無証拠性を持つ秘密入札プロトコルの安全性

許, 容碩
九州大学大学院システム情報科学府

櫻井, 幸一
九州大学大学院システム情報科学研究院

出版情報：2004年 暗号と情報セキュリティシンポジウム. 2, pp.827-832, 2004-01
バージョン：
権利関係：

無証拠性を持つ秘密入札プロトコルの安全性
On the Security of Sealed-bid Auction with Receipt-freeness

許容碩 * 櫻井幸一†
Yong-Sork HER Kouichi SAKURAI

あらまし 暗号技術を利用したさまざまな秘密電子競売のプロトコルが提案されている．安全な秘密電子競売システムのためにさまざまな条件を満たさわなければならない．最近，要求条件の中で入札談合防止のための無証拠性の技法が重要に認識されている．Abe-Suzuki と Chen-Lee-Kim は秘密入札方式のための無証拠性技法を提案した．本論文では，提案された秘密入札競売のプロトコルのための無証拠性技法を分析して，安全性に対する問題点を提示する．

キーワード 電子競売プロトコル， 無証拠性， 安全性， 入札談合防止

1 はじめに

1.1 動機

入札は価格が固定されない特別な商品を取り引きするための商取引である．実際オフラインでは，価格決定のためにさまざまな入札方式を利用しているし，最近ではオンラインの入札のために暗号技術とネットワークを利用した電子競売方式が提案されている．電子競売方式は大きく四種類に分類される．すなわち，English 入札方式，第 1 価格秘密入札方式，第 2 価格秘密入札方式，M+1 番目秘密入札方式である．English 入札方式は，入札者が入札時間の間に，他の入札者の入札価格を見ながら繰り返し入札をする．入札時間が終わった後，一番高い価格を入札した入札者が落札者になる．English 入札方式の特徴は入札価格をすべての入札者が見ることができし，繰り返し入札が可能であるということである．第 1 価格秘密入札方式は入札者がただ一度入札でき，他の入札者の価格を見ることができてはいけない．落札者は最高入札価格の入札者である．第 2 価格秘密入札方式は第 1 価格入札方式のようだが，落札者は自分の入札価格ではない 2 番目に高い入札価格を支払う．M+1 番目秘密入札方式は同じ品物が M 個ある時，入札する方式である．安全な秘密入札方式のためにさまざまな条件が必要である. 最近には，さまざまな条件の中で入札談合防止のための無証拠性の技法が重要に認識されている．特に，電子入札の場合には秘密入札方式の成功可否を決めることができる重要な条件である．完全な無証拠性の技法になるためには，入札者の価格談合と第三者による強制入札，そして，競売人による入札不正を考慮しなければならない．本論文では，このような条件を土台にして，既存の提案された電子競売での無証拠性技法を分析して，安全性に対する問題点を提示する．

1.2 関連研究

電子競売のために提案されたさまざまな秘密入札プロトコルがある．Kikuchi-Harkavy-Tygar は秘密入札プロトコルで tie-breaking を扱う方法を提案した [4]．Omote-Miyazi は効率性と興味を強調した 2 進木方式の秘密入札プロトコルを提案した [6，9]. Naor-Pinkas-Sumner は安全なプライバシーと正確性のために二つのサーバーを利用した秘密入札プロトコルを提案した [5]．Juels-Szydlo は [5] の方式を通信量と計算量を拡張したプロトコルを提案した．Baudron-Stern は準同型暗号を利用して circuit evaluation を基盤とした秘密入札方式を提案した [10]. Abe-Suzuki は準同型暗号を利用した M+1 番目の秘密入札方式を提案した [11]．Lee-Kim-Ma は 1 回の登録と公開検証を持った公開競売を提案した [8]．最近，電子投票と電子競売のための無証拠性技法が紹介されている．電子投票の場合にはいくつかの技法が提案された [1，2，3，7]．Benaloh-Tuinstra[1] は電子投票のための無証拠性技法を初めて提案したし， Abe-Suzuki[12] は電子競売のための最初の無証拠性技法を提案した．Benaloh-Tuinstra と Abe-Suzuki は投票ブースと競売ブースという物理的仮定をした．実際，オンラインでこのような仮定

* 九州大学大学院システム情報科学府, 〒 812-8581 福岡市東区箱崎 6-10-1, Graduate School of Information Science and Electrical Engineering, Kyushu University, 6-10-1 Hakozaki, Higashi-ku, Fukuoka, 812-8581 ysher@itslab.csce.kyushu-u.ac.jp
† 九州大学大学院システム情報科学研究院, 〒 812-8581 福岡市東区箱崎 6-10-1, Faculty of Information Science and Electrical Engineering, Kyushu University, 6-10-1 Hakozaki, Higashi-ku, Fukuoka, 812-8581 sakurai@csce.kyushu-u.ac.jp

を満たすことは難しいと知られていて，現実的ではないという評価を受けている．Sako-Kilian[2] は untappable channel を基盤にする無証拠性技法を提案した．彼らの技法の短所は mix-net を利用するから集計段階で多くの負荷量が発生するである．[3] で，Okamoto は物理的条件のような untappable channel を利用して trapdoor bit-commitment を基盤にする無証拠性技法を提案した．この技法は各投票者と各確認者の間に一方向安全なチャンネルを構成しにくいということが短所に指摘されている [7]．電子競売の場合には，Abe-Suzuki によって一番目無証拠性技法が提案された以後 Chen-Lee-Kim [16] が準同型暗号技術を利用した無証拠性技法を提案した．

1.3 論文の構成

第 2 章で，我々は秘密入札プロトコルのための無証拠性の技法を再確立する．再確立する無証拠性技法は入札に係わるすべての参加者に対する談合防止のための技法である．第 3 章では Abe-Suzuki と Chen-Lee-Kim の技法を紹介する．そして，第 4 章で，再確立した無証拠性技法を基盤にして Abe-Suzuki と Chen-Lee-Kim の技法の問題点を提示する．第 5 章で本論文の結論を説明する．

2 再確立された秘密入札方式のための無証拠性の技法

2.1 必要条件

秘密入札のための基本条件を説明する．

- **入札の無記名性**:落札者と落札価格以外にはいかなる情報も公開されてはいけない．
- **落札者の証明**:落札者と落札価格はすべての人が正確に理解するべきである．
- **否認防止**:落札者は自身の入札価格を否認できてはいけない．
- **入札価格の安全性**:誰も入札価格を修正したり取り消しすることができない．
- **入札者の公平性**:誰も外部の圧力を受けないで，平等に入札ができなければならない．
- **匿名性** :入札が進行される間に入札者と入札価格の関係は匿名性を保障しなければならない． 電子競売の結果は入札者と入札価格が共に発表される．

2.2 再確立された秘密入札方式のための無証拠性

この章で，我々は秘密入札競売のために無証拠性を再確立する．無証拠性の目的は全ての参加者に提供することになっている．全ての参加者は入札価格の情報を公開できる．我々は下記のように無証拠性を再確立する．

- **競売人の無証拠性 (RFA: Receipt-Free for Auctioneer)**：競売人は入札者の入札価格の情報に対して偽りを出来なくなければならない．また，競売人と第三者との通信を防がなければならない．

- **入札者の無証拠性（RFB: Receipt-Free for Bidder）**：入札者は自身の入札価格に対する情報だけでなく入札価格に対する情報を偽ることかできない．また，入札価格に対する情報のコピーを防がなければならない．

- **強制者 (第三者) の無証拠性（RFC：Receipt-Free for Coercer)**：第三者は入札者を雇用して，入札価格を調整して，理由ない低い価格で落札ができる．そして，第三者は自身の命令によって入札した入札者に補償をする．

3 Abe-Suzuki と Chen-Lee-Kim の無証拠性の技法

3.1 Abe-Suzuki の無証拠性の技法

前章で言及をしたが，電子競売の無証拠性のために，Abe-Suzuki は chameleon bit-commitment と一方向 untappable チャンネルと入札ブースを利用した．

■ 準備

$\{A_i \mid i = 0, 1, ..., a\}$ は競売人で，$\{B_j \mid j = 0, ..., b\}$ は入札者である．競売人は競売の価格リスト $P = \{l \| l = 0, ..., m\}$ を発表する．p と q は大きい素数で，$Z^*{}_q$ の位数 q の原始元素は g である．メッセージ M_0，M_1 は各々，入札しなかったことと入札したことを意味する．

■ 入札

入札で，各入札者は入札ブースで下記のように入札をする．各入札者は秘密鍵 $x_j \in Z_q$ を選択して，自身の署名と共に彼の公開鍵 $h_j = g^{x_j}$ を発表する．入札者 B_j は自身の入札価格 $p_j \in P$ を決定する．彼は彼の秘密 Seeds $r_{l,\,j} \in Z_q (l = 1, 2, ..., m)$ をランダムに選択して，chameleon bit-commitments の順序を計算する．

$$C_{l,\,j} = \begin{cases} g^{M_1} h^{r_{l,\,j}} & (l = p_j) \\ g^{M_0} h^{r_{l,\,j}} & (l \neq p_j) \end{cases}$$

入札者は彼の署名と commitments$(l_{1,\,j}, l_{2,\,j}, ..., l_{m,\,j})$ の順序を発表する．入札者は各競売人 A_i に chameleon bit-commit の秘密鍵 $log_g h_j = x_j$ と $log_g C_{i,\,j}$ を内部ゼロ知識証明により証明する．最後に，入札者は秘密 seeds $r_{i,\,j}$ のためで t-out-of-a を作る．彼は秘密シード $r^i{}_{i,\,j}$ の中で i 番目シード $r^i{}_{i,\,j}$ $(i = 1, 2, ..., m)$ を自身の署名と共に i 番目競売人に一方向 Untappable チャンネルを通し送ります．

■ オープニング

オープニングで，各競売人はすべての入札者の l 番目秘

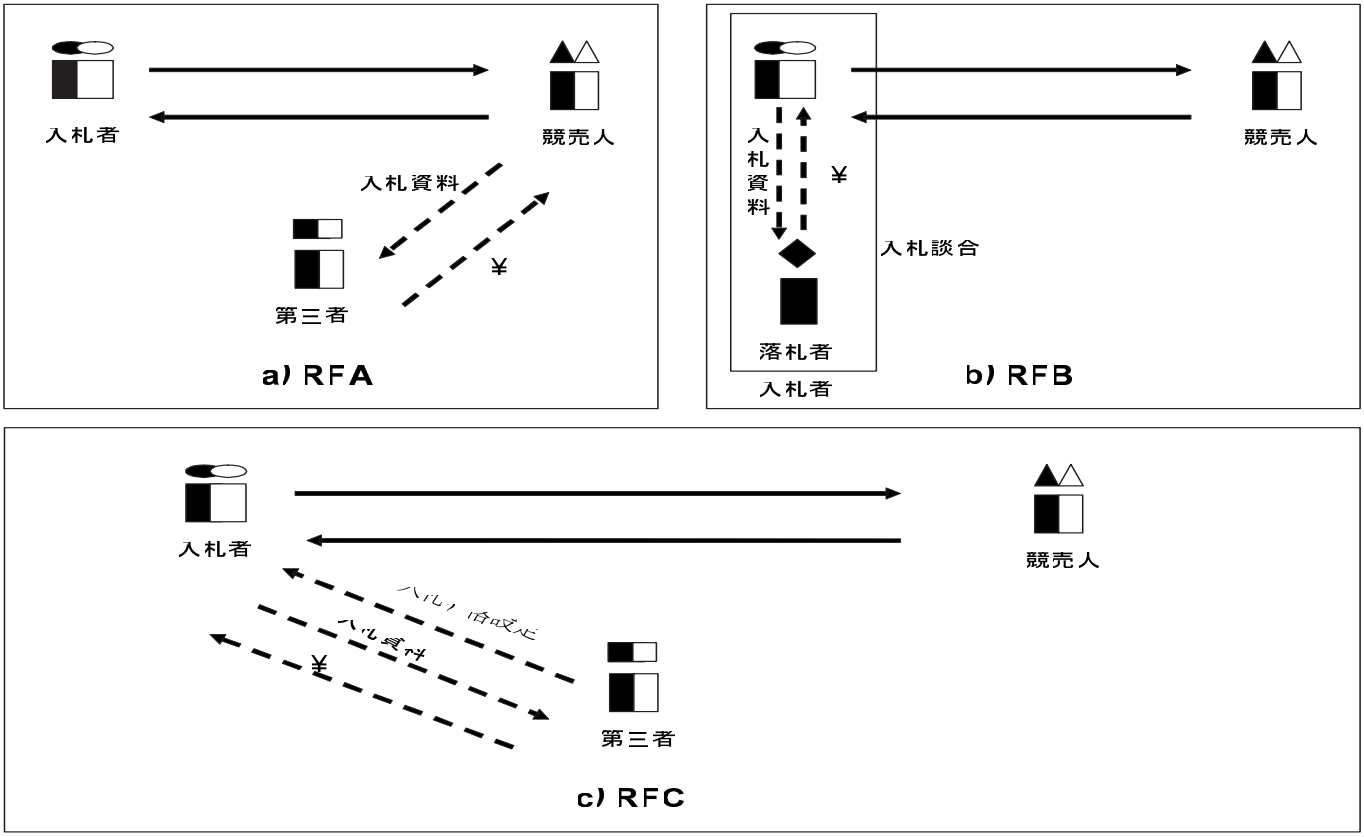

図 1: 再確立された無証拠性

密シード $r_{l,\,j}$ の $r^{i}_{l,\,j}$ $(j = 1, 2,..., b)$ を共有する．各競売人は下記のように秘密シード $r_{l,\,j}$ を復号する．

$$C_{l,\,j} = g^{M_1} h^{r_{l,\,j}}, \quad (j = 1, 2,..., b)$$

もし, j が存在すれば, 競売人は落札者と落札価格 $p_{win} = l$ を発表する．

3.2 Chen-Lee-Kim の無証拠性の技法

Chen-Lee-Kim は準同型暗号を利用した無証拠性を持つ電子競売を提案した．彼らは秘密入札方式と M+1 番目入札方式に適用可能な二つの無証拠性技法を提案した．本論文では秘密入札方式の無証拠性の技法に注目する．彼らの技法は競売のために，競売人，競売発行人，販売者，入札者で構成される．彼らは競売のために信頼機関に依存しなくて，競売発行人は 競売人と絶対交流をしないことを仮定する．

■ 入札

各入札者 B_i は販売者の助けで無証拠性の入札ベクトル $C^{*}_{i,\,j}$ を生成する．また，各入札者は入札ベクトルの合法性の証明をする．j は 1, 2,..., n である．各入札者は販売者に $C_{i,\,j} = (x_{i,\,j}, y_{i,\,j})$ を送る．販売者 S は β_j を 選択して， $u_j = g^{\beta_j}$ と $v_j = (h_1 h_2)^{\beta_j}$ を計算する．無証拠性の入札ベクトルは $C^{*}_{i,\,j} = (x_{i,\,j}, y_{i,\,j})$ である．販売者は γ_j,ς_j,$\delta_j \in_R Z_q$ 選択して，下記のように計算する．

$$(a_j, b_j) = (g^{\gamma_j}, (h_1 h_2)^{\gamma_j}), D_j = g^{\varsigma_j} h^{\delta_j}_{B_i}$$

販売者は $H_j = H(a_j, b_j, Dj, x^{*}_{i,\,j}, y^{*}_{i,\,j})$, $U_j = \gamma_j - \beta_j(H_j + \varsigma_j)$ を計算する．販売者は $(H_j, \varsigma_j, \delta_j, U_j)$ と $C^{*}_{i,\,j}$ を入札者 B_i に送る．販売者は下記のように計算する．

$H_j = H(g^{U_j}(x^{*}_{i,\,j}/x_{i,\,j})^{H_j+\varsigma_j},$
$(h_1 h_2)^{U_j}(y^{*}_{i,\,j}/y_{i,\,j})^{H_j+\varsigma_j},$
$g^{\varsigma_j} h^{\delta_j B_i}, x^{*}_{i,\,j}, y^{*}_{i,\,j}$

また，入札者は

$a_{1,\,j} = g^{r_j} x^{d_j}_{i,\,j}, b_{1,\,j} = (h_1 h_2)^{r_j}(y_{i,\,j}/G_2)^{d_j},$
$a_{2,\,j} = g^{w_j} g^{r_j} x^{d_j}_{i,\,j}, b_{2,\,j}(h_1 h_2)^{w_j};$

を計算する．入札者は販売者に $(a_{1,\,j}, b_{1,\,j})$ を送って，S は $r_{1,\,j}, r_{2,\,j}, d_{1,\,j} \in Z_q$ 選択する．

また，販売者 S は

$a'_{1,\,j} = a_{1,\,j} g^{r_{1,\,j}} x^{d_{1,\,j}}_{i,\,j},$
$b'_{1,\,j} = b_{1,\,j}(h_1 h_2)^{r_{1,\,j}}(y_{i,\,j}/G_1)^{d}_{1,\,j}$
$a'_{2,\,j} = a_{2,\,j} g^{r_{2,\,j}} x^{-d_{1,\,j}}_{i,\,j},$
$b'_{2,\,j} = b_{2,\,j}(h_1 h_2)^{r_{2,\,j}}(y_{i,\,j}/G_2)^{-d_j}$ 計算する．

販売者 S は $P_1 = (a'_{1,\,j}, b'_{1,\,j}, a'_{2,\,j}, b'_{2,\,j})$ を入札者に送る．入札者 B_i は $c_j = H(a'_{1,\,j}, b'_{1,\,j}, a'_{2,\,j}, b'_{2,\,j}), e_j = c_j - d_j$, $f_j = w_j - a_{ij} e_j$ を計算する．

$X = e_{p_i}, e_{p_i} = d_{p_i}, d_{p_i} = X; Y = f_{p_i}, f_{p_i} = r_{p_i}, r_{p_i} = Y$ をいう．入札者 B_i は (d_j, r_j), (e_j, f_j) を販売者 S 送る．販売者 S は $d'_{1,\,j} = d_j + d_{1,\,j}$, $d'_{2,\,j} = e_j - d_{1,\,j}$, $r'_{1,\,j} = r_j + r_{1,\,j} - d'_{1,\,j}\beta_j$, $r'_{2,\,j} = f_j + r_{2,\,j} - d'_{2,\,j}\beta_j$

を計算して，$P_2 = (d'_{1,j}, d'_{2,j}, r'_{1,j}, r'_{2,j})$ を入札者 B_i に送る．入札者 B_i は $c_j = d'_{1,j} + d'_{2,j}$ 計算して，
$c_j = H(gr'_{1,j}(x'_{i,j})^{d'_{2,j}}, (h_1h_2)^{r'_{1,j}}(y^*_{i,j}/G_1)^{d'_{1,j}},$
$gr'_{2,j}(x^*_{i,j})^{d'_{2,j}}, (h_1h_2)^{r'_{2,j}}(y^*_{i,j}/G_2)^{d'_{2,j}})$
を確認する．入札者 B_i は公開掲示板に $x^*_{i,j}$, P_1 と P_2 送る．

■ オープニング

競売発行人と競売人は競売結果を計算する．$j = n$ の時，競売発行人と競売人が独立的に最終価格ベクトルを下記のように計算する．

$$(X_j, Y_j) = (\sum_{i=1}^{m} x^*_{i,j}, \sum_{i=1}^{m} y^*_{i,j})$$

彼らは独立的に $X^{x1}{}_j$, $X^{x2}{}_j$ を発表して，彼らの公開鍵 h_1, h_2 を非内部ゼロ知識証明で提供する．R_j は次のように定義する．

$$R_j = Y_i/X^{x1+x2}{}_j = G_1^{l_j}G_2^{m-l_j}, (0 \le l_j \le \mathrm{m})$$

競売発行人 AI と競売人 A は $l_j \neq 0$ を満足な最初 j を決定して，落札価格は j である．競売発行人と競売人は落札価格を P_w を発表する．

4 Abe-Suzuki と Chen-Lee-Kim の技法に対する安全性の分析

4.1 Abe-Suzuki と Chen-Lee-Kim の技法に対する安全性の概要

秘密入札で，すべての入札者の入札価格を発表する必要はない．但し，落札者と落札値格だけ発表する．Abe-Suzuki は無証拠性を持つ電子競売のために chameleon bit-commitment と一方向 untappable チャンネルを利用した．すなわち，chameleon bit-commitment の秘密シードが領収書の役割をする．そして，この chameleon bit-commitment の秘密シードは入札者が生成する．また，入札価格は入札者の公開鍵により暗号化される．したがって，入札者は入札価格，秘密鍵などの全部の情報を知っている．入札価格の流出を防ぐために，彼らは入札者と競売人の間に一方向 untappable チャンネルを利用した．しかし, 競売時間が完了した後，入札者は入札価格の情報が流出されることができる．例えば，第三者 (強制者) は入札者に入札価格を命令する．第三者の命令に従った入札者は第三者から補償を受けるために，自身が第三者の命令によって入札したことを自身の秘密鍵と秘密シードを利用して証明できる．

Chen-Lee-Kim の技法の場合に，一方向 untappable チャンネルを競売発行人と販売者，競売人と販売者，各入札者と販売者の間に仮定する．各入札者と販売者の間の一方向 untappable チャンネルの使用は入札者が一般的場所でない，特定場所 (untappable チャンネルが可能な場所) でだけ入札が可能なために非現実的である．

4.2 競売人のため無証拠性:RFA

競売人は秘密入札で，落札者を決定する役割をする．彼は入札者の入札価格の情報が分かる．安全な秘密入札のために競売人により入札者の入札価格が漏れるのを防がなければならない．

■ Abe-Suzuki 技法での RFA

この技法で，あらゆる競売人は落札者と落札価格を決定するために共に復号化する．これは，競売人により落札者の秘密 シードが漏れる．それで， この技法は落札出来ない入札者には無証拠性を守ることができる．しがし, 落札者の無証拠性は守ることができない [16]．第三者は各入札者と競売人の一部に入札価格と入札資料を要求して, 自身の命令に服従した入札者と競売人には補償を約束する．自身の命令を確認するために第三者は理由ない低い価格で入札して，秘密シードを要求する．

準備

$\{A_i \mid i = 0, 1, ..., a\}$ は競売人で，$\{B_j \mid j = 0, ..., b\}$ は入札者という．残り部分は Abe-Suzuki の技法と同じである．

入札

入札で，各入札者は入札ブースで第三者の命令通りに入札をする．

オープニング

あらゆる競売人は落札者と落札価格を決定するために，秘密シード $r_{i,j}$ と下記のように計算する．

$$C_{l,j} = g^{M_1}h^{r_{l,j}}, \quad (j = 1, 2, ..., b)$$

各競売人は競売終了の後に, 落札者に対する秘密 シード $r_{i,j}$ を流出できる．

4.3 入札人のため無証拠性:RFB

秘密入札で，入札者間の入札談合防止は秘密入札の勝敗を左右する重要な要素である．この RFB はオフラインの入札でも重要な問である．

■ Abe-Suzuki 技法での RFB

入札者間の価格談合の問題は電子競売だけでなく，オフラインでももっとも大きい問題になっている．彼らはあらかじめ落札者を決定できて，入札者は落札者を見て，彼らの事前約束の履行可否を知ることができる．Abe-Suzuki の技法の場合，RFB の観点で下記のように弱点を持つ．

準備

我々は入札者を $\{B_j \| j = 0, ..., 10\}$ の 11 人で仮定する．そして， 下記のように価格を事前に決定する．

$B_0 = 1$, $B_1 = 1$, $B_2 = 1$, $B_3 = 1$, $B_4 = 1$, $B_5 = 2$, $B_6 = 1$, $B_7 = 2$, $B_8 = 1$, $B_9 = 1$, $B_{10} = 3$
他の部分は既存の Abe-Suzuki の技法と同じである．

入札
入札で，各入札者は入札ブースで事前に約束された入札価格通りに入札をする．

オープニング
オープニングで，各競売人は落札者と落札価格を決定する．落札者と落札価格を見て，談合した入札者らは自分らの約束の履行可否を判断できる．この約束が履行されたとすれば，落札者は B_{10} になって，落札価格は 3 である．

■ Chen-Lee-Kim 技法での RFB
この技法で，入札価格は入札者により暗号化される．それで，入札者は入札価格を事前に 談合できる．下記のように価格談合が可能である．

入札
我々は入札者を $\{B_j \| j = 0,..., 10\}$11 人で仮定する．競売人の秘密鍵は x_1 で，公開鍵は $h_2 = g^{x_2}$ である．販売者は価格リスト $P = \{l \| l = 0,..., m\}$ を発表する．各入札者 B_j は自身の秘密鍵を x_{B_i} 選択して，彼の公開鍵 $h_{B_i} = g^{xB_i}$ を発表する．彼は事前に談合された入札価格 $p_i \in P$ で入札をして，入札ベクトルを計算する．

$$C_{i,\,j} = (x_{i,\,j}, y_{i,\,j}) = (g^{a_{i,\,j}}, (h_1 h_2)^{a_{i,\,j}} G_1), \quad \text{if } j = p_i$$

$(a_{i,\,j} \in_R Z_q, \quad j = 1, 2,..., n)$
例えば，b_0 から b_9 までの入札者は入札価格 1 で入札をして，入札者 b_{10} は入札価格 2 で入札する．すなわち， 入札者 b_{10} の暗号された入札ベクトルは以下のようである．

$$C_{i,\,2} = (x_{i,\,2}, y_{i,\,2}) = (g^{a_{i,\,2}}, (h_1 h_2)^{a_{i,\,2}} G_1), \quad \text{if } j = p_i$$

b_0 から b_9 までの入札者の暗号された入札ベクトルは以下のようである．

$$C_{i,\,1} = (x_{i,\,1}, y_{i,\,1}) = (g^{a_{i,\,1}}, (h_1 h_2)^{a_{i,\,1}} G_1), \quad \text{if } j = p_i$$

オープニング
オープニングで，落札者は b_{10} となる．もし落札者が b_{10} でなければ，他の入札者は競売人により発表される落札者を見て，落札者が約束を履行しなかったことを知ることができる．提案した技法では入札者が自身の入札価格に対する暗号鍵を知っているということが問題になることができる．

4.4 第三者のため無証拠性:RFC

この章で，我々は第三者の観点で無証拠性，RFC に対して説明する．第三者は入札者に入札価格を事前に命令できて，入札者は補償を受けることができる．補償を受けるためには，第三者の要求の入札価格を入札をしたとのことを証明しなければならない．

■ Abe-Suzuki 技法での RFC

準備
$\{A_i \ | i = 0,..., a\}$ は競売人で，$\{B_j \ | j = 0,..., 10\}$ は入札者という．競売人は A で入札者は b という．B_{10} は入札強制者 (第三者) で，彼は理由ない低い価格で入札商品を落札できることを願う．そして，B_0 から B_9 は他の入札者に自身より低い価格で入札を要求する．他の部分は Abe-Suzuki の技法と同じである．

入札
各入札者は入札ブースで下記のように入札をする．入札者は秘密鍵 $x_j \in Z_q$ を選択して，彼の署名と共に彼の公開鍵 $h_j = g^{x_j}$ を発表する．入札者 (第三者) は，入札価格 $2 \in P$ で入札をして，他の入札者は入札価格 $1 \in P$ で入札をする．
入札者 B_j は彼の入札価格 $p_j \in P$ を決定する．彼は彼の秘密 Seeds$r_{l,\,j} \in Z_q (l = 1, 2,..., m)$ をランダムにするように選択して，chameleon bit-commitments の順序を計算する．

$$C_{l,\,j} = \begin{cases} g^{M_1} h^{r_{l,\,j}} & (l = p_j) \\ g^{M_0} h^{r_{l,\,j}} & (l \neq p_j) \end{cases}$$

入札者は彼の署名と commitments$(l_{1,\,j}, l_{2,\,j},..., l_{m,\,j})$ の順序を発表する．入札者は各競売人 A_i に chameleon bit-commit の秘密鍵 $log_g h_j = x_j$ と $log_g C_{i,\,j}$ を内部ゼロ知識証明により証明する．

オープニング
オープニングで落札者は最も高い価格を入札した B_{10} となる．他の入札者は補償を 受けるために，自身の入札価格 $p_j(1) \in P$ と秘密鍵 $x_j \in Z_q$ と秘密シード $r_{i,\,j} \in Z_q (l = 1, 2,..., m)$ を第三者を通し， 自身の入札価格を証明して， 補償を受ける．

5 結論

最近，暗号学的技術を基盤とした多くの秘密入札プロトコルが提案された．安全な秘密入札方式のためにいろいろな条件が必要である．その条件の中から談合防止のための無証拠性の技法は重要な要素である．秘密入札プロトコルのため最初の無証拠性の技法は Abe-Suzuki により提案され，Chen-Lee-Kim は準同型暗号を利用した無証拠性技法を提案した．しかし，提案された無証拠性の技法は完全な無証拠性の技法であると見ることができ

ない．入札価格の談合は競売に参加するすべての参加者を考慮ならなければならない．本論文で，我々は電子競売での無証拠性を再確立して，提案された無証拠性技法の安全性に対して分析した．

謝辞

本研究の一部は，文部科学省科学研究費補助金学術創成研究課題番号 14GS0218『社会基盤を構築するためのシステム LSI 設計手法の研究 (研究代表安浦寛人九州大学システム LSI 研究センター長) と 21 世紀 COE プログラム「システム情報科学での社会基盤システム形成」の支援を受けている．

参考文献

[1] J. Benaloh and D.Tuinstra.:*Receipt-Free Secret-Ballot Elections*, Proc. of STOC '94, pp544-553, 1994

[2] K.Sako and J.Kilian.:*Receipt-Free Mix-type Voting Scheme*, Proceeding of Eurocrypt '95, LNCS921, Springer-Verlag, pp393-403, 1995

[3] T.Okamotom.:*Receipt-Free Electronic Voting Scheme for Large Scale Elections*, Security Protocols Workshop, 1997

[4] H.Kikuchi.:*M.Harkavy and J.D.Tygar*, " *Multi-round Anonymous Auction Proto-cols*, Proceeding of Third USENIX Workshop on Electronic Commerce, pp61-74, 1998

[5] M.Naor, B.Pinkas and R.Summer.:*Privacy Preserving Auctions and Mechanism Design*, Proc. of ACM conference of E-commerce, pp129-139, 1999

[6] K.Omote and A.Miyaji.:*An anonymous auction protocol with a single non-trusted center binary trees*, Information security workshop-Proc. of ISW2000, LNCS 1975, Springer-Verlag, pp108-120, 2000

[7] M.Hirt and K.Sako.:*Efficient receipt-free voting based on homomorphic encryption*, Eurocrypt 2000, LNCS 1807, pp539-556, 2000

[8] B.C.Lee, K.J.Kim and J.S.Ma.:*Efficient Public Auction with One-Time Registra-tion and Public Verifiability*, Indocrypt 2001.

[9] K.Omote and A.Miyaji.:*An Anonymous Sealed-bid Auction with a Feature of Entertainment*, Transactions of Information Processing Society of Japan, Vol.42, No.8, Aug. 2001

[10] O.Baudron and J.Stern.:*Non-interactive Private Auctions*, Proc. of Financial Cryp-tography 2001, 2001

[11] M.Abe and K.Suzuki.:*M+1-st Price Auction using homomorphic encryption*, Proc. of Public Key Crytpography 2002, LNCS 2274, pp.115-124, 2002

[12] M.Abe and K.Suzuki.:*Receipt-Free Sealed-Bid Auction*, ISC2002, LNCS2433, pp191-199, 2002

[13] F.Brandt.:*Secure and Private Auctions without Auctioneers*, Technical Report FKI-245-02, Feb. 2002

[14] A.Juels and M.Szydlo.:*A Two-Server, Sealed-Bid Aucion Protocol*, Proc. of Finan-cial Cryptography 2002, 2002

[15] K.Omote.:*A Study on Electronic Auctions*, PhD theses, JAIST, 2002

[16] X.Chen, B.C. Lee and K.J.Kim.:*Receipt-free Electronic Auction Schemes Using homomorphic encryption*, Proc. of ICISC2003, pp275-290, 2003.