行政院國家科學委員會專題研究計畫成果報告

應用密碼技術進行工程競標中祕密底價制定之研究

Research on Cryptographic Solutions to Secretly Negotiating Reserve Prices for Project Bidding

計畫編號：NSC 88-2213-E-009-008
執行期限：87 年 08 月 01 日至 88 年 07 月 31 日
主持人：黃景彰　執行機構及單位名稱：國立交通大學資訊管理研究所

一、中文摘要

底價是保障公共工程品質的重要機制。要確實發揮保障工程品質、促進競標廠商公平競爭的作用，底價必須在開標前絕對保持隱密。本計畫設計了一個祕密底價制定協定，讓兩個底價制定者能夠在無法知道對方底價的情況下，正確地比較出兩者價格的大小。根據我們所設定的祕密底價制定協定，一群工程競標的底價制定者將可以共同產生一個祕密的底價。因此，本計畫的研究成果將有助於減少工程競標中底價外洩的情況，進一步提升工程競標的公平性。

關鍵詞：工程競標、底價、密碼技術

Abstract

Setting a reserve price for a publicly bid project helps to ensure the quality of the project. The price must be kept confidential before the opening of the bids; otherwise, the fairness of the bidding process would be infringed. In this research, we design a cryptographic protocol for two officials to compare their desired reserve prices without knowing the opponent's. With this protocol, a group of authorities responsible for the bidding of a public construction is able to negotiate a secret reserve price. We believe, the result can help prevent the leaking of reserve prices and ensure fairness in the bidding process.

Keywords: Auction for Public Construction, Reserve Price, Cryptographic Protocol

二、緣由與目的

競標活動是促成交易的一種常用方式。一般以最低價得標的祕密競標制度中，競標賣方通常會設立底價，以保障交易結果的品質。對於競標者而言，設定底價可以有效避免競標者之間削價競爭的損失，而賣方也能夠藉著設定底價嚇阻圍標等不良手段的發生。因此，設定底價已經成為最低價得標競標制度中用來保護交易品質的重要步驟。

底價的設立雖然有助於確保交易品質，但是也讓祕密競標活動的公平性更不容易維護。由於競標賣方可能私下將底價洩漏給特定競標者知道，使得特定競標者可以用接近底價的價格得標，這不但可能降低交易品質，也破壞了競標活動的公平精神。我們認為，在開標前防範底價外洩才能夠確實保護競標活動應該具有的公平性。

到目前為止，要防範資訊的創造者將資訊外洩的方法並不多。除了仰賴創造者本身的自律之外，就只能限制其行動自由與通訊自由。大學聯招的命題者需要入闈，就是因為入闈者可以完全掌握考題資訊，因此只好暫時限制其通訊與行動上的自由，以維護考試的公平性。我們希望在不需要限制底價制定者的通訊自由之下，能夠讓一群底價制定者共同制定出一個大家都滿意的底價，而且沒有人能夠在開標前確切知道最後的底價。由於制定底價的時間必定早於開標時間，因此制定底價時也要防止底價的外洩。

要防止底價於開標前不外洩，首先需要考慮的是制定底價的人數。如果制定底價的人數在兩個以上，我們可以考慮讓每個底價制定者輸入他認為合理的底價範圍，然後在底價範圍可以保持隱密的情況下，求出所有制定者底價範圍的交集。在這個交集中的最小值將成為這群底價制定者所共同決定的底價。利用這種方法，每個底價制定者所知道的資訊只是底價的範圍，但是不知道確切的底價數字。

對上述群體制定底價的過程來說，對所有制定者所給定的底價範圍求取交集是關鍵。求取底價範圍的交集需要找出底價範圍中下限的最大值以及上限的最小值，也就是說，我們需要對所有上限與下限進行比價。根據我們對現有文獻的瀏覽，與比價最有關係的研究就是競標協定[1,3,4,6]。然而，競標協定的決標步驟雖然也需要求取所有競標者標價的最大值，但是並不需要讓競標單位在比價時不可以知道標價，所以不符合底價制定時底價範圍保持隱密的要求。基於這個理由，我們設計了一個祕密的比價協定，讓比價雙方能夠在可信賴的第三者的協助下得到比價的結果。更重要的是，除非與底價制定者共謀，否則可信賴的第三者也無法知道比價雙方的底價，這是現有競標協定所無法達成的重要特性。

三、結果與討論

在這一節中，我們將介紹一個祕密底價制定的新方法。這個方法讓制定雙方在比價時無法知道對方的價格，並且無法否認比價時所提出的價格。我們用 **Alice** 與 **Bob** 代表兩位底價制定者，**Trent** 代表

一位可信賴的第三者，協助檢驗來自雙方的底價資訊。為了讓底價制定者可以作出承諾，我們使用了兩個雜湊函數，h()及g()，並且用<m,n>代表一個具有n個元素的雜湊函數串(hash chain)，其第一個元素是m。詳細的比價步驟如下：

Alice隨機選擇一個數x_1，並且利用h()雜湊函數製造出一個雜湊函數串$<x_1,n>=<x_1,x_2,\ldots,x_n>$，其中$x_{i+1}=h(x_i)$，$1\le i \le n-1$。為了保證這個雜湊函數串不會變動，Alice必須公佈$g(x_1)$與$g(x_n)$。

Bob隨機選擇一個數m。由於這個數將是Bob隨後設定底價的重要工具，因此Bob必須公佈g(m)，以承諾m不會改變。

Alice選擇自己的價格a，然後挑出$<x_1,n>$雜湊函數串中的第a個元素x_a後，送給Trent。Trent必須保持x_a的隱密性，以防Bob得知Alice的價格。

接下來，Alice將整個$<x_1,n>$雜湊函數串傳給Bob。為了確保Alice沒有作弊，Bob可以針對所收到的雜湊函數串$<y_1,n>$進行下列檢查：

- $g(y_1)=g(x_1)$。這個檢查讓Bob肯定所收到的雜湊函數串的第一個元素符合Alice在第1步驟所作的保證。
- $g(y_n)=g(x_n)$。這個檢查讓Bob肯定所收到的雜湊函數串的最後一個元素符合Alice在第1步驟所作的保證。
- $h(y_{i+1})=h(y_i)$，$1\le i \le n-1$。這個檢查讓Bob確定所收到的$<y_1,n>$的確是一個植基於h()雜湊函數的雜湊函數串。

透過這三項檢查步驟，Bob已經可以確定所收到的數列與Alice所承諾的雜湊函數串是一樣的。接下來，Bob選定他的價格b，並且去掉$<y_1,n>$雜湊函數串中的前b個元素，得到一個較小的雜湊函數串$<y_{b+1},n-b>$。然後，Bob將第2步驟中所選擇的m放在$<y_{b+1},n-b>$之前，製作出一個數列$S=(m, y_{b+1}, y_{b+2},\ldots,y_n)$，最後交給Trent。

Trent在接到Bob所送來的數列$T=(T_1,T_2,\ldots,T_k)$之後，必須進行下列檢查動作：

$g(T_1)=g(m)$。這個檢查讓Bob必須使用第二步驟中所作的承諾來標示出自己的價格，而且由於只有Bob知道m，因此Bob無法否認數列的真確性。

$g(T_k)=g(x_n)$。這個檢查讓Trent相信Bob所傳來數列的最後一個元素符合Alice在第1步驟所作的保證。

$h(T_{i+1})=h(T_i)$，$2\le i \le k-1$。這個檢查加上(2)的效果就是要讓Trent確定所收到的數列T的確包含Alice所製作的雜湊函數串的後段部份。

在檢查無誤之後，Trent只要察看數列T有沒有包含x_a，就可以決定Alice與Bob的價格大小。如果數列T中包含x_a，表示Alice的價格較大，否則Alice的價格絕對不會大於Bob的價格。

當需要揭曉價格的時候，Trent向Alice或Bob詢問x_1的值。由於Bob在第5步驟中已經把x_n傳給Trent，所以Trent可以利用雜湊函數的特性算出n。直到這個時候，Trent才知道Alice與Bob的價格。

接下來，我們將針對上述協定進行公平性、隱密性、正確性與效率上的簡單分析。

(1)比價公平性

公平性的討論必須考慮兩個問題：1. 底價制定者比價時的價格是否與最後揭曉的價格相同；2. 有沒有可能事先得知他人的出價。由於Alice在第1步驟時就已經公佈$g(x_1)$與$g(x_n)$，因此她送給Trent的x_a代表著對於價格a的一種不可反悔的承諾。同樣地，由於雜湊函數串的長度已經固定，所以Bob也不可能臨時將新的元素加入雜湊函數串中增加價格。所以我們可以相信，底價制定者不可能在作出承諾之後否認價格。

至於要事先得知他人底價，對於Alice來說是不可能做到的，因為她是第一個出價者。Bob要知道Alice的x_a則必須買通Trent。為了避免這種買通情況的發生，我們可以稍微修改上述協定，讓Alice不需要直接向Trent送出x_a。她可以送出雜湊函數串中的任何一個比x_a大的元素x_d，並且算出x_d與x_a在雜湊函數串中的距離d-a，然後將d-a用g()雜湊函數作出承諾送給Trent。這樣的設計讓Bob頂多只能知道x_d，但是無法知道x_a與x_d的距離，因為有g()雜湊函數的保護。Alice可以刻意選擇很大的d，讓Bob得不到有效的資訊。

在這個修訂的協定中，Trent要先察看數列T有沒有包含x_d。如果沒有，由於$x_d>x_a$，因此表示Bob的價格一定比Alice的價格大。如果有，讓我們假設$T_j = x_d$。這時Trent必須要求Alice送出d-a，並比較d-a與j-1的大小。如果d-a比較大，則表示Bob的價格較大，否則Bob的價格頂多等於Alice的價格。

從這個修改後的協定來看，不論是Alice還是Bob都沒有辦法在出價之前就得知對方的價格，再加上出價雙方都無法修改承諾過的價格，因此這個修訂過的協定可以滿足公平性的要求。

(2)價格隱密性

Trent知道Alice所選擇的x_a。如果要推導出x_a位於雜湊函數串中的位置，Trent必須設法知道x_1，再利用雜湊函數的特性推出a。由於Alice不可能透露與自己價格息息相關的x_1，因此Trent必須與Bob共謀，以取得x_1。至於Bob，從Alice所傳來的雜湊函數串中根本不可能知道Alice選擇哪一個元素送給Trent，除非他從Trent得到x_a。

接下來討論Bob價格的隱密性。由於Trent不知道Alice所製作的雜湊函數串的元素數目，他沒有辦法推導Bob的價格。因此要知道Bob價格的唯一方法就是與Alice共謀，取得整個雜湊函數串的第一個元素x_1，以及最後一個元素x_n，才能算出整個雜

湊函數串的長度，推得 Bob 的價格。

因此，本協定中的任何一個角色，包括 Trent，都無法只憑藉自己所擁有的資訊推得其他底價制定者的價格；也就是說，除非有共謀的情況發生，Trent 無法獲得任何底價制定者的價格資訊。根據文獻[2]，我們所設計的 Trent 屬於半信賴的第三者(semi-trusted third party)，或稱為有條件被信賴的第三者(conditionally trusted third party)。為了讓 Trent 更受信賴，我們建議還可以利用祕密分享[5]的方式來保護 x_a，並且可以將 Trent 的功能設計成伺服器，並且利用存取控制機制加以保護。

(3)比價正確性

我們可以發現，Alice 與 Bob 表示價格的方式是不一樣的。Alice 利用雜湊函數串中的第 a 個位置來表示自己的價格 a，而 Bob 則是用他所去掉$<y_1,n>$雜湊函數串中的元素數目來代表價格 b。由於各種檢查步驟可以確保 Alice 與 Bob 共享同一個雜湊函數串，因此如果在 Bob 所去掉的元素中包括代表 Alice 價格的 x_a，意味著 Bob 的價格一定高於 Alice 的價格，否則 Bob 的價格頂多與 Alice 的一樣大。

到目前為止，本協定一直假設高價的底價制定者將會得到較多的報償，因此底價制定者會在能力許可的範圍下盡量拉抬自己的出價。當這個前提不成立的時候，也就是協定的目的是要比出較低價者的時候，第三節所介紹的協定將出現漏洞。因為 Alice 可以刻意送給 Trent 一個 z，$z \notin <x_1,n>$雜湊函數串。所以在比價階段的時候，Trent 無法在 Bob 送來的數列 T 中找到 z，使得 Alice 在不公平的情況之下得到優勢。也就是說，第 3 節所介紹的比價協定並不適用於低價者得到較多報償的應用場合。

為了解決這個問題，我們可以對協定作一些小小的修正。把協定第 1 步驟中的 Alice 公佈的 $g(x_n)$ 改成 x_n，將使 Trent 在第 3 步驟時就可以檢驗 x_a 是不是屬於雜湊函數串的成員。基於雜湊函數的特點，Trent 無法從 x_n 推導出 x_1，所以直接公佈 x_n 不會暴露雜湊函數串的長度，又可以讓 Trent 檢查 Alice 所送來的 x_n，增加本協定的比價正確性與比價公平性。

(4)效率

一般來說，雜湊函數的運算要比對稱式及非對稱式加密函數要來得快速很多。在 Nurmi 的方法中，底價制定者必須將整個數列進行非對稱加密函數的解密動作，而我們的方法則只需要產生一整個雜湊函數串，在效率上快速許多。

四、結論

底價制定是工程競標過程中一個保障工程品質的重要步驟。本計畫成果可以讓一群有權制定底價的人可以透過本方法共同決定一個祕密的底價，而且在特定時間之前，底價的確切數字不會外洩。雖然這與目前底價的制定流程不甚符合，但是我們認為，唯有引用新的密碼方法改革現有的競標習慣，才能切實杜絕競標單位於開標前外洩底價等不公平的惡習。所以對於競標者來說，參與競標活動的公平性將可以有效提高。

除了工程競標上的應用之外，本成果還可以用在祕密競標活動中的比價步驟。由於本計畫設計了一個可以保障比價結果正確性的比價協定，而且比價雙方無法在出價之前獲取對方的價格資訊，公平性因而可以獲得保障。本方法的主要運作是雜湊函數運算，比起對稱式及非對稱式密碼系統常用到的指數運算及模運算都要來得快，有助於發展高效率的競標系統。在價格的隱密性方面，本協定中的 Trent 屬於半信賴的第三者，配合存取控制機制與祕密分享等技術將可以加強保護比價雙方出價的隱密性。

在計畫成果自評部份，我們的研究內容與計畫完全相符，並達成預期的目標—設計一個公平且隱密的底價制定協定。我們相信不論在學術上或工程競標的實際應用上，本研究成果都深具潛力。

五、參考文獻

[1] M. K. Franklin and M. K. Reiter, The Design and Implementation of a Secure Auction Service, *IEEE Transactions on Software Engineering*, 22 (5) (1996), pp.302-312.

[2] M. K. Franklin and M. K. Reiter, Fair Exchange with a Semi-Trusted Third Party, *Proceedings of the 4th ACM conference on Computer and Communications Security*, 1997.

[3] H. Kikuchi, M. Hakavy, D. Tygar, Multi-Round Anonymous Auction Protocols, *IEICE Transactions on Information & Systems*, vol. E82-D, no. 4, April 1999.

[4] H. Nurmi, Cryptographic Protocols for Auctions and Bargaining, *Proceedings of Results and Trends in Theoretical Computer Science*, 1994, pp. 317-324.

[5] A. Shamir, How to Share a Secret, *Communication of the ACM*, 24 (11) (1979), pp.612-613.

[6] 陳俊良，黃景彰，「網際網路上安全的工程競標通訊協定」，第八屆中華民國資訊安全研討會論文集，1998，187-196 頁。

(本成果報告著作人：廖耕億，黃景彰)