負いたい）と考える．請負意志（Yes/No）はリアルタイムに開示されていくので，談合グループのメンバは他の応札者すべての意志を確認することができる．その金額で，メンバ以外が請負の意志を示していないようであれば，談合グループは落札価格をつり上げたいと考える．このとき，同金額で実際に “Yes” を送っていたメンバは開示を否認し，競売を途中で降りる．この処理を繰り返すことで，談合グループは落札価格をできるだけ上げるような不正が可能である．ここでは，途中で降りることに対し，主催者は応札の匿名性により何の罰金も請求することができない．

一方，小林・森田方式や本提案方式では匿名性を必要条件としないため，まず主催者は誰が途中で降りようとしているかを特定できる．またハッシュ値や否認不可署名という証拠が残っているので，これを基に罰金を請求することができる．しかし，計算機の故障といった諸々のネットワーク問題を考えると，高額の罰金を設定することは考えにくい．ただし逆に罰金を少額に設定すると，多少の罰金を覚悟で価格操作の不正を行うことができる．

この問題に対する単純な解決法は，購入意思や否認証明をいったん主催者だけに送り，すべての応札者からの通知を受け取った段階で公開すればよい．これにより，意思・証明の送付順序を悪用した落札価格操作を防止することができる．ただし，主催者が一部の応札者に情報の垂れ流しを行わない，という仮定が必要となる．これは機関への信頼性をシステム構築の仮定から除外する，という意図から外れるものである．

### 6.4 一方向性関数を用いた高速な方式との比較

Stubblebine ら[24]や，小林ら[11]は，リバースハッシュ関数を用いた高速なオークション方式を提案している．前者は応札者の金額がオンラインで刻まれてゆく English 方式となっている．そのため，主催者に個人情報と応札内容の連結情報を渡さないためには，匿名通信路といった匿名性を確立する機構が必要である．

一方，後者では本稿と同じく，入札と Dutch 方式の混合方式になっている．また文献 16) の方式が持つ性質を持ち，かつ一方向性関数を巧みに利用した高速な方式である．ただし，各応札者の署名検証には，個人の公開鍵や仮名を用いることから，本稿で論じた問題を議論する必要がある．

## 7. おわりに

本稿では変換可能なグループ署名方式を提案し，同方式に基づき匿名性を強化する手法を示した．これは，入札の競争原理を促進する性質を持っている．本稿の提案手法では，抜けがけした応札者を公開情報から簡単に限定することはできないが，完全な無証拠性を備えてはいない．この点を今後検討する必要がある．また方式の安全性はいまだ発見的であるため，厳密な証明を今後の課題とする．

## 謝　辞

応札価格の秘匿性に関する問題点について，貴重なご指摘をいただいた査読者の方々に心より感謝申し上げます．

## 参考文献

1) 落札価格高止まり，朝日新聞朝刊 (1999.2.4).
2) Boyar, J., Chaum, D. and Damgard, I.: Convertible undeniable signatures, *Advances in Cryptology – CRYPTO '90*, LNCS, Vol.537, pp.189–205 (1990).
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) Chaum, D. and van Heyst, H.: Group signatures, *Advances in Cryptology – EUROCRYPT '91*, LNCS, Vol.547, pp.257–265 (1991).
6) 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).
7) Camenisch, J. and Michels, M.: A group signature scheme with improved efficiency,

*Advances in Cryptology – ASIACRYPT '98*, LNCS, Vol.1514, pp.160–174 (1998).
8) 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).
9) 井上信吾，松本　勉：電子匿名競売プロトコルに関する一考察，信学技報，ISEC95-5, pp.31–38 (1995).
10) 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).
11) 小林邦生，森田　光：大小比較に一方向性関数を用いた効率的な入札方式，信学技報，ISEC99-30, pp.31–37 (1999).
12) 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).
13) Kudo, M.: Secure electronic sealed-bid auction protocol with public key cryptography, *IEICE Trans. Fundamentals*, Vol.E81-A(1), pp.20–27 (1998).
14) 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).
15) Michels, M. and Stadler, M.: Efficient convertible undeniable signature schemes, *Proc. 4th Annual Workshop on Selected Areas in Cryptography* (*SAC '97*) (1997).
16) 宮崎真悟，櫻井幸一：公開掲示板を用いた秘策可能な電子入札システム，1999 年暗号と情報セキュリティシンポジウム，pp.41–46 (1999).
17) 宮崎真悟，櫻井幸一：グループ鍵を用いた匿名電子入札方式，コンピュータセキュリティシンポジウム '99, pp.117–122 (1999).
18) Menezes, A.J., van Oorschot, P.C. and Vanstone, S.A.: *HANDBOOK of APPLIED CRYPTOGRAPHY*, CRC Press (1997).
19) Miyazaki, S. and Sakurai, K.: A bulletin-board based digital auction scheme with bidding down strategy, *Proc. 1999 International Workshop on Cryptographic Techniques and E-Commerce*, pp.180–187 (1999).
20) 宮崎真悟，櫻井幸一：公開掲示板を用いた競り下げ電子オークション方式，情報処理学会論文誌, Vol.40, No.8, pp.3329–3336 (1999).
21) 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).
22) Petersen, H.: How to convert any digital signature scheme into a group signature scheme, *Security Protocols*, LNCS, Vol.1361, pp.178–190 (1997).
23) 佐古和恵：落札値以外を秘匿する全体検証可能な電子入札方式，1999 年暗号と情報セキュリティシンポジウム，pp.35–39 (1999).
24) Stubblebine, S.G. and Syverson, P.F.: Fair online auctions without special trusted parties, *Preproc. Financial Cryptography* (1999).
25) 山村三朗：ネットワーク上における入札の一手法，1988 年暗号と情報セキュリティワークショップ講演論文集，pp.41–50 (1988).

## 付録　離散対数の等価・非等価証明

離散対数の等価性・非等価性を証明する Michels らの手法[15]を記す．$z = \beta^x \pmod p$ と $y = \alpha^x \pmod p$ を満たす $x \in Z_q^*$ が存在するとき，等価性：$\log_\beta z = \log_\alpha y$ であること，また逆に，非等価性：$\log_\beta z \neq \log_\alpha y$ を証明するプロトコルである．

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，$r_\alpha = \alpha^k$，$r_\beta = \beta^k$，$\tilde{r}_\alpha = \alpha^{\tilde{k}}$，$\tilde{r}_\beta = \beta^{\tilde{k}} \pmod p$ 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

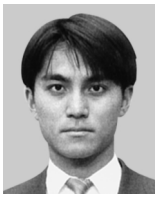
$$\alpha^s y^{v+w} = r_\alpha \pmod p$$
$$\alpha^{\tilde{s}} r_\alpha^{v+w} = \tilde{r}_\alpha \pmod p$$
$$\beta^{\tilde{s}} r_\beta^{v+w} = \tilde{r}_\beta \pmod p$$

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）：$\beta^s z^{v+w} \neq r_\beta \pmod p$

(平成 11 年 11 月 26 日受付)
(平成 12 年 6 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．現在，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，平成11年度情報処理学会論文賞受賞．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院情報工学部門助教授．平成9年9月よりコロンビア大学計算機科学科客員として1年間在籍．暗号理論・情報セキュリティ・計算複雑性理論・アルゴリズム工学・社会情報科学の研究に従事.「暗号理論の基礎」（平成8年，共立出版，監訳),「数論アルゴリズムと楕円暗号理論入門」（平成9年，シュプリンガー東京，訳），工学博士．平成11年度情報処理学会論文賞，平成11年度情報処理学会酒井記念特別賞受賞．電子情報通信学会，日本数学会各会員．