行政院國家科學委員會專題研究計畫成果報告

應用密碼技術在網際網路上進行工程競標與商品拍賣

Applying Cryptography to Project Bidding and Commodity Auction over the Internet

計畫編號：NSC 87-2213-E-009-005-
執行期限：86 年 8 月 1 日至 87 年 7 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

網際網路與密碼技術的日趨成熟已經使得網際網路成為一個適合進行電子商務的環境。本計畫引申主持人過去應用密碼技術的研究經驗，設計了一個可以應用於網際網路上的工程競標機制。由於本計畫的設計參考了相關的競標法規，我們相信將可以成為政府單位日後設計招標系統的理論基礎。

關鍵詞：網際網路、密碼技術、工程競標

Abstract

Internet technology with cryptography has created an environment for electronic commerce. Based upon our past research on applied cryptography, this project establishes a secure and fair bidding mechanism over the Internet. Since accordance with current law is taken into consideration, we believe, our efforts can contribute to a bidding system that can be implemented in the future.

Keywords: Internet, Cryptography, Bidding

二、緣由與目的

由於網際網路(Internet)的開放性與普遍性，在網路上進行安全且有私密需求的群體行為時，通常需要仰賴密碼技術(Cryptography)產生可信賴的溝通管道。網路上的無記名投票與電子資料交換便是其中兩個相當熱門的例子。依據研究結果，在網路上從事這些群體行為，大多具有下列數個優點：一、促進無紙環境；二、縮減因地理因素導致的隔閡與不便；三、加速文件的傳遞。由此可知，結合網路與密碼技術已經可以建立一個安全、迅速而且無遠弗屆的溝通工具。

目前，電子商務的研究可以說是十分熱門，大部分的學者都將焦點放在電子付款機制上面。我們認為，電子付款機制適用於已有固定價格的買賣行為當中；對於價格必須經由議價或競價程序的商品而言，必須設計一套新的機制，才能在網際網路上進行這種較複雜的交易行為。工程競標便是其中一個十分常見的例子。

以工程競標的過程為例，由於投標人多半散居各地，投標文件必須仰賴掛號郵件[13]。如果招標過程（包含招標、投標、開標與決標）能夠電腦化及網路化，對於減低成本與提高效率將有很大助益；再加上密碼技術可提供安全保護並保持隱密，因此將可確保招標流程的公正性，提升招標作業的公信力。為了達成上述目標，本計畫應用密碼技術設計了一個在網際網路上進行的工程競標機制，使競價活動能夠移植於網際網路上進行。

三、結果與討論

為了建構一個安全而且公平的網際網路工程競標機制，本計畫參考了一些現有的密碼協定來達成各項安全性需求。我們將先介紹個別密碼協定的功能，然後再介紹本計畫所設計的競標機制。

(一)個別密碼協定

1. 匿名通訊：為了保障競標廠商的身分不會事先外洩，我們採用匿名化混亂器(Anonymous MIX)[1]與匿名帳號來達成匿名的功能。匿名化混亂器可以任意延遲在網路傳遞資料的傳送時間以及資料長度，使惡意第三者無法根據網路流量資訊來追蹤資訊的來源。當匿名帳號的提供者是可信賴的時候，匿名帳號可以讓第三者無法找出訊息傳送者的真實身分，使得身分隱私能夠得到更完善的保障。
2. 不可抵賴性(non-repudiation)[2,3,4]：所謂不可抵賴性，就是要讓競標廠商可以相信所投出的標單已經被真確地收到，也讓主辦單位握有競標廠商投標的證據。這在競標機制中是不可或缺的，否則將會導致競標雙方無法相互信賴。本計畫參考伺服器簽章[5]的原理，在競標廠商與主辦單位之間設計一個可信賴的第三者，這個可信賴的第三者協助標單收送雙方進行簽章動作，以及各自得到發送證明(NRO)與接收證明(NRR)。伺服器簽章的應用除了達成公平性的要求之外，由於標單收送雙方不須自行產生簽章，因此可以有效減少這兩個地方的計算負荷。
3. 領取標單的隱密性：競標廠商所領取的標單必須完全相同，避免主辦單位可以在決標前利用標單的差異性猜出廠商的身分。但是在決標之後，主辦單位必須能夠從標單得知競標廠商的身分，以便與得標者進行簽約等後續程序。為了滿足上述需求，本計畫利用日後可驗證身分的盲目簽章[6]。在這種盲目簽章的方法中，競標廠商事先向一個可信賴的第三者 TTP 申請身分憑證，並且用這個 TTP 的公開金鑰將身分憑證加密起來。加密後的身分憑證將隨著廠商自行製作的空白標單以及一些亂數送給主辦單位，由其抽樣檢驗(cut and choose)身分憑證確實無誤之後，將所有文件簽章後送回競標廠商。抽樣檢驗可以讓主辦單位無法記錄所有資訊，使得主辦單位無法將標單與發送者的身分加以關連；如果廠商故意放入錯誤的身分憑證，主辦單位將有相當大的機率可以檢驗出錯誤。由於身分憑證已經用可信賴第三者的公開金鑰加密過，主辦單位需要知道得標者身分時，必須得到此可信賴的第三者的協助。這種日後可驗證身分的盲目簽章的使用，使得本計畫可以達成標單領取時的身分保密、並且在決標時確定得標者身分。
4. 決標的公正性：主辦單位決標的公正性往往是整個競標機制的關鍵。為了避免主辦單位決標不公的疑慮，我們將決定得標者的決策點分散，減輕決標不公可能導致的風險。這樣的理念與密碼學之中的祕密分享協定相同：分派者將祕密切分成 n 等分，發給 n 個人；我們可以預定一個門檻值 k，只要其中 k 個人交出他所持有的祕密等分，整個祕密便可以重組回來。也就是說，只要 n 個人當中的 k 個人運作正常，即使其餘 n-k 個人都有問題，仍然不影響正常運作。

   在許多種祕密分享協定當中，本計畫採用的是眾人皆可檢驗的祕密分享(publicly verifiable secret sharing)[7]。我們在主辦單位內設計一個收文單位，負責收集競標廠商送來的加密標單，並在投標時間截止後分派給主辦單位內部的各個

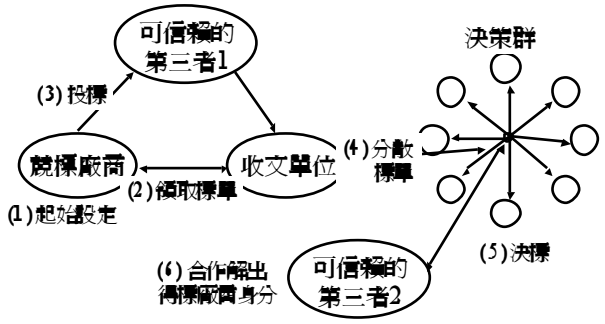
決策點。每個人都可以檢驗收文單位是否正確分發個別祕密等分。決標時，只要決策點數目達到門檻值,這些加密標單便可以重組回來。

5. 標單的隱密性：競標廠商所傳送的標單內容必須經過加密，以避免標價在決標前就外洩。由於我們在主辦單位內部設立了多個決策點，因此所有決策點必須都能夠把加過密的標單解密。本計畫依據 Agnew 等人所提出的方法[9]，將 Elgamal 非對稱加密法[10]加以變化之後，產生一個適用於群體的非對稱加密法，其加解密過程請參見下表。

公開金鑰：p: 質數，h: 小於 p 的整數 $y=\Pi y_i=h^{x_i} \bmod p$
私密金鑰：x_i:小於 p 的整數
加密：任選一個與 p-1 互質的亂數 k 要加密的訊息為 M $a=h^k \bmod p$ $b=y^k M \bmod p$
解密：$M=b/a^{\Sigma x_i} \bmod p$

(二)本計畫所設計的招標機制

接下來，我們先用下圖解說整個競標機制，接下來再分別介紹每個步驟。



1. 起始設定：競標廠商先取得一個匿名電子郵件帳號。我們設計讓可信賴的第三者 1 擔任簽章伺服器與匿名化混亂器，可信賴的第三者 2 則負責發給廠商的身分憑證。另外，主辦單位應事先公佈標的物資訊、空白標單、標號，以及一把用來加密標單的公開金鑰。
2. 領標單：競標廠商將利用日後可驗證身分的盲目簽章方法，將含有自行製作的空白標單、標號、以及用可信賴的第三者 2 的公開金鑰所加密的身分憑證等多份資訊送給招標單位的收文單位。收文單位經過隨機檢驗程序確定標單無誤之後，將標單簽章後送回。由於這個經由收文單位簽章過的標單含有可信賴第三者 2 的加密身分憑證，廠商可以在下一個階段用來投標，不須擔心身分事先被發現，也不會有主辦單位否認標單合法性的爭議發生。
3. 投標：在投標階段，競標廠商準備合法標單、投標金額、以及一個防止重複攻擊的時間章戳，用主辦單位公佈的公開金鑰加密之後，加上此次投標的標號，送給收文單位。這個傳送過程必須透過可信賴的第三者 1，競標廠商與收文單位會分別從這個可信賴第三者收到接收證明與發送證明。
4. 分散標單：收文單位檢驗競標廠商所發送的標單無誤之後，加上一個序號用來識別每張標單，然後把編號過的標單分散給各個決策點。每個決策者可以利用眾人皆可檢驗的祕密分享方法，檢查收文單位是否正確地將標單分發給每個決策者。
5. 決標：每個決策點都監控投標截止時間。一旦時間截止，決策點應向收文單位發出"停止接收標單"的命令。當收文單位收到命令的數目已經超過門檻值,便須停止接收標單。接下來，超過門檻值的決策點可以將廠商的標單加以還原。每個決策點應該提供自己的私密金鑰，以便組出一把代表主辦單位的私密金鑰。藉著這把私密金鑰，每個決策點都可以將重組後的每張標單解密，然後開始比較標價。當得標者產生後，標單中加過密的廠商身分

憑證必須送往可信賴的第三者 2，由這個可信賴第三者將憑證解密。因此，得標者身分到這個時候才揭曉。

(三)討論

1. 安全性分析：由於使用了許多現有的密碼協定，本計畫所設計的競標機制的安全性將植基於這些密碼協定的安全性。就我們目前所探討的文獻當中，還沒有發現記載有效破解這些密碼協定的方法。
2. 公平性分析：就主辦單位與競標廠商之間的公平性而言，由於我們引入了簽章伺服器來製作發送證明與簽收證明，主辦單位將很難否認曾經收到標單，競標廠商也無法抵賴曾經投標。這使得廠商與主辦單位處於一個公平的地位。

   就各個競標廠商之間的公平性來說，由於廠商的身分資訊是由可信賴第三者的公開金鑰所加密的身分憑證，其他人很難知道標單中的廠商身分。再加上我們採用了匿名化混亂器與匿名帳號來達成匿名的功能，因此惡意的第三者很難從網路上的流量分析來追蹤廠商身分。既然競標廠商的身分在決標之前保持完全隱密，主辦單位很難從標單中分辨廠商的身分，想要圖利特定廠商十分不容易。

四、計畫成果自評

本計畫已經按照說明書的說明，設計出一個適用於網際網路環境的工程競標機制。本研究的成果，曾經發表於 1998 年的資訊安全年會[11]，並且也成為國立交通大學資管所的碩士學位論文[12]。我們將持續改進，使本研究結果能夠提高社會的可接受性(social acceptance)[8]，作為將來進行系統發展的基礎。

五、參考文獻

[1] D. Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms," Communications of the ACM, vol. 24, n. 2, Feb 1983, pp. 84-88.

[2] ISO/IEC JTC1, Information Technology, SC.2nd ISO/IEC CD 13888-1 Information Technology-Security Techniques-Non-repudiation-Part 1: General Model. *ISO/IEC JTC 1/SC 27 N 1105*, May 1995.

[3] ISO/IEC JTC1, Information Technology, SC.2nd ISO/IEC CD 13888-2 Information Technology-Security Techniques-Non-repudiation-Part 2: Using Symmetric Encipherment Algorithms. *ISO/IEC JTC 1/SC 27 N 1106*, July 1995.

[4] ISO/IEC JTC1, Information Technology, SC.2nd ISO/IEC CD 13888-3 Information Technology-Security Techniques-Non-repudiation-Part 3: Using Asymmetric Techniques. *ISO/IEC JTC 1/SC 27 N 1107*, Sep 1995.

[5] N. Asokan and G. Tsudik and M. Waidner, "Server-Supported Signatures," *ESORICS'96*, pp. 131-143, 1996.

[6] M. Stadler and J.M. Pivereau and J. Camenisch, "Fair Blind Signatures," *Adv. In Cryptology-EUROCRYPT'95*, pp. 209-219, 1995.

[7] M. Stadler, "Publicly Verifiable Secret Sharing," *Adv. In Cryptology-EUROCRYPT'96*, pp. 190-199, 1996.

[8] J.J. Hwang, "A Conventional Approach to Secret Balloting in Computer Networks," *Computers & Security*, v. 15, n. 3, 1996, pp. 249-263.

[9] G.B. Agnew, R.C. Mullin, and S.A. Vanstone, "Improved Digital Signature Scheme Based on Descrete Exponentiation," *Electronics Letters*, vol. 26, n. 14, 1990, pp. 1024-1025.

[10] T. ElGamal, "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," *Adv. In Cryptology-CRYPTO'84,* pp. 10-18, 1983.

[11] 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。
[12] 陳俊良，「網際網路上的工程競標：應用密碼學理論建立一個安全且公平的商業機制」，國立交通大學資訊管理研究所，碩士論文，1998。
[13] 行政院公共工程委員會，*公共工程常用法規彙編*，民國八十五年七月