

行政院國家科學委員會專題研究計畫 成果報告

頻譜規劃配置與管理基礎研究--子計畫二:無線頻譜執照釋 出的機制設計(3/3) 研究成果報告(完整版)

計畫類別：整合型
計畫編號：NSC 99-2219-E-009-002-
執行期間：99年08月01日至100年07月31日
執行單位：國立交通大學工業工程與管理學系(所)

計畫主持人：梁高榮

計畫參與人員：碩士班研究生-兼任助理人員：劉思宇
碩士班研究生-兼任助理人員：連惠珍
碩士班研究生-兼任助理人員：朱明典
碩士班研究生-兼任助理人員：彭思瑜
碩士班研究生-兼任助理人員：鄭仲元
碩士班研究生-兼任助理人員：方本欣
碩士班研究生-兼任助理人員：張宏
碩士班研究生-兼任助理人員：張舜龍
碩士班研究生-兼任助理人員：林哲慧
碩士班研究生-兼任助理人員：徐宏智

處理方式：本計畫涉及專利或其他智慧財產權，2年後可公開查詢

中華民國 100 年 08 月 01 日

行政院國家科學委員會補助專題研究計畫 成果報告
 期中進度報告

頻譜規劃配置與管理基礎研究-子計畫二：

無線頻譜執照釋出的機制設計(3/3)

計畫類別： 個別型計畫 整合型計畫

計畫編號：NSC 99-2219-E-009-002-

執行期間：99年8月1日至100年7月31日

執行機構及系所：國立交通大學工業工程與管理學系

計畫主持人：梁高榮

共同主持人：

計畫參與人員：劉思宇、連慧珍、朱明典、彭思瑜、鄭仲元、方本欣、張舜龍、
徐宏智、張宏、林哲慧

成果報告類型(依經費核定清單規定繳交)： 精簡報告 完整報告

本計畫除繳交成果報告外，另須繳交以下出國心得報告：

- 赴國外出差或研習心得報告
- 赴大陸地區出差或研習心得報告
- 出席國際學術會議心得報告
- 國際合作研究計畫國外研究報告

處理方式：除列管計畫及下列情形者外，得立即公開查詢

涉及專利或其他智慧財產權， 一年 二年後可公開查詢

中華民國 100 年 7 月 31 日

中文摘要：

基於兩項特色，本報告提出新的無線公正拍賣方法來改善頻譜資源的分配機制。首先是實作出賽局理論裡的斂核觀念來滿足公正的原則。從公正理論的觀點來看，透過斂核觀念所產生的價格比傳統用核觀念產生的價格好。其次是實作出密碼學裡的秘密分享技術。從務實面考量來說，這可以避免無線競價過程中潛在的圍標問題。此外為了彰顯本方法的實用性，本報告已將無線公正拍賣方法在手機上實作出來。

關鍵字：公正拍賣；斂核；無線競標；秘密分享技術；舒-瑞氏演算法

英文摘要：

A new wireless justice-based auction method has been proposed as a better spectrum resource assignment mechanism due to two salient features. One is to implement the nucleolus concept in game theory for satisfying the requirements of justice. From a justice-theoretic viewpoint, the generated price based on the nucleolus is a better approach than the traditional price based the core concept. The other is to implement the secret-sharing technology in cryptography. From a practical consideration, this is to avoid the potential corruption problem in wireless bidding process. Moreover the proposed justice-based wireless auction method has been implemented on mobile phones for showing its feasibility.

Keywords: Justice-based Auction; Nucleolus; Wireless Bidding; Secret-Sharing Technology; Solymosi-Raghavan Algorithm

目錄：

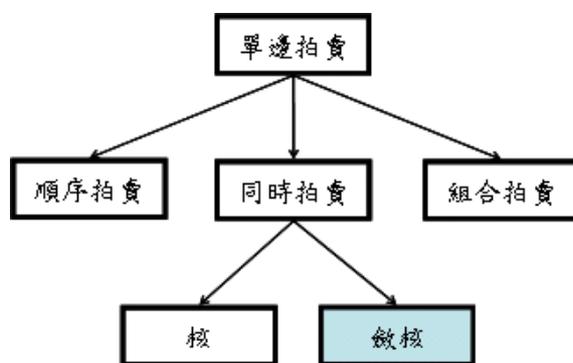
報告內容：

中文摘要	p. I
英文摘要	p. II
一、前言	p. 1
二、指派賽局的公正拍賣	p. 2
三、用秘密分享技術產生標單矩陣	p. 3
四、用利潤矩陣產生得標者名單	p. 5
五、用滿意度矩陣產生得標價格	p. 6
六、操作示範	p. 9
七、結論	p. 14
參考文獻	p. 15
計畫成果自評	p. 16

一、前言

進行無線頻譜產權轉移時，大家都希望在公開、公平、公益及公正的環境下進行交易。這裡公開是指交易訊息的透明化，也就是說讓有能力參與交易的人都能參加。公平是指交易的人都在平等的基礎上競爭，而非某些人有特權。公益是指將交易的利益極大化，這樣參與交易的人才能分享最大的利益，也就是經濟學裡的柏瑞圖最佳化(Pareto-optimal)[1]結果。公正是指交易時能堅持照顧到弱勢團體的正義原則[10]，也就是說將最弱勢團體的利益極大化。目前採用單邊拍賣(One-sided Auction)[1]來進行產權轉移時，大都能考量到公開、公平、及公益的原則，而本報告將探討如何在單邊拍賣裡的同時拍賣(Simultaneous Auction)[1, 9]進行公正拍賣(Justice-based Auction)；特別是透過無線競標(Wireless Bidding)方式來進行公正的拍賣。

在單邊拍賣制度中，通常可再細分為順序拍賣(Sequential Auction)、同時拍賣及組合拍賣(Combinatorial Auction)三大類[4]，如圖一所示。這裡順序拍賣指的是將待拍賣物依照順序而分別拍賣之。如果待拍賣物彼此是獨立的，也就是說沒有互補性或替代性等關係，則順序拍賣常被採用。同時拍賣是指參與競價的人可對任一待拍賣物同時出價。如果限定參與競價的人最多只能得標一次，則該同時拍賣稱為指派賽局(Assignment Game)[1, 8, 13]。組合拍賣是指參與競價的人可對任一組待拍賣物出價[4]。同時拍賣及組合拍賣常用於待拍賣物是相關的場景裡，也就是說待拍賣物可能具有互補性或替代性的關係。對參與競價的人來說，他們在組合拍賣裡會比在同時拍賣裡有更多的選擇機會。



圖一 單邊拍賣分類

對待拍賣物來說，指派賽局可以產生核裡價格(The Imputation of Core)[1, 9]，也就是說經濟學裡的柏瑞圖最佳化結果。柏瑞圖最佳化的結果符合前述的公益原則，但不一定會符合公正原則。前述的公正原則來自公正理論(Justice Theory)[10]，隨後發現其理念可用賽局理論(Game Theory)裡的斂核(Nucleolus)[6, 9, 11]數學模式描述。在公正理論裡，這是指將最弱勢團體的福利最大化。在賽局理論裡，這是指將最小滿意度(Satisfaction)[14]團體的滿意度極大化。對指派賽局來說，其斂核的計算更可透過舒-瑞氏演算法(Solymosi-Raghavan Algorithm)[3, 14]來計算。當核裡價格存在時，這裡必須再強調的是斂核價格一定是核裡價格，但核裡價格不一定是斂核價格。

由於指派賽局常透過電腦網路來進行產權的轉移，例如我國的第三代行動通信執照[2, 3]就是透過開放式電腦網路進行同時拍賣並產生核裡價格。如果採用標單內容不開放方式來競標，則開標過程會有洩露底標的危機存在。針對此問題，本報告將採用秘密分享技術(Secret Sharing Technology)[1, 12]並從無線競標的角度來說明如何防止洩露底標。秘密分享技術使得公正拍賣更容易進行。

為說明無線競標的公正拍賣，底下先說明指派賽局的公正拍賣架構。公正拍賣包含標單、得標者名單與得標價格三項要素，所以其內容可分成(1)用秘密分享技術[1, 12]產生標單矩陣(Bids Matrix)、(2)用利潤矩陣(Profits Matrix)產生得標者名單、與(3)用滿意度矩陣(Satisfaction Matrix)產生得標價格三項步驟來依序進行。隨後說明秘密分享技術的內容，並舉例來說明標單矩陣的產生。其次將標單矩陣轉成利潤矩陣，再說明如何透過匈牙利人法(Hungarian Method)[8]來從利潤矩陣產生得標者名單。隨後將利潤矩陣轉成滿意度矩陣後，再用舒-瑞氏演算法[14]算出得標價格。接著說明實作後的操作步驟；這包含採用 J2ME(Java 2 Platform, Micro Edition)技術[5]來實作秘密分享方法，而用 J2SE(Java 2 Platform, Standard Edition)技術[5]實作斂核開標系統。最後則是結論。

二、指派賽局的公正拍賣

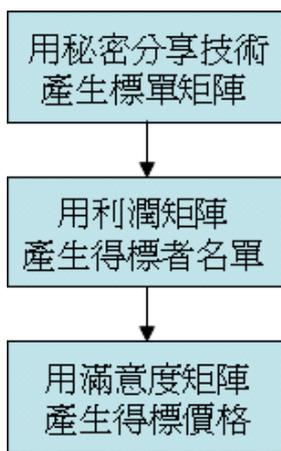
在拍賣型式(Auction Type)[7]中，同時拍賣常依待拍賣物數目、標單內容及成交價格三項特性來分類。就待拍賣物數目來說，它可分為單件拍賣與多件拍賣兩大類。就標單內容來說，它可依內容是否公開而分為開式拍賣與閉式拍賣兩大類。就成交價格來說，它可依標單價格的最高價、次高價及公正價而分為首價拍賣、次價拍賣及公正價拍賣三大類。理論上，首價拍賣的平均價格及次價拍賣的價格都是核裡價格[3]，而公正價是斂核價格。依這三項特性，表一顯示共十二種的拍賣型式，而用其特性來命名。對單件拍賣來說，傳統上首價開式拍賣又稱為荷蘭式拍賣(Dutch Auction)，首價閉式拍賣稱為投標法，次價開式拍賣稱為英國式拍賣(English Auction)，而次價閉式拍賣稱為維氏拍賣(Vickrey Auction)[7]。

本報告主要是分析公正拍賣，由於單件拍賣是多件拍賣的特例，所以將針對多件拍賣來說明。就多件拍賣的公正價格形成來說，同時開式公正拍賣只要對最後一回合進行閉式公正拍賣的計算就可以。所以本報告的分析重點將集中於閉式公正拍賣的說明上。

表一 拍賣型式

	拍賣型式	開式	閉式
單件拍賣	首價	荷蘭式拍賣	投標法
	次價	英國式拍賣	維氏拍賣
	公正價	開式公正拍賣	閉式公正拍賣
多件拍賣 (指派賽局)	首價	同時荷蘭式拍賣	投標法
	次價	同時英國式拍賣	維氏拍賣
	公正價	同時開式公正拍賣	閉式公正拍賣

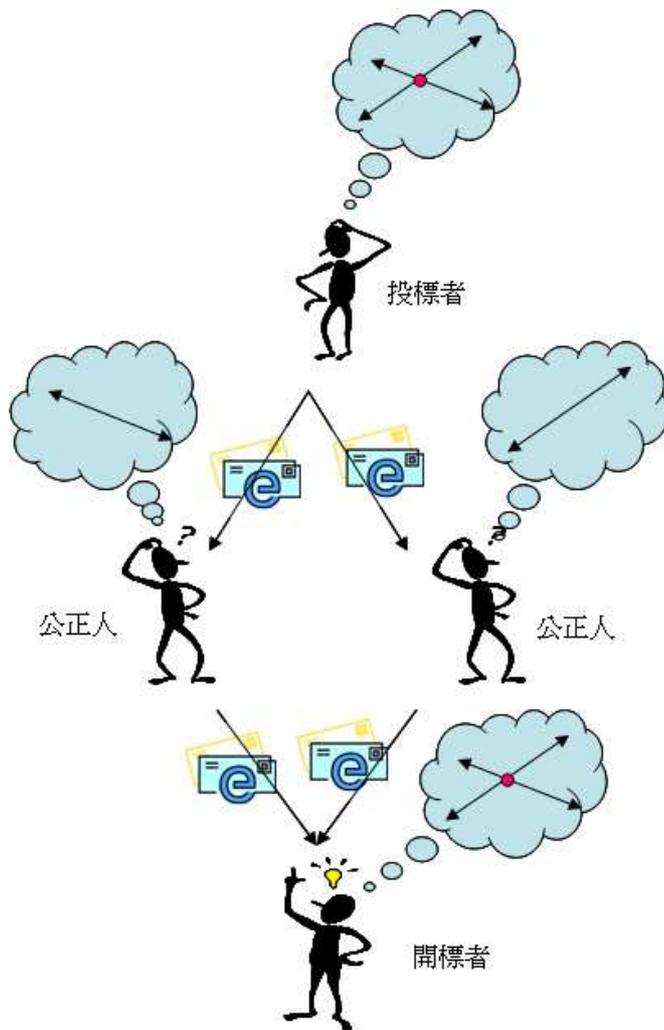
公正拍賣的內容包括標單、得標者名單與得標價格三項要素，而這三者可用標單矩陣、利潤矩陣與滿意度矩陣來產生。從此角度來看，公正拍賣的作業流程可分為三項步驟，如圖二所示。第一步驟為用秘密分享技術產生標單矩陣；這是將所有投標者的標單透過秘密分享技術匯入並整理於標單矩陣中。第二步驟為用利潤矩陣產生得標者名單；這是將所有投標者的競價減去標的物底價後所產生的利潤矩陣。再透過匈牙利人法求出最佳指派的得標者。第三步驟為用滿意度矩陣算出得標價格；這是透過滿意度轉移方式將最小滿意度團體給予極大化，也就是求其斂核的成交價格解。



圖二 公正拍賣的作業流程

三、用秘密分享技術產生標單矩陣

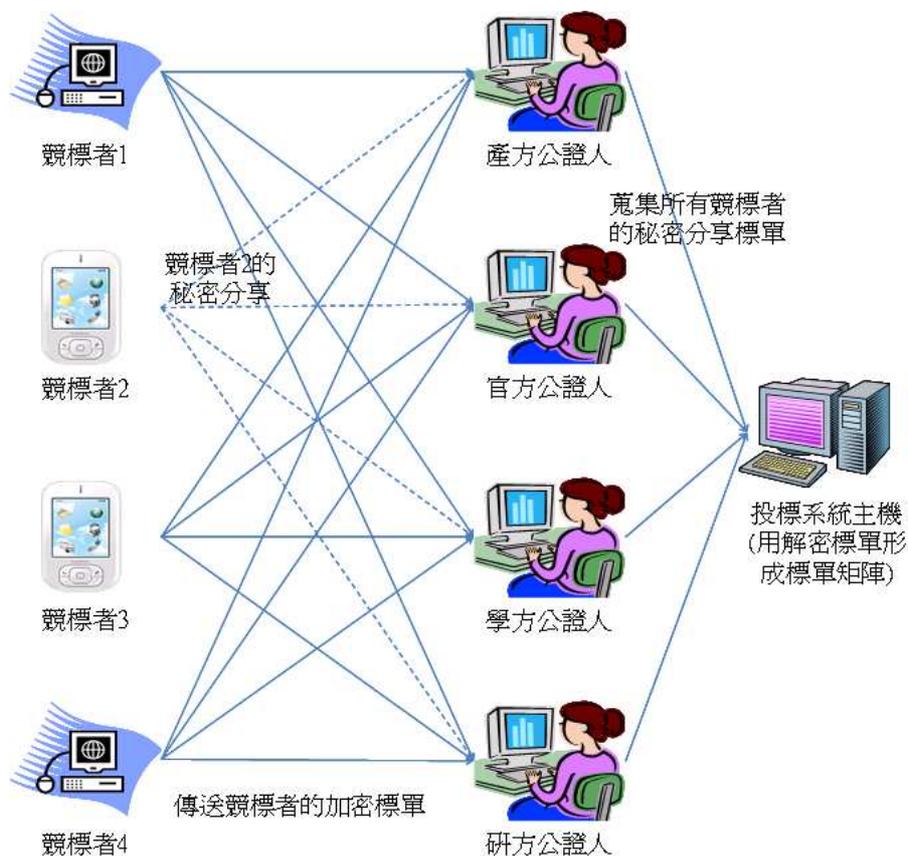
由表一可以知道標單有開式與閉式兩種呈現方式。如果要建構一套網際網路上的投標系統，則必需要考量這兩種標單的處理。由於開式標單是公開進行的，因此沒有洩密的問題；但閉式標單就必需另外特別處理來防止標單內容的洩漏。特別是當在網路上繳交標單後，如何防止收標單人的洩密。目前最常採用的防止洩密方法是秘密分享[1, 12]技術，所以本報告採用秘密分享技術來防止洩密。



圖三 秘密分享型的投標觀念

對秘密分享技術而言，這是將標單以不同的方法加密後，再寄給不同的公證人；但如果開標人蒐集全到公證人的加密標單後，則可透過解密技術還原出原始標單的內容。例如，假設空間中某點的 X 座標代表標單底價，則可將通過此點的两條直線之方程式分別寄給兩位公證人。每位公證人無法憑著單一直線方程式解出該點的座標，但開標人蒐集到公證人的兩條直線方程式就可解出該點的座標，如圖三所示。

本網路投標系統就採用圖三的秘密分享技術來設計，而更詳細的設計細節可參考[1, 12]。在圖四的架構中，這裡投標人可能會在不同的時間投標，但開標時間一到，開標人會同時取得所有公證人的加密標單並解出標單的底價。如果採用手機上網投標，則為防止電信公司半路攔標，標單還好是經過 RSA 法則裡的公匙(Public Key)[1]加密後再傳送會較為安全。



圖四 秘密分享型的網路投標系統

取得所有投標人的標單底價後，開標人就可建立標單矩陣。底下採用表二為例來說明標單矩陣的內容。假設現有三樣待拍賣的物品，分別為 X、Y 和 Z，且其底價各為 100 萬元、200 萬元及 300 萬元。現有四位投標人 A、B、C 和 D 分別對 X、Y 和 Z 三項拍賣物進行投標。本拍賣規定每一位買方最多只能得標一項物品，此即為一個典型的三物四人指派賽局[8, 13]。透過圖四的網路投標系統，開標人建立的標單矩陣如表二所示。它代表 A 對 X、Y 和 Z 的投標金額分別為 370 萬元、490 萬元及 500 萬元；B 對 X、Y 和 Z 的投標金額分別為 310 萬元、220 萬元及 460 萬元；C 對 X、Y 和 Z 的投標金額分別為 140 萬元、260 萬元及 300 萬元；D 對 X、Y 和 Z 的投標金額分別為 380 萬元、280 萬元及 320 萬元。這裡投標金額不代表得標金額，而代表其出價上限。換言之，這裡投標金額代表投標人對該拍賣物的最少獲利金額，否則投標人決不會出此價格。

表二 標單矩陣(單位：萬元)

產品	拍賣底價	A 出價	B 出價	C 出價	D 出價
X	100	370	310	140	380
Y	200	490	220	260	280
Z	300	500	460	300	320

四、用利潤矩陣產生得標者名單

在建立投標矩陣後，接著就是將投標矩陣轉為利潤矩陣，再用利潤矩陣產生得標者名單。對利潤矩陣的產生來說，這是將表二中所有買方對拍賣物的出價減去各拍賣物的拍賣底價後可以得到利潤矩陣如表三所示。例如表三的第二列第二行的金額 270 萬元($= 370 - 100 = a_{XA}$)代表買方 A 取得拍賣物 X 時得到的利潤。餘此類推，就可由表二產生表三。由於出價一定要高或等於拍賣底價，所以利潤矩陣的元素 a_{ij} 沒有負值，即 $a_{ij} \geq 0$ 。 a_{ij} 又稱為利潤的理論值，它代表利潤團體(Coalition)理論上可以共同得到的利潤。更由於利潤矩陣的元素數目比投標矩陣少，又可降低計算得標者名單的計算複雜度，故採用利潤矩陣來計算得標者名單。

表三 利潤矩陣(單位：萬元)

產品	A	B	C	D
X	270	210	40	280
Y	290	20	60	80
Z	200	160	0	20

對利潤矩陣來說，它的功能是用來產生得標者名單。由於拍賣的目的在產生核裡價格[8, 13]，也就是柏瑞圖最佳化[11]。柏瑞圖最佳化下的得標者名單結果也可透過匈牙利人法來計算。例如表三的陰影區就是得標者名單；換言之，拍賣物 X 的得主為 D，拍賣物 Y 的得主為 A，拍賣物 Z 的得主為 B。匈牙利人法的執行細節可參考[1]。

雖然匈牙利人法可以產生得標者名單，它卻無法產生公正的得標價格。例如買方 D 的投標金額為 280，它代表 $a_{XD} = 280$ ，但卻不知道買方 D 應付多少利潤給 X。同理，買方 A 與 B 也有會面對同樣的問題。又公正的得標價格要求最小滿意度團體的利潤最大化。這最小滿意度最大化過程需要有滿意度的初始解，然後再針對初始解改進直到收斂[6, 11]為止。這收斂的解就稱為斂核。為了產生斂核，這必需先將利潤矩陣轉為滿意度矩陣方可進行，底下將詳細說明之。

五、用滿意度矩陣產生得標價格

產生得標者名單後，接著是用滿意度矩陣產生得標價格。得標價格的產生可分(1)建立滿意度矩陣、(2)滿意度矩陣性質、(3)最小滿意度最大化及(4)計算的簡化四部份來說明清楚。對建立滿意度矩陣而言，它來自利潤矩陣。更詳細來說，這是先將競價者重新整理，並使得未得標者在前，而得標者在後並呈對角線化排列。接著增加代表賣方實際利潤的 U 欄與買方實質利潤的 V 列。例如表三可依此法則轉換為表四的格式，而表四的陰影區代表對角線化的結果。滿意度矩陣的初始值可用對角線化值來設定，例如得標者的出價可以先放入 U 欄內，而 V 列的值先設定為 0，如表四所示。滿意度矩陣的元素 s_{ij} 稱為利潤團體 $\{i, j\}$ 的滿意度，它的定義為 $s_{ij} = u_i + v_j - a_{ij}$ ，其中 u_i 為賣方實際利潤， v_j 為買方實際利潤， a_{ij} 為前述的利潤理論值。當實際利潤和大於理論利潤時，滿意度為正值；反之，滿意度為負值。例如在表四中， $s_{XC} = 240 = u_X + v_C - a_{XC} = 280 + 0 - 40$ ， $s_{XD} = 0 = u_X + v_D - a_{XD} = 280 + 0 - 280$ ，餘則類推。

表四 滿意度矩陣(單位：萬元)

	賣方利潤 U	C	D	A	B
買方利潤 V	0	0	0	0	0
X	280	240	0	10	70
Y	290	230	210	0	270
Z	160	160	140	-40	0

對滿意度矩陣性質而言，這可分為(1)得標者團體與(2)非得標者團體兩部份來說明。就得標者團體來說，這是指表四的陰影區。觀察其滿意度矩陣可以發現得標者團體的滿意度一定為 0，故又稱為固定滿意度(Settled Satisfaction)。就非得標者團體來說，這是指表四裡的非陰影區。其滿意度可透過利潤的流動來調整，故又稱為變動滿意度(Unsettled Satisfaction)。例如表五中，如果 Y 退回 1 萬元，則 $s_{YC} = 229$ ， $s_{YD} = 209$ ， $s_{YB} = 269$ ，但為了保持得標者團體 $s_{YA} = 0$ 的性質，所以會產生 $v_A = 1$ ， $s_{XA} = 11$ ， $s_{ZA} = -39$ 的結果。這裡可以看出利潤的流動會產生滿意度的改善，例如原先 $s_{ZA} = -40$ ，但結果為 $s_{ZA} = -39$ 。由於 $s_{ZA} = -40$ 是表四非得標者團體的最小滿意度，而利潤的流動會改善最小滿意度。持續最小滿意度的最大化就會達到計算出斂核的目的。

表五 滿意度矩陣的利潤流動(單位：萬元)

	賣方利潤 U	C	D	A	B
買方利潤 V	0	0	0	1	0
X	280	240	0	11	70
Y	289	229	209	0	269
Z	160	160	140	-39	0

對最小滿意度最大化而言，這是透過利潤的流動來調整最小滿意度。換言之，利潤的流動是先找出最小滿意度值 α 與決定最大調整值 β 。例如表四的最小滿意度是 $\alpha = s_{ZA} = -40$ ，而第二小滿意度是 $s_{VD} = 0$ ；為保持 s_{ZA} 是最小滿意度，利潤的流動結果是造成 $s_{ZA} \leq s_{VD} = 0$ 。決定利潤流動的上限值就稱為最大調整值 β ，這裡 $\alpha + \beta \leq s_{VD}$ 或 $\beta \leq 0 - (-40) = 40$ 。所以表四的 A 欄全部加 40，但為了保持得標者團體的滿意度為 0，表四的 Y 列全部減 40。用最大調整值重新計算滿意度矩陣後就可得到表六。綜合言之，找出最小滿意度值 α 就是從非得標者團體找出最小滿意度值。接著找出最大調整值 β 就是找出可以調整利潤流動的最大值。

表六 用最大調整值重算滿意度矩陣(單位：萬元)

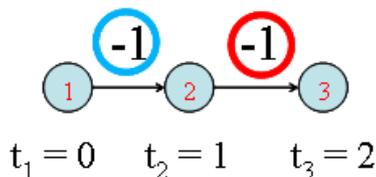
	賣方利潤 U	C	D	A	B
買方利潤 V	0	0	0	40	0
X	280	240	0	50	70
Y	250	190	170	0	230

Z	160	160	140	0	0
---	-----	-----	-----	---	---

當最小滿意度有很多個時，則需要採用有向圖(Directed Graph)技術[3, 14]來處理。以表七為例，如果以對角線為座標標準，則兩個最小滿意度可分別用座標(1, 2)及(2, 3)來代表，其值都是-1。改善最小滿意度時會涉及利潤的流動，而這流動可用向量來表達。仔細觀察可以發現前一向量的頭會變成後一向量的尾。連接所有的向量可構成有向圖，例如表七的所有最小滿意度可構成圖五的有向圖。如果有向圖包括迴徑(Cycle)時，則利潤的流動會造成問題，故可將迴徑融合以簡化有向圖。又不含迴徑的有向圖非常容易計算其 β 值，這時 t_j 值為連接向量的數目和。又最大調整值 β 可寫成表八上方的通式[3, 14]，其中 x_i 代表第 i 欄要增加的量，而 y_j 代表第 j 列要減少的量。表八上方的通式又可簡化而成為表八下方的公式。綜合研之，這是用 α 值座標畫有向圖，再計算箭號數目產生 t_j 值，接著由 t_j 值計算 s_j 值，隨後由 t_j 值與 s_j 值計算 β 值；而有向圖有迴路時，則進行迴路的融合。換言之，一直在有向圖上重覆此程序就可計算出斂核。

表七 最大調整值 β 的計算

	賣方利潤U	C	D	A	s_i
買方利潤V	0	0	0	0	0
X	6	0	-1	0	0
Y	5	5	0	-1	-1
Z	8	6	3	0	-2
t_j	0	0	+1	+2	

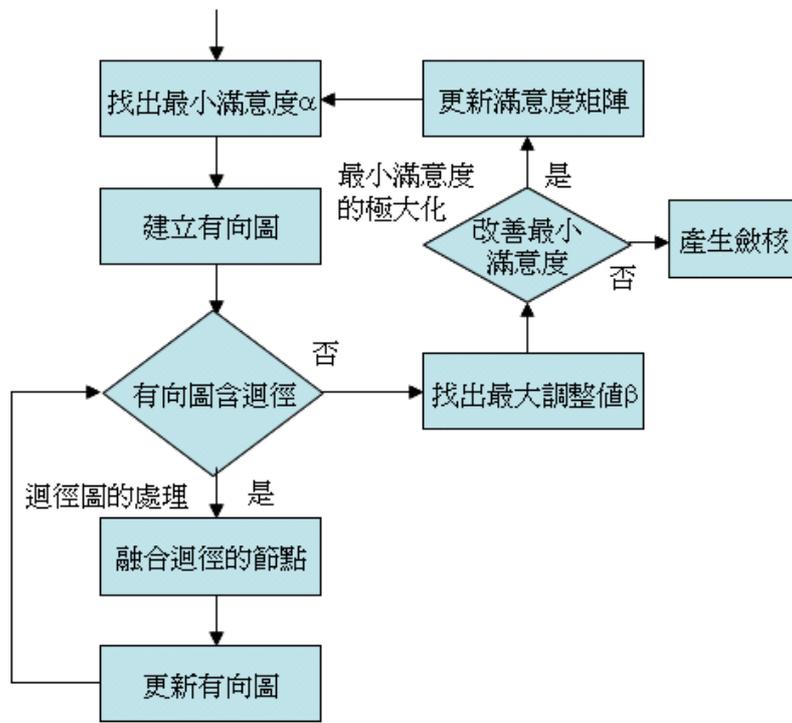


圖五 有向圖

表八 最大調整值 β 的計算

$Max \beta$ $\alpha + \beta \leq s_{ij} + \beta(x_i + y_j)$ $\beta \geq 0$
$Max \beta$ $\beta \leq \frac{s_{ij} - \alpha}{1 - (x_i + y_j)}$ $\beta \geq 0$

上述計算斂核的流程可分成最小滿意度的極大化與迴徑圖的處理兩個步驟來進行。最小滿意度的極大化是指調整實際利潤值 U_i 及 V_j 來改善滿意度。迴徑圖的處理是指將迴徑的點融合來產生沒有迴徑的有向圖。這兩個步驟的綜合使用如圖六所示。



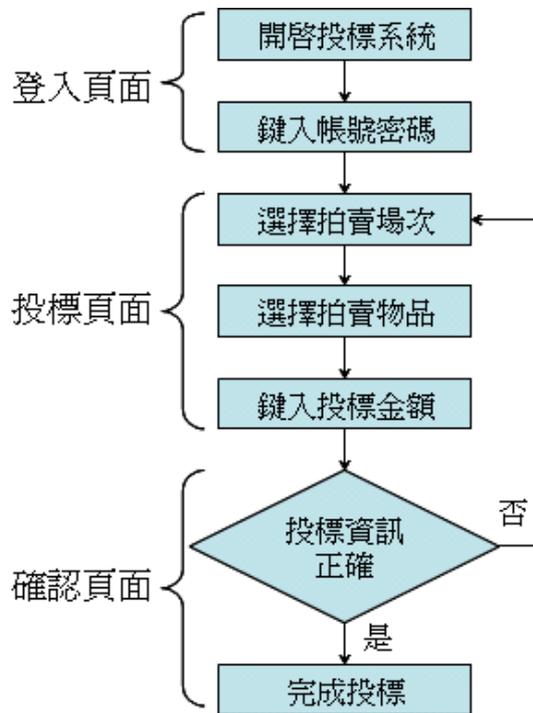
圖六 計算斂核流程

對計算的簡化而言，這是將最小滿意度的利潤團體透過舒-瑞氏演算法給予極大化。以表四為例，這裡有{X、Y、Z、A、B、C、D}7個成員，所以共有 $127(=2^7-1)$ 個部分集合或利潤團體；但由於每一位買方最多只能得標一項物品，事實上只會形成 $19(=(3+1) \times (4+1) - 1)$ 個實值上的利潤團體。從有向圖的角度來看，這涉及非得標者團體間的利潤流動，即有 $9(=4 \times 3 - 3)$ 種組合的計算。所以只要針對這9種組合來進行最小滿意度的最大化就可算出公正的得標價格。

六、操作示範

對指派賽局的公正拍賣而言，本實作系統由手機加密投標與公正價格開標兩套系統組成。前者採用 J2ME 技術[5]來進行開發，而後者採用 J2SE 技術[5]來進行開發。底下分別說明其各項功能與操作方式。

對手機加密投標系統而言，這包含鍵入帳號密碼、選擇拍賣場次、選擇拍賣物品、鍵入投標金額、確認投標資訊等動作。這些動作的操作介面可分成登入、投標及確認三頁面來分工，而操作時可依登入頁面、投標頁面及確認頁面順序來執行。加密投標的作業流程與三頁面的關係如圖七所示，而底下分別說明頁面的設計內容。



圖七 無線投標的作業流程

對登入頁面來說，這是由圖八(a)的頁面進行身份辨識，也就是輸入競標者的帳號及密碼。更詳細來說，這包含「帳號密碼」及「空值」兩項辨識功能。對前者來說，資料庫將自動比對是否擁有此組帳號密碼。對後者來說，如果帳號密碼處未鍵入任何值，這時畫面也會出現警告訊息。如果無法通過身份辨識，則會出現圖八(b)的錯誤訊息。待身份辨識通過後，競標者方可進行投標。



(a) 登入頁面 (b) 錯誤訊息



(c) 投標頁面 (d) 確認頁面
圖八 手機加密投標系統

對投標頁面來說，圖八(c)的畫面包含「拍賣場次」、「拍賣物品」、及「出價金額」三個輸入選項及「物品圖片」一個輸出項。競標者先利用「拍賣場次」的下拉式選單選擇要參與競標的拍賣場次。接著用「拍賣物品」的下拉式選單選取待拍賣物品。這時「物品圖片」出現該物品的圖片供競標者進行確認。最後競標者可於「拍賣物品」下方輸入出價金額，而此輸入選項亦有除錯機制。例如出價金額僅能輸入數字，及當無鍵入值時，畫面將出現錯誤訊息。出價金額輸入完後，再按下左下方的「送出」按鈕。

對確認頁面來說，畫面將再度呈現「拍賣場次」、「拍賣物品」、「物品圖片」及「出價金額」四項資訊供競標者確認。如果競標者要修改資料，這時可按下左方上一頁按鈕回到投標頁面進行修改。當競標者確認資料無誤後，這時可按下右方「確認送出」按鈕即可完成投標，如圖八(d)的畫面所示。換言之，這些競標資訊將透過秘密分享技術傳送至四位公證人，手機投標系統也隨之結束。圖九顯示投標者進行無線競標的情形。



圖九 無線競標的使用情形

對公正價格開標系統而言，其操作主要可分為表九的三大步驟，而使用時必須依序進行。第一步驟的主要功能在確認開標者的身份，而其人機介面為「安全認證」頁面。由於標單的機密性，因此必須確保開標的帳號與密碼正確後，開標者方可進入本系統操作。第二步驟的主要功能在取得標單矩陣，而其人機介面為「標單矩陣」頁面。這是透過解密方式來取得所有的標單。第三步驟的主要功能在產生利潤矩陣與滿意度矩陣，而其人機介面為「公正價格」頁面。利潤矩陣可用來產生得標者名單，而

滿意度矩陣則用來產生公正價格。這裡頁面是採用標籤頁面(Tabbed Panel)[5]程式設計方式呈現。底下分別說明「安全認證」頁面、「標單矩陣」頁面及「公正價格」頁面的使用。

表九 公正價格開標系統

操作步驟	1	2	3
功能說明	進行身份確認	獲得標單矩陣	從滿意度矩陣計算價格
頁面名稱	安全認證	標單矩陣	公正價格

就「安全認證」頁面來說，當開標系統啟動時，圖十的畫面就會自動出現。這時使用者可輸入帳號與密碼來確認身份。當輸入完成後，這時可按下送出鍵以供認證資料庫進行驗證。當驗證成功後，系統將自動切換至「標單矩陣」頁面。



圖十 「安全認證」頁面

就「標單矩陣」頁面來說，該畫面包含「清空資料庫」、「傳回加密標單」、「開始解密標單」及「進行開標」四個按鈕，及「加密標單」及「解密標單」兩個表格，如圖十一所示。操作時，先按下「清空資料庫」按鈕將所有的資料表清空以避免留下上次開標的殘遺資料。接著按下「傳回加密標單」按鈕，這時系統會自動向公證方發出收集加密標單的要求，而收集到的加密標單會顯示於「加密標單」表格中。確定加密標單接收完成後，再按下「開始解密標單」按鈕，這時系統會將加密標單自動解密，而解密後的標單顯示於「解密標單」表格中。在得到各個競標者的原始標單後，接著按下「進行開標」按鈕，這時畫面會自動切換至「公正價格」頁面。



圖十一 「標單矩陣」頁面

就「公正價格」頁面來說，該畫面包含「列印標單矩陣」、「求出得標者名單」、「計算斂核」及「斂核價格」四個按鈕，及「利潤矩陣」、「滿意度矩陣」及「斂核變數區」三個反應區塊。操作時，先按下「列印標單矩陣」按鈕，這時系統將會自動將標單矩陣轉成利潤矩陣並顯示於「利潤矩陣」區塊中。得到利潤矩陣後，接著按下「求出得標者名單」按鈕，系統會自動求出得標者名單，並以紅色字體標示於「利潤矩陣」區塊裡。找出得標者後就可以按下「計算斂核」按鈕，此時圖十二中的「滿意度矩陣」展示區及「斂核變數區」皆會出現計算結果。前者顯示出當前的滿意度矩陣。而後者則提供開標方進行各階段滿意度矩陣的比對。

以表四為例，圖十二可以看到「斂核變數區」包含「第 i 次滿意度」、「當前最小滿意度」及「當前最大調整值」三個標題。對「第 i 次滿意度」來說，這是以下拉式選單方式讓開標方可選擇觀看不同階段滿意度矩陣的計算過程。選定下拉式選單內容時，「滿意度矩陣」展示區會顯示對應的滿意度矩陣；同樣地，在「斂核變數區」內亦會顯示對應的最小滿意度 α 值及最大調整值 β 以方便開標方進行資料查核動作。



圖十二 「公正價格」頁面

當確認資料無誤後，這時可按下「斂核價格」按鈕，而系統會跳出一個斂核價格的新視窗來顯示出本次的拍賣結果。在斂核價格視窗各有四行，第一行是拍賣產品的名稱，第二行是得標者編號，第三行是競標金額，而第四行則是最終的斂核價格。例如圖十三的視窗中的第二列表表示拍賣產品 X 的得標者為買方 D，其得標金額為 380 萬元，而最終斂核所求出來的斂核價格則為含底價的 313.33 萬元。



圖十三 斂核價格

七、結論

為了達成以無線競標方式來進行公正的拍賣，本報告先說明其背後的學理要求，接著再提出達成該目標的兩項關鍵技術，即秘密分享技術及斂核計算技術。在分析完這兩項關鍵技術的各項執行細節後，本報告再提出各項執行細節的組合與操作方式。最後以這兩項關鍵技術為基礎，而分別開發出手機加密投標與公正價格開標兩套系統來。目前以這兩套系統的操作經驗來說，這已實現以無線競標方式來進行公正拍賣的原始構想。

[補充說明]：本計畫的執行內容與原先提案內容有點差異。這是由於當初提案時，國科會的審查委員要求要稍為調整方向以符合國家的總體研究需要。換言之，這是要強調組合拍賣技術的引進台灣；詳細說明請參考第二年的結案報告內容。

參考文獻：

- [1] 梁高榮，農產品交易工程學，國立交通大學出版社，1999年。
- [2] 梁高榮、許鈞豪，「第三代行動通訊執照拍賣軟體的規範測試」，機械工業，三月，210-224頁，2002。
- [3] 劉思宇、梁高榮，「透過無線競標進行公正拍賣」，機械工業，四月，141-151頁，2011。
- [4] 顧佳樺、梁高榮，「調頻廣播執照釋出的組合拍賣分析」，機械工業，六月，89-98頁，2010。
- [5] Deitel, H. M. and Deitel P. J., Java How to Program, 7th ed., Prentice Hall, 2007
- [6] Kohlberg, E., "The Nucleolus as a Solution of a Minimization Problem," SIAM Journal on Applied Mathematics, Vol. 23, pp. 34-39, 1972.
- [7] Krishna, V., Auction Theory, Academic Press, 2002.
- [8] Kuhn, H.W., "The Hungarian Method for the Assignment Game," Naval Research Logistics Quarterly, Vol. 2, pp. 83-97, 1955.
- [9] Owen, G., Game Theory, 3rd Ed., Academic Press, 1995.
- [10] Rawls, J., A Theory of Justice, President and Fellows of Harvard College, 1971.
- [11] Schmeidler, D., "The Nucleolus of a Characteristic Function Game," SIAM Journal on Applied Mathematics, Vol. 17, No. 6, pp. 1163-1170, 1969.
- [12] Shamir, A., "How to Share a Secret," Communications of the ACM, Vol. 22, No. 11, pp. 612-613, 1979.
- [13] Shapley, L. S. and Shubik, M., "The Assignment Game I: the Core," International Journal of Game Theory, Vol. 1, pp. 111-130, 1972.
- [14] Solymosi, T. and Raghavan, T. E. S., "An Algorithm for Finding the Nucleolus of Assignment Games," International Journal of Game Theory, pp. 119-143, 1994.

國科會補助專題研究計畫成果報告自評表

請就研究內容與原計畫相符程度、達成預期目標情況、研究成果之學術或應用價值（簡要敘述成果所代表之意義、價值、影響或進一步發展之可能性）、是否適合在學術期刊發表或申請專利、主要發現或其他有關價值等，作一綜合評估。

1. 請就研究內容與原計畫相符程度、達成預期目標情況作一綜合評估

達成目標

未達成目標（請說明，以 100 字為限）

實驗失敗

因故實驗中斷

其他原因

說明：

2. 研究成果在學術期刊發表或申請專利等情形：

論文： 已發表 未發表之文稿 撰寫中 無

專利： 已獲得 申請中 無

技轉： 已技轉 洽談中 無

其他：（以 100 字為限）

3. 請依學術成就、技術創新、社會影響等方面，評估研究成果之學術或應用價值（簡要敘述成果所代表之意義、價值、影響或進一步發展之可能性）（以 500 字為限）

1. 學術成就與技術創新:傳統上，無線頻譜執照釋出的價格主要有兩大類:首價與次價。本計畫則推薦第三類:公正價。首價與次價的優點是具有 Pareto-optimal 的性質，而公正價除具有 Pareto-optimal 性質外再加上斂核 (Nucleolus) 的特色，所以會符合經濟學裡公正的定義。除了建立計算公正價的計算流程外，本計畫已利用無線網路技術開發出其拍賣機制的軟體來。這也是目前已知可完整運作的第一套計算公正價軟體。

2. 社會影響:目前全世界尚沒有用公正價釋出無線頻譜執照的案例。如果我國可以實施，則將是全世界第一個採用此機制釋照的國家。(此方法很好用,但未普及的原因是其數學太難。)

國科會補助計畫衍生研發成果推廣資料表

日期:2011/07/28

國科會補助計畫	計畫名稱: 子計畫二:無線頻譜執照釋出的機制設計(3/3)
	計畫主持人: 梁高榮
	計畫編號: 99-2219-E-009-002- 學門領域: 無線通訊(國家型)
無研發成果推廣資料	

99 年度專題研究計畫研究成果彙整表

計畫主持人：梁高榮		計畫編號：99-2219-E-009-002-					
計畫名稱：頻譜規劃配置與管理基礎研究--子計畫二：無線頻譜執照釋出的機制設計(3/3)							
成果項目		量化			單位	備註（質化說明：如數個計畫共同成果、成果列為該期刊之封面故事...等）	
		實際已達成數（被接受或已發表）	預期總達成數(含實際已達成數)	本計畫實際貢獻百分比			
國內	論文著作	期刊論文	1	1	100%	篇	劉思宇，梁高榮，' ' 透過無線競標進行公正拍賣，' ' 機械工業,141-151,4月,2011.
		研究報告/技術報告	1	1	100%		
		研討會論文	0	0	100%		
		專書	0	0	100%		
	專利	申請中件數	0	0	100%	件	
		已獲得件數	0	0	100%		
	技術移轉	件數	0	0	100%	件	
		權利金	0	0	100%	千元	
	參與計畫人力 (本國籍)	碩士生	0	0	100%	人次	
		博士生	0	0	100%		
		博士後研究員	0	0	100%		
		專任助理	0	0	100%		
國外	論文著作	期刊論文	0	0	100%	篇	
		研究報告/技術報告	0	0	100%		
		研討會論文	0	0	100%		
		專書	0	0	100%	章/本	
	專利	申請中件數	0	0	100%	件	
		已獲得件數	0	0	100%		
	技術移轉	件數	0	0	100%	件	
		權利金	0	0	100%	千元	
	參與計畫人力 (外國籍)	碩士生	0	0	100%	人次	
		博士生	0	0	100%		
		博士後研究員	0	0	100%		
		專任助理	0	0	100%		

<p>其他成果 (無法以量化表達之成果如辦理學術活動、獲得獎項、重要國際合作、研究成果國際影響力及其他協助產業技術發展之具體效益事項等，請以文字敘述填列。)</p>	無。
--	----

	成果項目	量化	名稱或內容性質簡述
科 教 處 計 畫 加 填 項 目	測驗工具(含質性與量性)	0	
	課程/模組	0	
	電腦及網路系統或工具	0	
	教材	0	
	舉辦之活動/競賽	0	
	研討會/工作坊	0	
	電子報、網站	0	
	計畫成果推廣之參與(閱聽)人數	0	

國科會補助專題研究計畫成果報告自評表

請就研究內容與原計畫相符程度、達成預期目標情況、研究成果之學術或應用價值（簡要敘述成果所代表之意義、價值、影響或進一步發展之可能性）、是否適合在學術期刊發表或申請專利、主要發現或其他有關價值等，作一綜合評估。

1. 請就研究內容與原計畫相符程度、達成預期目標情況作一綜合評估

達成目標

未達成目標（請說明，以 100 字為限）

實驗失敗

因故實驗中斷

其他原因

說明：

2. 研究成果在學術期刊發表或申請專利等情形：

論文： 已發表 未發表之文稿 撰寫中 無

專利： 已獲得 申請中 無

技轉： 已技轉 洽談中 無

其他：（以 100 字為限）

3. 請依學術成就、技術創新、社會影響等方面，評估研究成果之學術或應用價值（簡要敘述成果所代表之意義、價值、影響或進一步發展之可能性）（以 500 字為限）

1. 學術成就與技術創新:傳統上，無線頻譜執照釋出的價格主要有兩大類:首價與次價。本計畫則推薦第三類:公正價。首價與次價的優點是具有 Pareto-optimal 的性質，而公正價除具有 Pareto-optimal 性質外再加上斂核(Nucleolus)的特色，所以會符合經濟學裡公正的定義。除了建立計算公正價的計算流程外，本計畫已利用無線網路技術開發出其拍賣機制的軟體來。這也是目前已知可完整運作的第一套計算公正價軟體。

2. 社會影響:目前全世界尚沒有用公正價釋出無線頻譜執照的案例。如果我國可以實施，則將是全世界第一個採用此機制釋照的國家。(此方法很好用,但未普及的原因是其數學太難。)