無需揭露未得標價之第(M + 1)高價秘密競標協定

The (M + 1)st-Price Sealed-bid Auction Protocol without Revealing Losing Bids

吳宗成
國立台灣科技大學資訊管理系
tcwu@cs.ntust.edu.tw

黃士原
國立台灣科技大學資訊管理系
D9209101@mail.ntust.edu.tw

摘要

所謂第(M + 1)**高價秘密競標，意指投標者**(bidders)**參與** M **項相同物品的拍賣，並投出彌封標單，開標單位排序前** M **高順位出價的投標者，即為得標者**(winners)**，並以第**(M + 1)**高價作為全部得標者的成交價。在各種不同的競標機制中，第** (M + 1)**高價秘密競標較能反應物品真實價格，廣泛用於金融商品拍賣，如股票與政府公債拍賣。我們在本論文中提出一個適用於網際網路環境的第**(M + 1)**高價秘密競標協定。系統共有四種參與角色：投標者、競標管理中心**(auction manager)**、競標商**(auctioneer)**及仲裁者**(arbitrator)**等。當投標者向競標管理中心註冊後，可匿名地多次參與競標活動。此外，我們所提出的協定尚可滿足下列安全需求：未得標價之私密性**(secrecy of losing bids)**、不可偽造性**(unforgeability)**、不可陷害性**(no framing)**、公平性**(fairness)**、無連結性**(unlinkability)**、可追蹤性**(traceability)**、可驗證性**(verifiability) **及不可否認性**(non-repudiation)**等。**

關鍵詞：第(M + 1)**高價秘密競標、未得標價之私密性、匿名性、不可偽造性**

一、序論

隨著電子商務的蓬勃發展，各種的網路交易方式因應而生，其中網路競標(Internet auction)**是最熱門的線上交易活動之一。根據** Forrester Research (**見** http://www.forrester.com) **的研究報告預測,全球商業活動將有百分之八十的比例透過網際網路進行處理，其中網路競標佔所有線上交易活動的四分之一**[19]**。目前最為人所熟悉的競標方式大抵上區分為公開拍賣**(open-cry auction) [12, 14, 17, 18]**與秘密競標**(sealed-bid auction) [1, 2, 3, 6, 9, 10, 13, 16, 21]**兩大類，其中秘密競標大多運用在政府採購、合約簽訂及金融商品的拍賣，如近來台灣高科技廠商(鴻海、華碩等)的合約簽訂亦漸採用網路秘密競標方式，其競標交易金額常高至數十億至數百億。由此可見，網路競標將成為重要的交易主流之一。**

與一般的秘密競標相較，第 (M + 1)**高價秘密競標具誘因相容**(incentive compatibility) [11, 20]**特性，誘使投標者以物品真實估價**(true evaluation)**作為出價，較能反應物品合理市場價格**(reasonable market price) **，因此常用於金融商品拍賣。此外，當** M = 1 **時，為第**(M + 1)**高價秘密競標的特例，即第二高價秘密競標，又稱為** Vickrey auction [13]**。在** 2001 **年，**Kikuchi [9,10] **利用可驗證秘密分享方法**(verifiable secret sharing)**提出第**(M + 1)**高價秘密競標協定，該方法滿足未得標價的私密性，但該論文缺點為開標單位個數需大於所有出價個數的總和，否則無法重建多項式，故要有非常多開標單位合作才能找出得標價。**2002 **年，**Abe **與** Suzuki [1, 2] **利用同構加密**(homomorphic encryption)**及混和與匹配技術**(mix and match technique) [8]**建構出第**(M + 1)**高價秘密競標協定，但缺點為每個投標者在出價階段需執行非常多次的零資訊證明**(zero-knowledge proof)**，降低整體運算效率。**

基本上，一個第(M + 1)**高價秘密競協定應滿足下列安全需求：**

1. **單次註冊**(one-time registration)**：投標者向競標管理機構註冊後，即可匿名多次參與競標活動。**
2. **匿名性**(anonymity)**：除了投標者自己與競標管理中心外，競標商與其他人均無法辨識投標者身份。**
3. **未得標價之私密性**(secrecy of losing bids)**：除了得標價外，其餘的出價維持私密。**
4. **不可偽造性**(unforgeability)**：其他的投標者沒有能力偽造他人的投標資訊進行投標。**
5. **不可陷害性**(no framing)**：競標商或其他**

的投標者沒有能力假冒其他合法的競標者。

6. **公平性**(fairness)：競標商會公平處理每筆投標資訊，無法偏袒某個投標者。
7. **無連結性**(unlinkability)：任何人無能力獲知同一個投標者在不同場競標的關連性。
8. **可追蹤性**(traceability)：在競標結束後，競標管理機構可識別得標者之身分。
9. **可驗證性**(verifiability)：在競標結束後，每個人可驗證得標資訊的合法性。
10. **不可否認性**(non-repudiation)：得標者得標後無法抵賴投標，防止投標者隨意、不負責任的出價。

本論文將提出一個無需揭露未得標價的第$(M+1)$高價秘密競標協定，該協定滿足前述特性，並在計算複雜度與通訊成本優於過去學者所提出的第$(M+1)$高價秘密競標協定。

二、本論文提出的協定

系統的參與角色共包含 n 個投標者(bidders)、一個競標管理中心(auction manager，AM)、一個競標商(auctioneer，A_u)及一個仲裁者(arbitrator，A_r)等角色，其中將 A_r 視為安全應用模組(secure application module，SAM)。任何人只要通過合法註冊程序即可成為投標者，由於單次註冊特性，投標者參與下場次競標不需再註冊。AM 為公正第三者，其負責之工作包括處理投標者註冊與託管投標者真實身分、公開系統參數、管理佈告欄、找出得標者與公布競標結果等。A_r 執行開標程序與找出得標價(winning price)，A_u 協助 A_r 開標。

在介紹本論文所提出的秘密競協定前，我們先定義以下參數：

B_i	令集合 $B=\{B_1, B_2, ..., B_n\}$，其中 B_i 代表第 i 個投標者，n 為投標者個數
BB	AM 管理的佈告欄(bulletin board)，儲存允諾值與得標資訊
ID_i	B_i 的身分資訊
PID_i	B_i 的假名
GID	GID(group identity information)為集合 B 的識別符
AID_f	AID(auction identity information)為第 f 場競標的識別符
(x, y)	一個體(entity)的金鑰對(key pair)
$E_y(\cdot)$	以公鑰 y 為加密金鑰的非對稱式加密函數
$D_x(\cdot)$	以私鑰 x 為解密金鑰的非對稱式解密函數
V	AM 公布的合法出價序列(price list) $V=\{v_k \mid 1\le k\le c\}$，其中共有 c 個合法出價由小到大排列
v_z	B_i 對商品的出價，其中 $v_z\in V$，$1\le z\le c$
a_i, b_i	B_i 根據出價 v_z 所產生的兩個出價字串
$h(\cdot)$	單向雜湊函數，如 SHA-1 [7]

本論文提出的第$(M+1)$高價秘密競協定分為五個階段：初始階段(initialization phase)、投標者註冊階段(bidder registration phase)、出價階段(bid submission phase)、開標階段(bid open phase)及得標者識別階段(winners identification phase)。在本論文中，投標者 B_i 利用群體簽章(group signature) [4]對出價進行簽署，競標商無法由出價資訊得知投標者真實身分，可達成投標者的匿名性。接下來，我們將本競標協定各階段的詳細作法敘述如下：

【初始階段】 AM 選擇兩個大質數 p 與 q，計算 $N=pq$ 及選擇一個整數 g，其中 g 的秩(order)最大為 $f(N)$。然後 AM 計算 RSA 金鑰對(e, d)，其中 e 與 d 滿足 $ed=1 \pmod{f(N)}$，f 為 Euler' s totient function。AM 選擇一個質數 w，其中 w 滿足 $w<f(N)$，最後公開參數 $\{N, g, e, w, h, GID\}$。AM、A_u 及 A_r 分別公布其公開金鑰。

【投標者註冊階段】 假設 B_i 向 AM 進行註冊，其投標者註冊程序如下所述：

步驟 1. B_i 隨機選擇一個整數 $x_i\in Z_w$ 做為私鑰，然後計算相對應的公鑰 y_i：

$$y_i = g^{x_i} \bmod N \qquad (1)$$

步驟 2. B_i 利用 Camenisch 等人[4]提到的離散對數之資訊簽章，計算 (g_i, e_i) 如下：

$$g_i = h(g^{h(s_i\|ID_i\|PID_i)} \bmod N) \qquad (2)$$

$$e_i = h(s_i \| ID_i \| PID_i) - x_i g_i \qquad (3)$$

其中 $s_i\in Z_w$ 為隨機亂數，然後傳送一個加密訊息 $E_{y_{AM}}(ID_i, PID_i, y_i, g_i, e_i)$ 給 AM。

步驟 3. AM 將 $E_{y_{AM}}(ID_i, PID_i, y_i, g_i, e_i)$ 解密，然後利用下列判斷式來驗證 B_i 是否知道 y_i 的離散對數值。

$$g_i = h(g^{e_i} y_i^{g_i} \bmod N) \quad (4)$$

步驟 4. **當** *AM* **信任** B_i **確實知道** y_i **的離散對數值** x_i **，** *AM* **就接受** B_i **的註冊，並將** $\{ID_i, PID_i, y_i\}$ **秘密保存，然後公布一個允諾值** $com_i = h(ID_i \| PID_i \| y_i)$ **在佈告欄** *BB* **上，以確保不可否認性的需求。**

步驟 5. *AM* **計算** B_i **的會員憑證**(membership certificate) $cert_i$ **：**

$$cert_i = (y_i + h(GID))^{d+1} \bmod N \quad (5)$$

並傳送 $cert_i$ **給** B_i **。**

步驟 6. B_i **利用下列判斷式驗證** $cert_i$ **的正確性。**

$$(y_i + h(GID))^{e+1} = cert_i^e \pmod N \quad (6)$$

當判斷式成立，則 B_i **接受** $cert_i$ **為合法憑證，並完成註冊。**

當 B_i **完成註冊程序後，我們將** B_i **的公鑰** y_i **視為他的會員金鑰**(membership key)**。**

【出價階段】在競標 AID_f **開始前，** *AM* **公布本次競拍商品項目、合法出價序列**(price list) $V = \{v_k \mid 1 \le k \le c\}$ **及投標截止時間等相關訊息於** *BB***。當** B_i **欲參與這次競標活動，則執行下列步驟：**

步驟 1. B_i **對商品出價為** $v_z \in V$ **，依據** v_z **產生兩個長度為** c bits **的字串** a_i **與** b_i **。**
首先，投標者亂數產生長度為 c bits **的字串** a_i **，其中每個字元** $a_{i,x} \in \{0, 1\}$ (for x = 1, 2, …, c)**。接著依下列規則產生字串** b_i **：**

$$\begin{cases} \text{if} \quad x \le z \quad , \quad \text{then} \quad b_{i,x} \ne a_{i,x} \\ (b_{i,x} \in \{0, 1\}, \text{for } x = 1, 2, \ldots, c) \\ \text{else} \quad b_{i,x} = a_{i,x} \end{cases}$$

然後 B_i **計算** $enc1_i = E_{y_{A_r}}(a_i)$ **與** $enc2_i = E_{y_{A_u}}(b_i)$ **。**

步驟 2. B_i **隨機選擇一個亂數** $s_i' \in Z_w^*$ **使得** $\gcd(s_i', e) = 1$**，然後計算其衍生會員憑證** (derived membership certificate) $cert_i'$ **與衍生會員金鑰** (derived membership key) y_i' **，利用** $cert_i'$ **與** y_i' **防止攻擊者獲取簽章的連結性：**

$$cert_i' = cert_i^{s_i'} \bmod N \quad (7)$$

$$y_i' = y_i^{s_i'} \bmod N \quad (8)$$

步驟 3. B_i **隨機選擇一個亂數** $u_i \in Z_w$ **並計算群體簽章**

$$d_i = (enc1_i \| AID_f) g^{u_i} \bmod N \quad (9)$$

$$l_i = s_i' x_i d_i + u_i \quad (10)$$

然後秘密傳送 $\{AID_f, (s_i', cert_i', y_i', d_i, l_i)\}$ **給** A_r**，其中** $gs1_i = (s_i', cert_i', y_i', d_i, l_i)$ **為一個具訊息復原的群體簽章。** B_i **計算** $enc2_i$ **的群體簽章** $gs2_i$ **並傳送** $\{AID_f, gs2_i\}$ **給** A_u**。**

步驟 4. A_r **先驗證** $\gcd(s_i', e) = 1$ **然後再驗證：**

$$cert_i'^e = (y_i' + h(GID)^{s_i'})^{e+1} \pmod N \quad (11)$$

$$enc1_i \| AID_f = g^{-l_i} y_i'^{d_i} d_i \pmod N \quad (12)$$

若驗證通過，則表示 $gs1_i$ **為一個合法的群體簽章，亦代表為合法出價。** A_u **同樣去驗證群體簽章** $gs2_i$ **的合法性。**

【開標階段】競標 AID_f **投標截止後，** A_r **與** A_u **分別計算** $a_i = D_{x_{A_r}}(enc1_i)$ **與** $b_i = D_{x_{A_u}}(enc2_i)$ **。** A_r **初始設定索引值** $min = 1$ **與** $max = (c+1)$ **，並設定搜尋索引值** $a = \lfloor (min + max)/2 \rfloor$ **及計數器** $x = 0$**。詳細的開標程序敘述如下：**

步驟 1. A_r **與** A_u **執行下列動作：**

(1-1) A_r **從字串** a_1 , a_2 , …, a_n **萃取字元** $a_{1,a}$, $a_{2,a}$, …, $a_{n,a}$ **。**

(1-2) A_u **從字串** b_1 , b_2 , …, b_n **萃取字元** $b_{1,a}$, $b_{2,a}$, …, $b_{n,a}$ **，然後傳送至** A_r**。**

步驟 2. A_r **計算大於、等於出價** a **的投標人數**

$$x = \sum_{j=1}^{n} (a_{j,a} \oplus b_{j,a}) \text{ 。}$$

步驟 3. A_r **判斷是否找到得標價：**

(3-1) **若** $x \geq (M+1)$**，則令** $min = a$**，否則** $max = a$**。**

(3-2) **令** $a = \lfloor (min + max)/2 \rfloor$ **。如果** $a = min$**，則輸出得標價** v_{min}**，否則回到步驟** 1**。**

步驟 4. A_r **與** A_u **執行下列動作找出得標者：**

(4-1) **在步驟** 3**，出價大於、等於** v_{min} **的** $(M+1)$**個人中，將出價為** v_{min} **的投標者刪除，剩餘的** M **個人為得標者**(winners)**。所以在**$(M+1)$**個得標候選字串**(candidate string) a_j **與** b_j **中，** A_r **萃取字元** $a_{j,a+1}$**，** A_u **萃取字元** $b_{j,a+1}$ **並傳送至** A_r**。** A_r **檢查** $a_{j,a+1} \oplus b_{j,a+1}$**，若結果為** 0**，則將這對** a_j **與** b_j **從得標候選字串中刪除。最後剩餘字串**(remainder string)**為得標字串**(winning string)**。**

(4-2) A_r **公布含有得標字串的得標資訊** $\{AID_f, gs1_i\}$ **於公佈欄** BB**。**

【得標者識別階段】 AM **從** BB **讀取**$(M+1)$**筆的得標資訊** $\{AID_f, gs1_i\}$**，然後搜尋滿足** $y_i' = y_i^{s_i'} \bmod N$ **的資訊**$\{ID_i, PID_i, y_i\}$**。最後**AM **公布**$(M+1)$**筆的假名** PID_i **為得標者。**

以下我們說明本論文中所使用到的驗證式均是正確的。

定理 1. 如果(4)**式成立，則代表** B_i **確實擁有會員金鑰** y_i **的離散對數值** x_i**。**

證明：

$$g_i = h(g^{e_i} y_i^{g_i} \bmod N)$$

$$= h(g^{h(s_i \| ID_i \| PID_i) - x_i g_i} y_i^{g_i} \bmod N) \quad \text{(根據(3)式)}$$

$$= h(g^{h(s_i \| ID_i \| PID_i) - x_i g_i} g^{x_i r_i} \bmod N) \quad \text{(根據(1)式)}$$

$$= h(g^{h(s_i \| ID_i \| PID_i)} \bmod N)$$

由此可知， B_i **握有秘密值** x_i**。**

定理 2. 若(6)**式成立，則會員憑證** $cert_i$ **確實由** AM **所發出。**

證明：

$$cert_i^e = (y_i + h(GID))^{(d+1)e} \quad \text{(根據(5)式)}$$

$$= (y_i + h(GID))^{1+e}$$

$$= (y_i + h(GID))^{e+1} (\bmod N)$$

定理 3. 若(11)**式與**(12)**式成立，則** $gs1_i$ **為合法的群體簽章，其中訊息** $enc1_i$ **的復原經由**(12)**式完成。**

證明：

$$cert_i'^e = cert_i^{s_i' e} \quad \text{(根據(7)式)}$$

$$= (y_i + h(GID))^{s_i' e(d+1)} \quad \text{(根據(5)式)}$$

$$= (y_i + h(GID))^{s_i' + s_i' e}$$

$$= (y_i' + h(GID)^{s_i'})^{e+1} (\bmod N) \quad \text{(根據(8)式)}$$

當(11)**式成立，則可以確保** B_i **確實為提出衍生會員憑證** $cert_i'$ **與衍生會員金鑰** y_i' **的合法投標者。**

$$g^{-l_i} y_i'^{d_i} d_i = g^{-s_i' x_i d_i - u_i} y_i'^{d_i} d_i \quad \text{(根據(10)式)}$$

$$= g^{-s_i' x_i d_i - u_i} y_i^{s_i' d_i} d_i \quad \text{(根據(8)式)}$$

$$= g^{-s_i' x_i d_i - u_i} g^{s_i' d_i x_i} d_i \quad \text{(根據(1)式)}$$

$$= g^{-s_i' x_i d_i - u_i} g^{s_i' x_i d_i} (enc1_i \| AID_f) g^{u_i} \quad \text{(根據(9)式)}$$

$$= enc1_i \| AID_f$$

當(12)**式成立，則可確保** B_i **不但是一個合法投標者，亦確定他是衍生會員金鑰** y_i' **的真正擁有者，因為** B_i **不知道** y_i' **的離散對數值，就無法計算出滿足**(12)**式的** (d_i, l_i)**。**

三、安全性分析與效率評估

本論文所提出的協定，其安全性主要植基於下列的密碼學假設，當假設成立，則本論文的協定是安全的。

因式分解假設(FAC)：令 N **為兩大質數** p **與** q **乘積的合成數，欲由** N **分解出** p **與** q**，在計算上是不可行的**[4]**。**

解合成數之離散對數假設(DLMC)：令 N **為兩**

大質數 p 與 q 乘積的合成數，g 為一個在乘法群 $(Z/Z_n)^*$ 中最大秩的整數。給定一個整數 y 滿足 $y = g^x \bmod N$，欲從給定的 y 值求出 x 值為計算上不可行[12]。

(一) 安全性分析

以下我們分別說明本論文提出的協定滿足安全需求：單次註冊、匿名性、未得標價之私密性、不可偽造性、不可陷害性、公平性、無連結性、可追蹤性、可驗證性、不可否認性等。

達成單次註冊之分析：即使開標結果公布後，B_i 在投標者註冊階段產生的私鑰 x_i 並未曝光，因此 B_i 仍可匿名參與下一輪競標，並直接出價，省略再註冊的計算與通訊成本。

達成匿名性之分析：因群體簽章特性，每個人可驗證群體簽章的合法性，但無法得知是何人所出價。只有競標管理中心 AM 知道投標者身分，因為他知道投標者身分資訊 ID_i 與會員金鑰 y_i 之間的關係。

達成未得標價之私密性的分析：在開標階段，A_u 利用一個出價計數器來找出得標價，因此沒有揭露未得標價，故除了得標價外，其餘出價皆維持私密性。

達成不可偽造性之分析：除非攻擊者可以產生滿足(11)式的 $cert_i^*$，s_i^*，y_i^* 及 y_i^* 的離散對數 x_i^*，否則無法偽造合法的群體簽章。不幸的，攻擊者可用下述方法計算出 $cert_i^*$，s_i^*，y_i^* 及 y_i^* 的離散對數 x_i^*：

(i) 給定兩個整數 a^* 與 b^*，然後計算 $cert_i^* = (g^{a^*} + h(GID)^{b^*})^{e+1} \bmod N$。

(ii) 計算 $cert_i^*$ 的 e 次方：$cert_i^{*e} = (g^{a^* e} + h(GID)^{b^* e})^{e+1} \bmod N$。

(iii) 令 $s_i^* = b^* e$，$x_i^* = a^* e$ 及 $y_i^* = g^{x_i^*} \bmod N$。

如果攻擊者利用上述方法，他可偽造一個滿足(11)式與(12)式的群體簽章。但本論文提出的協定，在驗證群提簽章前，競標商需先檢查 $\gcd(s_i^*, e) = 1$，若 $\gcd(s_i^*, e) \neq 1$，則簽章不合法。因此，上述攻擊方法無法通過簽章驗證程序。

達成不可陷害性之分析：若某一投標者或 AM 獲得 B_i 的私鑰 x_i，則他們可假冒 B_i 簽署一個合法的群體簽章。但攻擊者要從系統的公開資訊中求得 x_i，將面臨解開合成數之離散對數的困難度。

達成公平性之分析：因為投標者的出價為匿名，其他人無法在系統公開的資訊中得知投標者出價，因此競標商會公平的處理每一筆出價資訊。

達成無連結性之分析：如果攻擊者可以取得 B_i 的會員金鑰 y_i 與會員憑證 $cert_i$，則他可以獲得群體簽章的連結性。為防止攻擊者得知簽章連結性，故本協定利用(7)式與(8)式來防止會員金鑰與會員憑證的曝光。除非攻擊者能解開合成數之離散對數的能力，否則無法取得 y_i 與 $cert_i$。

達成可追蹤性之分析：AM 有能力打開群體簽章以辨識投標者。因為只有 B_i 與 AM 知道 $\{ID_i, PID_i, y_i\}$，所以 AM 可藉由搜尋滿足 $y_i' = y_i^{s_i'} \bmod N$ 的資訊 $\{ID_i, PID_i, y_i\}$ 來找出得標者身分。

達成可驗證性之分析：每個人可驗證群體簽章的合法性，如果 B_i 簽署的群體簽章是合法的，則其投標亦是合法的。

達成不可否認性之分析：開標後，得標者不可否認得標資訊(winning bid)為他所投出。當一個得標者否認投標，AM 可公開滿足 $y_i' = y_i^{s_i'} \bmod N$ 的資訊 $\{ID_i, PID_i, y_i\}$。任何人可藉由計算 $com_i' = h(ID_i, PID_i, y_i)$ 並檢查 $com_i = com_i'$ 來確認得標者。所以，得標者無法否認得標。

(二) 效率評估

為方便進行效率評估，下列符號用來分析本論文所提出之協定的效率。令 T_E 為模指數運算所需的計算時間，T_M 為模乘法運算所需的計算時間，T_I 為模反元素所需的計算時間，T_H 為單向雜湊函數所需的計算時間，T_{ENC} 為加密一個訊息所需的計算時間，T_{DEC} 為解密一個密文所需的計算時間。對於其他運算度量指標，如模加法與模減法運算，因計算時間相對小於上述的度量指標，因此在我們的效率分析上將其省略。

表一與表二列出的是本論文所提出的協定與 Abe-Suzuki 協定[1, 2]及 Kikuchi 協定[9, 10]在計算時間與通訊成本的比較表。從表一與表二可發現，本論文所提出之協定計算效率與通訊成本皆優於其他協定

四、結論

我們提出了一個無需揭露未得標價之第(*M* + 1)高價秘密競標協定。在本協定中，除了得標價與得標者外，其餘資訊均維持私密性。此外，因單次註冊特性，每個投標者可匿名地多次參與競標活動，不需再次註冊。本論文提出的協定另滿足不可偽造性、不可陷害性、公平性、無連結性、可追蹤性、可驗證性及不可否認性等特色。另外，本論文提出的協定不管在計算複雜度與通訊成本上皆比過去學者所提出的第(*M* + 1)高價秘密競標協定更有效率。

五、參考文獻

[1] M. Abe and K. Suzuki, "*M* + 1-st Price Auction Using Homomorphic Encryption", *Public Key Cryptography PKC'02*, LNCS 2274, 2002, pp. 115-124.

[2] M. Abe and K. Suzuki, "*M* + 1-st Price Auction Using Homomorphic Encryption", *IEICE Transactions of Fundamentals*, Vol. E86-A, No. 1, 2003, pp. 136-141.

[3] C. Cachin, "Efficient Private Bidding and Auctions with an Oblivious Third Party", *The Sixth ACM Conference on Computer and Communications Security CCS'99*, 1999, pp. 120-127.

[4] J. Camenisch and M. Stadler, "Efficient Group Signatrue Schemes for Large Groups", *Advances in Cryptology - CRYPTO'97*, LNCS 1296, 1997, pp. 410-424.

[5] Y.S. Chang, T.C. Wu and S.C. Huang, "ElGamal-like Digital Signature and Multisignature Schemes Using Self-certified Public Keys", *The Journal of Systems and Software*, Vol. 50, No. 2, 2000, pp. 99-105.

[6] M.K. Franklin and M.K. Reiter, "The Design and Implementation of A Secure Auction Service", *IEEE Transaction on Software Engineering*, Vol. 22, No. 5, 1996, pp. 302-312.

[7] ISO 10118-3, "Information Technology - Security Techniques - Hash Functions - Part 3: Dedicated Hash-functions", International Organization for Standardization, 1998.

[8] M. Jakobsson and A. Juels, "Mix and Match: Secure Function Evaluation via Ciphertexts", *Advances in Cryptology - ASIACRYPT'00*, LNCS 1976, 2000, pp. 162-177.

[9] H. Kikuchi, "(*M*+1)st-price Auction Protocol", *Financial Cryptography FC'01*, LNCS 2339, 2001, pp. 351-363.

[10] H. Kikuchi, "(*M*+1)st-price Auction Protocol", *IEICE Transactions of Fundamentals*, Vol. E85-A, No. 3, 2002, pp. 676-684.

[11] P. Klemperer, "Auction Theory: A Guide to the Literature", *Journal of Economic Surveys*, Vol. 13, No. 3, 1999, pp. 227-286.

[12] M. Kumar and S. Feldman, "Internet Auctions", *The Third USENIX Workshop on Electronic Commerce*, 1998, pp. 49-60.

[13] H. Lipmaa, N. Asokan and V. Niemi, "Secure Vickrey Auctions without Threshold Trust", *Financial Cryptography FC'02*, 2002.

[14] B. Lee, K. Kim, and J Ma, "Efficient Public Auction with One-Time Registration and Public Verifiability", *Progress in Cryptology INDOCRYPT'01*, LNCS 2247, 2001, pp. 162-174.

[15] K. McCurley, "A Distribution System Equivalent to Factoring", *Journal of Cryptology*, Vol. 1, No. 2, 1988, pp. 95-105.

[16] M. Naor, B. Pinkas and R. Sumner, "Privacy Preserving Auctions and Mechanism Design", *Proceeding of ACM Conference on Electronic Commerce E-COMMERCE'99*, 1999, pp. 120-127.

[17] K. Omote and A. Miyaji, "A Practical English Auction with One-Time Registration", *Information Security and Privacy ACISP'01*, LNCS 2119, 2001, pp. 221-234.

[18] S. G. Stubblebine and P. E. Syverson, "Fair On-line" Auction without Special Trusted Parties, *Financial Cryptography FC'99*, LNCS 1648, 1999, pp. 230-240.

[19] Y. A. Tung, R. D. Gopal and A. B. Whinston, "Multiple Online Auctions", *Computer*, Vol. 36, No. 2, 2003, pp. 100-102.

[20] W. Vickrey, "Counterspeculation, Auctions, and Competitive Sealed Tenders", *Journal of Finance*, Vol. 16, No. 8, 1961, pp. 8-37.

[21] K. Viswanathan, C. Boyd and E. Dawson, "A Three Phased Schema for Sealed Bid Auction System Design" *Information Security and Privacy ACISP'00*, LNCS 1841, 2000, pp. 412-426.

表一 計算複雜度比較表

	投標者	**競標商**
本論文的協定	$14\,T_E + 9\,T_M + 4\,T_H$	$10\,T_E + 6\,T_M + 2\,T_H + 2\,T_I$
Abe-Suzuki **協定**	cT_{ENC}	$ncT_M + MT_{DEC}$
Kikuchi **協定**	$3cT_E + 2cT_M$	$3\,T_E + 2\,T_M$

註 1：**我們將** A_u **與** A_r **的計算成本併入競標商計算**

表二 通訊成本比較表

	投標者	**競標商**
本論文的協定	$12\|N\|$ ($\approx 24\|p\|$)	$12\|N\|$ ($\approx 24\|p\|$)
Abe-Suzuki **協定**	$c\|p\|$	$c\|p\|$
Kikuchi **協定**	$(m+c)\|p\|$	$m\|p\|$

註 2：$|x|$**代表整數** x **的位元數**(bit length)

註 3：m **為競標商個數**