電気通信大学紀要 16 巻 1 号 pp.15-21（2003）〔解説〕

電子オークションプロトコルの技術動向

— 第一価格秘密入札プロトコルについて —

太 田 和 夫* 今 井 識† 森 田 光‡§

Technical Trends of Electronic Auction Protocols

— First-price Sealed-bid Auction Protocols —

Kazuo Ohta Satoru Imai Hikaru Morita

Abstract

Auction is one of the methods assigning something such as goods or works to two or more people, called bidders. The well-known auction is English auction. This is an auction such that bidders bid up a price, and the highest bidder is determined as the winner when bidding time is over. On the other hand, for selections of order-received constructor of public-works, another type of auction, first-price sealed-bid auction is generally used. In this type of auction, first, each bidder bids for her/his price, and when the bids are opened, the highest (lowest) price bidder is determined as the winner, and gets goods or works at the price for which she/he bids. In this paper, we introduce the current technical trends of electronic first-price sealed-bid auction protocols, using cryptographic techniques for the purpose of keeping bidders' privacy and robustness of the protocols.

Keywords: electronic auction, commitment, hash function, hash chain, public-key cryptosystem

* 電気通信大学電気通信学部情報通信工学科，Department of Information and Communication Engineering, The University of Electro-Communications

† 電気通信大学 大学院電気通信学研究科 情報通信工学専攻 Graduate School of Electro-Communications, The University of Electro-Communications

‡ NTT サービスインテグレーション基盤研究所，NTT Service Integration Laboratories

§ 電気通信大学 大学院情報システム学研究科 情報システム運用学専攻 客員教授，Graduate School of Information Systems, The Universityof Electro-Communications

1　はじめに

1.1　オークションとは

オークション（入札）とは，財，仕事等（以下財という）を割り当てる方法のひとつである。

オークションの構成要素として，図１を考える。オークションの参加者には，主催者（売り手や発注元）と入札者（買い手や受注希望者）がいる。主催者と入札者は，双方とも複数いる場合がある．また，信頼できる第三者（Trusted Third Party, 以下TTPとよぶ）を置く場合もある。

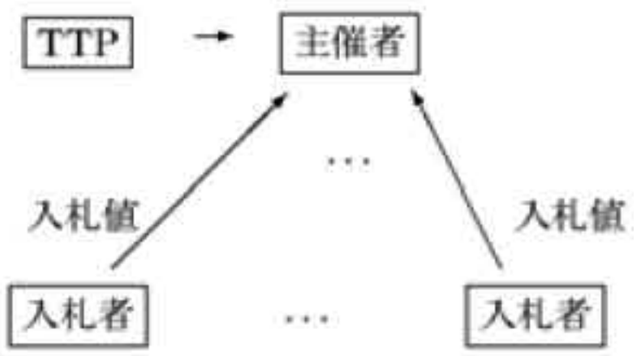

図１：オークションの構成要素

従来から，骨董品のオークション，市場での競り，公共事業の入札[1]など，社会の中でオークションは広く行われてきた。そこでは，オークション開始前に入札者が予め入札者としての資格をみたすことの確認や，信用できる主催者がオークションの場を提供しているとの暗黙の前提のもとに，入札・開札が行われてきた。従来のオークションを電子化する場合には，TTPを前提としたプロトコルを適用できよう。

オークションには，割り当てる財の種類および数（ユニット）がそれぞれ単数のものと複数のものが存在する。例えば，複数の商品を，「10個のセットで1,000円で買いたい」とか，「ふたつ揃っていたら10,000円出すけど，1つずつだったら１個3,000円」などという込み入った条件で入札をするオークションもあり得る。また，落札者が複数人いるようなオークションも考えられる[1]。

今回は最もシンプルな，単一種類，単一ユニットの場合に限定して，電子オークションの技術動向を紹介する。

1.2　オークションプロトコル[1]

まず，代表的な単一種類，単一ユニットのオークションプロトコルを紹介する。

第一価格秘密入札 (First-price sealed-bid auction)：各入札者は他の入札者の入札値を知らされずに入札する。最高値の入札者が，その値で落札する。

英国型 (English auction)：入札値は公開され，入札者は自分の入札値を上方に自由に変えることができる。誰も値の変更をのぞまなくなった時点で，最高値の入札者が自分の入札値を支払う。

オランダ型 (Dutch auction)：主催者は最初の値段を宣言し，ある買手がストップというまで価格を下げていく。ストップと言った入札者が，その時点での値で落札する。

第二価格秘密入札 (Second-price sealed-bid auction/ Vickrey auction)：各入札者は他の入札者の入札値を知らされずに入札する。最高値の入札者が，二番目の値で落札する[2]。

以下では，比較的普及しているオークションの中で，プライバシを守り，落札者と落札値以外の余計な情報をもらさないことを目的とした，第一価格秘密入札に限定して話をする。

2　電子オークションプロトコルの要求条件

2.1　背景

近年，インターネットなどのオープンネットワークの普及により，インターネットオークションなどの新しいタイプのオークションの必要性が生じている。すなわち，不特定多数の個人が入札者として参加するタイプのオークションであり，更には個人が主催者として自ら所有する財を競売にかけるような形態までもが予想される。

新しいオークションでは，誰でも簡単に参加することができる半面，事前に入札者を特定できなかったり，オークションの主催者が本当に信用できる相手なのかどうかがわからず入札者が不安を感じるなど，従来のオークションの暗黙の前提とみなされてきた「主催者と入札者の間の信頼関係」が成立しなくなると予想される。従って，TTPに安全性の根拠を頼らなくとも安全が保証できるプロトコルが必要となろう。

また，入札値は嗜好などを表す個人情報なので，入札者のプライバシーを重視する観点から，オークションで第三者にもれる情報は，落札者と落札値のみの必要最小限あることが望ましい。もし，個人情報を自らコントロールできるようなプロトコルが実現できるなら，その方が利用者として安心してオークションに参加できよう。

2.2　要求条件

以上の背景をふまえて，第一価格秘密入札オークションプロトコルの要求条件には，以下のようなものが設定されている[2][3][4]。

1 公共事業の入札は低い価格をつけたものを落札者とするが，今回は説明の簡単化のため，高い価格をつけたものを落札者とするオークションのみを例にとる。

2 第二価格秘密入札方式は，Vickreyにより経済学的に最適なオークションであることが証明されているが，これは世の中で広く普及しているとは言えない。

入札値の秘匿性：落札値以外の入札値を知ることができないこと。

頑強性：入札者の不正な入札を排除または検出できること。

公開検証可能性：誰でも，正しく落札者が決定されているか否かを納得できること。

入札の効率：入札者において，プロトコル実行にかかる計算量および通信量が少ないこと。

開札の効率：主催者において，プロトコル実行にかかる計算量が少ないこと。

入札者の Walk Through 性：入札者は入札時に一度だけ立ち会って，開札時には立ち会わずに済むこと。

3　基本技術

電子オークションプロトコルを実現するための基本技術を，以下に列挙する。なお，以降の説明で用いる記号は次のとおり。

［記号］

m	：	主催者の数
n	：	入札者の数
H,G	：	ハッシュ関数
k	：	価格の総数
p_{max}	：	最高価格
p_{min}	：	最低価格
v_i	：	入札者 i の入札値
p	：	価格
pk_p	：	価格 p に対応する公開鍵
sk_p	：	価格 p に対応する秘密鍵
IV^i	：	入札者iのハッシュ連鎖の初期値

3.1　公開鍵暗号

公開鍵暗号では，異なる鍵を２つ用意し，一方を公開し，もう一方を秘密にする。公開された鍵（公開鍵）から落し戸（秘密鍵）を求めることが現実的な時間内にできないことを前提としている。公開鍵を用いてメッセージから暗号文を得ることと，秘密鍵を用いて暗号文からメッセージを得ることは容易だが，秘密鍵なしで暗号文からメッセージを得るのは困難である。送信者は受信者の公開鍵を用いてメッセージから暗号文を作り，受信者は自分の秘密鍵で暗号文からメッセージを得る。

共通鍵暗号では，通信する相手の数だけ鍵を準備する必要がある。しかし公開鍵暗号では，暗号化に必要な公開鍵を他人に知られても問題ないため，１人あたり１組の公開鍵と秘密鍵を保持するだけで，不特定多数の相手と秘密通信が可能となる。この特徴は，あらかじめ通信相手が決まっていないインターネットのようなオープンネットワークとの親和性があり，実際 SSL などで使われている。

3.2　ハッシュ関数

ハッシュ関数は，一般的に以下のような性質をもつ関数である[5]。

- preimage resistance（一方向性）
  ある y が与えられているとき $H(x')=y$ なる x'を見つけることが計算量的に困難である。
- 2nd-preimage resistance（耐衝突性）
  あるxに対して $H(x)=H(x')$ をみたすような$x'\neq x$見つけることが計算量的に困難である。

3.3　コミットメント

コミットメントとは，送り手と受け手の間で行われる以下のような手続きである。

［**コミットフェーズ**］　送り手は受け手に対して，ある値 v をコミットする。この時点では，受け手はその値の内容を知ることができない。

［**オープンフェーズ**］　送り手が受け手に値を明かす。このとき，送り手がコミットした値と明かした値が等しいことが保証される。

一般的に，このようなコミットメントは一方向性関数により実現されることが知られている。

4　第一価格秘密入札プロトコルの例

第一価格秘密入札プロトコルとしていくつか例をあげて，これらの特徴を説明しよう。

4.1　コミットメントを用いた方式[6]

入札者iは，入札値v_iと乱数r_iに対するコミットメント値c_iを作成し，c_iを主催者に送ることにより入札を行う。r_iを用いることにより，c_iの取りうるパターンを増やしていることに注意。開札フェーズで，入札者iは（v_i, r_i）を主催者に送る。入札フェーズでは主催者はc_iしか知らないので，ハッシュ関数のもつ一方向性により，v_iを知ることができないことに注意。

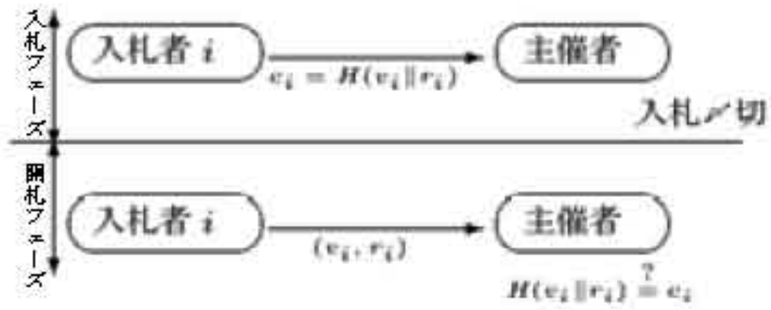

図２：コミットメントを用いた方式

［入札フェーズ］

Step1）入札者 i は，$c_i=H(v_i \| r_i)$ を，主催者に送る。

［開札フェーズ］

Step2）主催者は，入札者から (v_i, r_i) を受け取り，
$H(v_i \| r_i) \stackrel{?}{=} c_i$ をチェックする。

Step3）主催者は，落札者と落札値を決定する。

Step4）主催者は落札者と落札値を公開する。

本方式の要求条件に対する充足度は以下のとおり。

- 主催者以外に対する入札値の秘匿性はみたされる。
- ハッシュ関数の一方向性により，入札フェーズにおいて主催者に対する入札値の秘匿性はみたされる。
- 開札フェーズにおいて，主催者に対する入札値の秘匿性がみたされない。
- コミットメントの性質により，入札フェーズでの v_i と開札フェーズでの v_i が同一であることをチェックできる（Step2）ので，頑強性はみたされる。
- ハッシュ関数を1回実行して，c_i のみ送信するので，入札の効率はよい。
- 開札時の計算は，ハッシュ関数を1回実行して，あとは入札値同士を比較するだけである。
- 公開検証可能性はみたされない。Step4 を下の Step4' に置き換えるとみたされるようになるが，主催者以外に対する入札値の秘匿性がみたされなくなる。

  Step4'）主催者は全ての入札者の入札値を公開する。
- 入札者の Walk Through 性はみたされない。（開札フェーズで v_i, r_i を主催者に送らなければならない）

まとめ：効率に優れ，頑強性をみたすが，開札フェーズで入札値の秘匿性がない。公開検証可能性と入札フェーズでの入札値の秘匿性が両立しない。入札者の Walk Through 性はみたされない。

4.2　公開鍵暗号を用いた方式[3]

次に，入札値の秘匿性を保証できる方式を紹介する。

TTP が，各価格ごとの公開鍵 $\{pk_p\}$ と秘密鍵 $\{sk_p\}$ を作り，$\{pk_p\}$ を公開する。入札者は全ての価格 p について pk_p で入札情報（その価格が入札値か否か）を暗号化し，主催者に送る。TTP が価格の高いほうから順に秘密鍵を主催者に開示し，落札者と落札値を決定する。落札した時点で，秘密鍵の開示を中止する。これによって，開札フェーズでの入札値の秘匿性を保証する。

価格	公開鍵	入札者 1	入札者 2	入札者 3	秘密鍵
4	pk_4	$E_{pk_4}(\times \| r_{1,4})$	$E_{pk_4}(\times \| r_{2,4})$	$E_{pk_4}(\times \| r_{3,4})$	sk_4
3	pk_3	$E_{pk_3}(\times \| r_{1,3})$	$E_{pk_3}(\circ \| r_{2,3})$	$E_{pk_3}(\times \| r_{3,3})$	sk_3
2	pk_2	$E_{pk_2}(\circ \| r_{1,2})$	$E_{pk_2}(\times \| r_{2,2})$	$E_{pk_2}(\times \| r_{3,2})$	sk_2
1	pk_1	$E_{pk_1}(\times \| r_{1,1})$	$E_{pk_1}(\times \| r_{2,1})$	$E_{pk_1}(\circ \| r_{3,1})$	sk_1

［準備フェーズ］

Step0）TTP は全ての価格 p について $\{pk_p\}$，$\{sk_p\}$ を作り，$\{pk_p\}$ を公開する。

［入札フェーズ］

Step1）入札者 i は，$\{E_{pk_p}(\circ$ または $\times \| r_i, p)\}$ を主催者に送る。

［開札フェーズ］

Step2）$p \leftarrow p_{max}$ とし，TTP は主催者に最も高い価格に対応する秘密鍵 sk_p を渡す。

Step3.1）主催者は，sk_p を用いて価格 p に関する暗号文を復号し，その値段に○をつけている入札者がいた場合はこれを落札者とし，p を落札値とする。

Step3.2）Step3.1 で落札者と落札値が決まらない場合は，$p \leftarrow p-1$ とし，主催者は TTP から sk_p を受け取り，Step3.1 以下を繰り返す。決まった場合は，Step4 へ。

Step4）落札者と落札値が決定したら，主催者は落札値以上の sk_p を全て公開する。

本方式の要求条件に対する充足度は以下のとおり。

- 主催者と TTP が結託しなければ，入札値の秘匿性はみたされる。
- 入札者が2つ以上の価格に○をつけたとしても，○がついている最も高い価格が入札値とみなすことで問題にならない。頑強性はみたされる。
- Step4 で公開された落札値以上の sk_p より，誰でも落札値と落札者を検証できるので，公開検証可能性がみたされる。
- 入札フェーズにおいて，入札者は k 回暗号化を行わなければならないので，入札の効率は良くない。
- 開札フェーズにおいて，主催者は最悪の場合 nk 回の復号を行わなければならないので，開札の効率は良くない。
- 入札者の Walk Through 性をみたす。

まとめ：入札値の秘匿性，頑強性，公開検証可能性はみたされるものの，入札の効率が悪い。TTP に安全性が依存していることも問題である。

4.3　ハッシュ連鎖を用いた方式[7]

入札者iは，あらかじめ定められた回数だけハッシュ関数を施したコミットメント$H^{p_{max}+1}(IV^i)$を公開する（p_{max}は最高価格を表す）。入札値v_iに対応する$H^{v_i}(IV^i)$を別のハッシュ関数Gを用いてコミットメントする（$G(H^{v_i}(IV^i))$を公開）[3]。主催者は，すべての入札者にp_{max}から順に$H^p(IV^i)_{(1\le i\le n)}$を公開させ，$H^p(IV^i)_{(1\le i\le n)}$が$H^{p_{max}+1}(IV^i)_{(1\le i\le n)}$と関連づくことを検証する。もし，$H^p(IV^i)=G(H^{v_i}(IV^i))$なる$i$が存在すれば，入札者$i$が落札者，そのときの$p$が落札値となる。

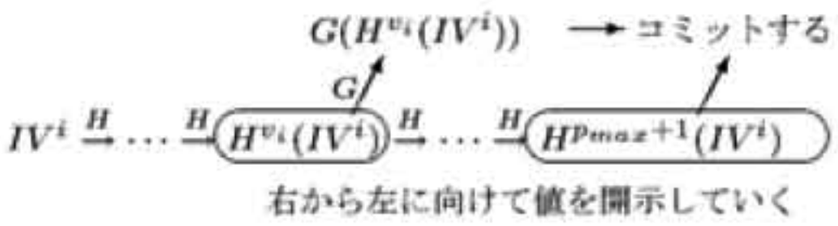

図３：ハッシュ連鎖を用いた方式

［入札フェーズ］

Step1）入札者iは，$H^{p_{max}+1}(IV^i)$および$G(H^{v_i}(IV^i))$を主催者に送る。

［開札フェーズ］

Step2）$p \leftarrow p_{max}$;

Step3）入札者iは$H^p(IV^i)$を公開する。

誰でも，$H^{p_{max}-p+1}(H^p(IV^i)) = H^{p_{max}+1}(IV^i)$かつ$G(H^p(IV^i)) = G(H^{v_i}(IV^i))$なる$i$が存在するかを調べることができる。

存在すれば$p_{win} \leftarrow p$として終了。

存在しなければ，$p \leftarrow p-1$としてStep3を繰り返す。

本方式の要求条件に対する充足度は以下のとおり。

- 最高価格から順に，その価格での入札者が存在するか否かを判定するので，入札値の秘匿性をみたす。
- ハッシュの一方向性および耐衝突性により，不正な入札がプロトコルの実行に影響をあたえることは難しく，頑強性をみたす。
- Step3で入札者が公開する情報により，誰でも落札者と落札値を決める作業を実行できるので，公開検証可能性をみたす。
- 入札者は，入札フェーズではたかだかk回程度のハッシュ計算を行えばよいので，入札の効率はよい。
- 主催者は，開札フェーズにおいて入札者から公開された情報$H^p(IV^i)$に対して多くともk回のハッシュ関数を実行し，入札フェーズで入札者から受け取った情報との比較を行えばよいので，開札の効率はよい。（ハッシュ関数の計算は高速[4]）

まとめ：入札値の秘匿性，頑強性，公開検証可能性をみたし，効率もよく優れた方式であるが，入札者のWalk Through性をみたさない。

4.4　乱数対を用いた方式[4][5]

この方式は主催者を２人仮定する。入札者iは，入札値v_iより大きい価格pについては２つの同じ値を，v_i以下のpについては２つの異なる乱数を選んで，２つの値$\{R_{i,1}(p)\}$，$\{R_{i,2}(p)\}$を別々に２人の主催者に送る。２人の主催者は協力して，最も大きいp（$=p_{max}$）から順にある入札者について$R_{i,1}(p) \neq R_{i,2}(p)$が成り立つような最大の$p$を求める。全ての入札者について$R_{i,1}(p)=R_{i,2}(p)$が成り立つときのみ$f_1=f_2$が成り立つことに注意。

$$\begin{cases} f_1 = H(R_{1,1}(p) \| R_{2,1}(p) \| \cdots \| R_{n,1}(p)) \\ f_2 = H(R_{1,2}(p) \| R_{2,2}(p) \| \cdots \| R_{n,2}(p)) \end{cases}$$

［入札フェーズ］

Step1）入札者iは，主催者１，主催者２にそれぞれ$\{R_{i,1}(p)\}$，$\{R_{i,2}(p)\}$を送る。

［開札フェーズ］

Step2）$p \leftarrow p_{max}$

Step3）

$f_1 \neq f_2$：落札値$p_{win} \leftarrow p$。

$f_1 = f_2$：$p \leftarrow p-1$；Step3を繰り返す。

Step4）２人の主催者は，p_{win}及び，$p \ge p_{win}$について$\{R_{i,1}(p)\}$，$\{R_{i,2}(p)\}$を公開する。

本方式の要求条件に対する充足度は以下のとおり。

- ２人の主催者が結託しなければ，入札値の秘匿性はみたされる。

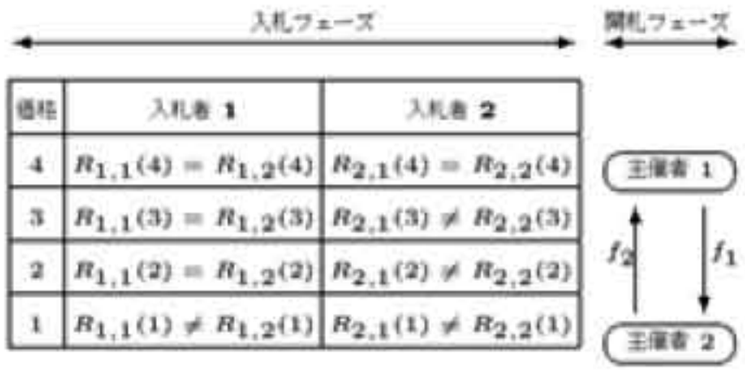

図４：乱数対を用いた方式

3　GとHのコミットを別々にせず，一つのハッシュ値の中に２つの要素を織り込む手法も文献[7]中で提案されているが，ここでは割愛する。

4　公開鍵暗号の計算と比較すると，100万倍程度高速である。

5　文献[4]中では，最初から効率の良い落札値決定法を提案しているが，本稿では基本的なアイディアを紹介した後に，その拡張という形で紹介する。

・入札者が，同じ値を２つ以上の価格について主催者に送った場合，小さい価格のほうを入札値とみなせばプロトコルは動作する。よって，頑強性はみたされる。
・Step4 で公開された情報により，公開検証可能性がみたされる。
・入札フェーズにおいて，入札者は同じ数の対または異なる数の対を価格の総数（k）分用意して主催者に送ればよい。よって，入札の効率は良い。
・開札フェーズにおいて，主催者は p ごとに，１回ずつハッシュ関数を計算しそのハッシュ値を別の主催者に送る作業を，最大 k 回行えばよい。よって，入札の効率は良い。

まとめ：入札値の秘匿性，頑強性，公開検証可能性をみたし，効率がよい。

文献[4]で提案されている落札値決定手順を以下に示す。

Step2′）$v_{max} \leftarrow p_{max}$; $v_{min} \leftarrow p_{min}$; $p \leftarrow \lceil (v_{max}+v_{min})/2 \rceil$;
Step3′）以下の処理を繰り返し，$v_{max}=v_{min}$のとき，落札値 $p_{win} \leftarrow p$ としてStep4 へ。
$f_1=f_2$
$v_{max} \leftarrow p-1$;
$p \leftarrow \lceil (v_{max}+v_{min})/2 \rceil$;
$f_1 \neq f_2$:
$v_{min} \leftarrow p$;
$p \leftarrow \lceil (v_{max}+v_{min})/2 \rceil$;
（f_1とf_2の定義はStep3 と同じ）

Step2, Step3 をStep2′, Step3′に置き換えることにより，ハッシュ値を計算して別の主催者に送る作業が$\log_2(k)$ 回程度になる。このとき，入札者が同じ値を２つ以上の価格について主催者に送った場合に問題が生じるようになり，頑強性がみたされなくなるが，その解決策も検討されている[8]。

5　まとめ

表１に，各方式の比較結果を示した。

以上，第一価格秘密入札プロトコルの技術を概観した。

オークション主催者を信用できる場合には，コミットメント方式で実用上十分であろう。入札値を秘密にするニーズが無く，複数の主催者が結託しないと仮定できるなら，入札値の秘匿性，頑強性，公開検証可能性，入札者の Walk Through 性をみたし，かつ効率のよいプロトコルが，コミットメント方式で実現できる。

しかし，不特定多数の個人がオークションに参加し，その結果を誰もが容易に閲覧できる環境が提供される場合には，必要最小限の情報の公開にとどめて，落札者と落札値のみが開示対象となる方式のほうが安心できる。

今後は，入札者のプライバシ保護の観点から，本稿で紹介したような，落札値以外の入札値を秘匿可能なプライバシ重視型のオークションも必要になろう。

今後の研究テーマとして，

(1) 複数の信頼できる主催者を仮定せずに，効率よく入札値の秘匿性と公開検証可能性を両立する第一価格秘密入札プロトコルの研究，
(2) 経済学的に最適な方式であることが証明されている第二価格秘密入札を電子的に実現するプロトコルの研究

などが興味深い。

6　謝辞

公共事業の入札の現行方式について，ていねいに解説し，入札者の立場から種々の意見を聞かせてくれた，宮下勝久氏に感謝します。

表１：方式の比較

	コミットメント方式		公開鍵暗号を用いる方式	ハッシュ連鎖を用いる方式	乱数対による方式
	Step 4	Step 4′			
入札値の秘匿性	△	×	○	○	○
頑強性	○		○	○	○
公開検証可能性	×	○	○	○	○
入札の効率	○		×	○	○
開札の効率	○		×	○	○
Walk Through 性	×		○	×	○
主催者の数	1		1	1	2
TTP の必要性	なし		必要	なし	なし

参考文献

[1] 横尾真．インターネットオークションの理論と応用．人工知能学会誌，Vol. 15, No. 3, pp. 404-411, 2000.

[2] H.Kikuchi, M.Hakavy, and D.Tyger. Multi-Roun d Anonymous Auction Protocols. *IEICE Trans. on Information and Systems,* Vol. E82-D, No. 4, pp. 769-777, 1999.

[3] K.Sako. An Auction Protocol Which Hides Bids of Losers. *In Proc. of 3rd International Workshop on Practice and Theory in Public Key Cryptosystems, PKC 2000,* Vol. 1751 of Lecture Notes in Computer Science, pp. 422-432. Springer-Verlag, 2000.

[4] 千田浩司，小林邦生，森田光．対称サーバーをもちいたログオーダー比較の電子入札方式．2001 年暗号と情報セキュリティシンポジウム，SCIS2001, pp. 569-573, 2001.

[5] Alfred J. Menezes, Paul C. van Oorschot, andScott A. Vanstone. *Handbook of Applied cryptography*. CRC Press LLC, 1996.

[6] http://www.ntt.co.jp/news/news01/0104/010425.html.

[7] K.Suzuki, K.Kobayashi, and H.Morita. Efficient Sealed-bid Auctions using Hash Chain. Vol. 2015 *of Lecture Notes in Computer Science*, pp. 183-191. Springer-Verlag, 2001.

[8] 森田光，千田浩司，太田和夫，今井識．乱数連鎖を用いた入札方式．2003 年暗号と情報セキュリティシンポジウム，SCIS2003, 2A-4, 2003.