行政院國家科學委員會專題研究計畫　成果報告

群體授權予群體的門檻式代理簽章法之設計

計畫類別：個別型計畫
計畫編號：NSC91-2213-E-032-014-
執行期間：91 年 08 月 01 日至 92 年 07 月 31 日
執行單位：淡江大學資訊工程學系

計畫主持人：黃心嘉

計畫參與人員：詹定法　李韻華

報告類型：精簡報告

處理方式：本計畫可公開查詢

中　華　民　國 92 年 8 月 13 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

群體授權予群體的門檻式代理簽章法之設計

計畫類別：☑個別型計畫　□整合型計畫

計畫編號：NSC91-2213-Z-032-014

執行期間：91 年 8 月 1 日至 92 年 7 月 31 日

計畫主持人：黃心嘉　淡江大學資工系　副教授

計畫參與人員：詹定法　淡江大學資工系　研究生

李韻華　淡江大學資工系　研究生

本成果報告包括以下應繳交之附件：

□赴國外出差或研習心得報告一份

□赴大陸地區出差或研習心得報告一份

□出席國際學術會議心得報告及發表之論文各一份

□國際合作研究計畫國外研究報告書一份

執行單位：淡江大學資工系

中　華　民　國　九十二　年七 月三十一 日

行政院國家科學委員會專題研究計畫成果報告

群體授權予群體的門檻式代理簽章法之設計

The Design of Threshold Proxy Threshold Signature Schemes

計畫編號：NSC91-2213-Z-032-014

執行期限：91 年 8 月 1 日至 92 年 7 月 31 日

主持人：黃心嘉　淡江大學資工系　副教授

計畫參與人員：詹定法　淡江大學資工系 研究生

李韻華　淡江大學資工系 研究生

E-mail: sjhwang@mail.tku.edu.tw

一、中英文摘要

本計畫提出一套新的群體授權予群體的門檻式代理簽章法。在此新方法中，代理的授權必須獲得原始簽章群與代理簽章群的共同門檻式同意。此外同時提供指定代理簽章群的功能，並對原始簽章群與代理簽章群同時提供公平的保護。原始簽章群也可以指定代理簽章群。

關鍵詞： 門檻式代理式簽章、代理簽章、數位簽章。

Abstract

In this project, a new threshold proxy threshold signature scheme is proposed. In this scheme, the proxy authenticated is based on the threshold agreement of the original group and proxy group at the same time. Moreover, the scheme provides the fair protection both for the original group and proxy group. In this scheme, the proxy group is specified by the original group.

Keywords: threshold proxy signatures, proxy signature, digital signature.

二、緣由與目的

於 1996 年 Mambo 等日本學者[13, 14]提出了代理簽章的概念，隨後就有許多的代理簽章法[8, 10-15, 18-19,]與群體導向式代理簽章法 [3-7, 9, 16-20, 23, 24]被提出。門檻式代理簽章法的概念是一位原始簽章者允許授權予 m 位代理簽章者所組成的代理群，並且要求至少需要其中 c 個代理簽章者，才可以產生代理簽章。若代理簽章者不足 c 個人時，則不允許產生代理簽章。然而在現實生活中，存在由 n 位原始簽章者所組成的原始簽章群授權給由 m 位代理簽章者所組成的代理群的需求，並且要求至少需要原始簽章群中 t 個原始簽章者才可以授權代理群，至少需要其中 c 個代理簽章者，才可以產生代理簽章。在本報告中，我們將設計一個安全的群體授權予群體的門檻式代理簽章法，同時提供指定代理簽章群的功能，並對原始簽章群與代理簽章群提共公平的保護。

三、結果與討論

在本章節中，我們首先簡述研究成果，接著對該研究成果進行安全性分析。主要的研究結果如下所述。

[系統建置階段]

這個階段需由一公信的中心 T 建制公開的系統參數。p 與 q 為兩個大質數滿足 q|p-1，g 是 Z_q^* 中次序為 q 的元素，另外 h 為一公開的單向赫序函數。

對原始簽章群$\{U_1, U_2, \ldots, U_n\}$，每一個原始簽章者 U_i 有自己獨特的代號 ID_{ui} 與一個獨特的公開值 x_{ui}，T 為原始簽章群任意造一個 t-1 次方的秘密多項式 $f_o(x)= s_0+ a_1x+ a_2x^2+ \ldots+ a_{t-1}x^{t-1} \bmod q$，並公開的參數 $A_i=g^{a_i} \bmod p$ (i= 1, 2, …, t-1)，原始簽章群的秘密金匙為 $s_o \in Z_q^*$，原始簽章群的公開金匙為 $y_o=g^{s_o} \bmod p$。原始簽章者 U_i 的個別秘密金匙為 $f_o(x_{oi}) \bmod q$，個別公開金匙為 $y_{oi}= g^{f_o(x_{oi})} \bmod p$。

對代理簽章群$\{P_1, P_2, \ldots, P_m\}$，每一個代理簽章者 P_i 有自己獨特的代號 ID_{pi} 與一個獨特的公開值 x_{pi}，T 為代理簽章群任意造一個 c-1 次方的秘密多項式 $f_p(x)= s_p+ b_1x+ b_2x^2+ \ldots+ b_{c-1}x^{c-1} \bmod q$，並公開的參數 $B_j=g^{b_j} \bmod p$ (i= 1, 2, …, c-1)，代理簽章群的秘密金匙為 $s_p \in Z_q^*$，代理簽章群的公開金匙為 $y_p=g^{s_p} \bmod p$。代理簽章者 P_i 的個別秘密金匙為 $f_p(x_{pi}) \bmod q$，個別公開金匙為 $y_{pi}= g^{f_p(x_{pi})} \bmod p$。

符號 w 代表代理的授權書，記錄著代理的細節，例如：原始簽章者及代理簽章者的公開公匙，代理期間等資訊。內容至少包含所有原始簽章者的 ID_{ui}'s 與個別公開金匙 y_{oi}'s，所有代理簽章者的 ID_{pj}'s 與個別公開金匙 y_{pj}'s ，原始簽章群的公開金匙 y_o 與代理簽章群的公開金匙 y_p。

[授權階段]

在這個階段中，原始簽章群$\{U_1, U_2, \ldots, U_n\}$授權代理簽章群$\{P_1, P_2, \ldots, P_m\}$為代理群。在不失一般性下，假設 $U_1, U_2, \ldots, U_t$ 與 $P_1, P_2, \ldots, P_c$ 共同產生授權憑證，授權過程如下所示：

步驟一：每一個原始簽章者 U_i 選擇一個亂數值 $k_{oi} \in Z_q^*$，計算 $K_{oi}= g^{k_{oi}} \bmod p$，廣播 K_{oi} 給一位事先指定的整合者。同時每一個代理簽章者 P_i 也選擇一個亂數值 $k_{pi} \in Z_q^*$，計算 $K_{pi}= g^{k_{pi}} \bmod p$，廣播 K_{pi} 給整合者。

步驟二：所有人(含整合者)計算 $K= \prod_{i=1}^{t} K_{oi} \prod_{j=1}^{c} K_{pj} \bmod p$。

步驟三：每一個原始簽章者 U_i 計算 $v_{oi}= f_o(x_{oi})L_{si}y_oh(w) + k_{oi}K \bmod q$，並將 v_{oi} 送給整合者，此處 $L_{si}= \prod_{j=1, j\neq i}^{t} \frac{-x_{oi}}{x_{oj}-x_{oi}} \bmod q$。每一個代理簽章者 P_i 計算 $v_{pj}= f_p(x_{pj})L_{vj}y_ph(w) + k_{pj}K \bmod q$，並將 v_{pj} 送給整合者，此處 $L_{pj}= \prod_{i=1, i\neq j}^{c} \frac{-x_{pj}}{x_{pi}-x_{pj}} \bmod q$。

步驟四：整合者利用 $g^{v_{oi}} \equiv y_{oi}^{L_{si} y_o h(w)} K_{oi}^{K} \pmod p$檢驗所有 v_{oi} 的正確性，利用 $g^{v_{pj}} \equiv y_{pj}^{L_{vj} y_p h(w)} K_{pj}^{K} \pmod p$檢驗所有 v_{pj} 的正確性。

步驟五：若所有 v_{oi} 與 v_{pj} 皆正確，整合者計算 $V=\sum_{i=1}^{t} v_{oi} + \sum_{j=1}^{c} v_{pj} \bmod q$，廣播(K, V)給原始簽章群與代理簽章群的所有成員。所有成員利用 $g^V \equiv K^K (y_o^{y_o} y_p^{y_p})^{h(w)} \pmod p$檢驗(K, V)的正確性。

最終代理憑證為(K, V)。

[代理簽章的產生階段]

不失一般性下，假設代理簽章者 $P_1, P_2, \ldots, P_c$ 欲代理原始簽章群簽署一個文件 M ，並假設 P_1 為召集人，其代理簽章的產生及驗證步驟如下所示：

步驟七：每一個代理簽章者 P_j 選擇一個亂數 $d_{pj} \in Z_q^*$。

步驟七：每一個代理簽章者 P_j 計算 $D_{pj}= g^{d_{pj}} \bmod p$ 並且廣播 D_{pj} 給其他 c-1 個人。

步驟八：每一個 P_j 計算 $D=\prod_{j=1}^{c} D_{pj} \bmod p$ 與 $s_{pj}= V d_{pj} D + f_p(x_{pj}) L_{vj} h(M) y_p \bmod q$。

步驟九：每一個 P_j 送(D_{pj}, s_{pj})給整合者。召集人 P_1 送(w, (K, V), M) 給整合者。

步驟十：整合者用 $g^V \equiv K^K (y_o^{y_o} y_p^{y_p})^{h(w)} \pmod p$檢驗(K, V)的正確性。

步驟十一：整合者計算 $D=\prod_{j=1}^{c} D_{pj} \bmod p$，用 $g^{s_{pj}} \equiv (D_{pj})^{DV} (y_{pj})^{L_{vj} h(M) y_p} \pmod p$ 檢驗所有(D_{pj}, s_{pj})的正確性。如果都正確，計算 $S=\sum_{j=1}^{c} s_{pj} \bmod q$。最終群體授權予群體的門檻式代理簽章為(w, (K, V), M, (D, S))。

[代理簽章的確認階段]

步驟十二：驗證者利用 $g^V \equiv K^K (y_o^{y_o} y_p^{y_p})^{h(w)} \pmod p$檢驗(K, V)的正確性。

步驟十三：驗證者利用 $g^S \equiv D^{DV} y_p^{y_p h(M)} \pmod p$ 檢驗(D, S)的正確性。

底下進行安全分析。這個系統是架構在植基離散對數難題的門檻式簽章法上，攻擊者欲求得系統中的秘密金匙或亂數值都必然面臨求離散對數的難題，同樣的，系統中多項式的係數也是受離散對數難題的保護。由原始簽章者所簽署的授權憑證(w, V)基本上是門檻式簽章，是無法被偽造的，而系統中的授權書指明了代理簽章群，所以代理者是無法轉移授權給其他人。

在這個系統中，利用了 Lagrange 插入多項式，實現了原始(或代理)簽章群 n(或 m)個人中必須要有 t(或 c)個或以上的原始(或代理)簽章者才能完成授權(或簽署文件)的要求。另一方面，由於系統中不只使用了代理金匙，更利用了代理簽章群的金匙，所以原始簽章群無法任意偽造代理簽章。由上所述，我們可知此系統同時提供對原始簽章者與代理簽章者的保護。

四、計畫成果自評

在計劃中，我們提出了一個安全的群體授權予群體的門檻式代理簽章法，此簽章法可提供指定代理簽章者的功能，而安全性方面主要架構在著名的離散對數問題上，換言之，對任何一位攻擊者而言，在進行攻擊時，需事先解決求解離散對數的問題。另一方面，本方法也同時提供了對原始簽章者及代理簽章者的保護，因此本計畫的結果，符合了當時計畫書所提的目標與要求。

五、參考文獻

[1] Harn, L., "Group-oriented (t, n) threshold digital signature scheme and digital multisignature," *IEE Proceedings: Computers and Digital Techniques*, Vol. 141, No. 5, pp. 307-313, 1994.

[2] Harn, L., "Digital multisignature with distinguished signing authorities," *ELECTRONICS LETTERS*, Vol. 35, No. 4, pp.294-295, 1999.

[3] Hsu, Chien-Lung, Wu, Tzong-Sun, and Wu, Tzong-Chen, "New nonrepudiable threshold proxy signature scheme with known signers," *The Journal of Systems and Software*, Vol. 58, pp. 119-124, 2001.

[4] Hwang, Min-Shiang, Lin, Iuon-Chang, and LU, Eric Jui-Lin, "A secure nonrepudiable threshold proxy signature scheme with known signers," *INFORMATICA*, Vol. 11, No. 2, pp. 137-144, 2000.

[5] Hwang, S. J. and Chen, Chiu-Chin, "A New Proxy Multi-Signature Scheme," *International Workshop on Cryptology and Network Security*, Taipei, Taiwan, R.O.C., Sep., 2001, pp. 199-204.

[6] Hwang, S. J. and Chen, Chiu-Chin, "A New Multi-Proxy Multi-Signature Scheme," *National Computer Symposium*, Taipei, Taiwan, R.O.C., Dec., 2001, pp. F019-F026.

[7] Hwang, S. J. and Chen, Chiu-Chin, "Cryptanalysis of nonrepudiable threshold proxy signatures with known signers," *2002 Information Security Conference*, Taichung, Taiwan, R.O.C., May 16-17, 2002, pp. 243-246, also in *Journal of Informatica*, Vol. 53, No. 2, Nov. 2002, pp. 131-134.

[8] Hwang, S.-J. and Shi, Chi-Hwai, "The Specifiable Proxy Signature," *National Computer symposium 1999*, Taipei, Taiwan, R.O.C., Dec. 1999, pp. 190-197.

[9] Hwang, S. J. and Shi, Chi-Hwai, "A Simple Multi-Proxy Signature Scheme," *Proceedings of the Tenth National Conference on Information Security*, Hualien, Taiwan, R.O.C., 2000, pp. 134-138.

[10] Hwang, S. J. and Shi, Chi-Hwai, "A Proxy Signature Scheme without Using One-Way Hash Functions," *2000 International Computer Symposium*, Chiayi, Taiwan, R.O.C., Dec. 2000, pp. 60-64.

[11] Kim, S., Park, S., and Won, D., "Proxy Signatures," *ICICS '97, Lecture Notes in Computer Science*, Vol. 1334, Springer, Berlin, 1997, pp. 223-232.

[12] Lee, Narn-Yih, Hwang, Tzonelih, and Wang, Chih Hung, "On Zhang's Nonrepudiable Proxy Signature Schemes," *Third Australasian Conference, ACISP '98*, 1998, pp. 415-422.

[13] MAMBO, Masahiro, USUDA, Keisuke, and OKAMOTO, Eiji, "Proxy Signatures: Delegation of the Power to Sign Message," *IEICE. Transaction Fundamentals*, Vol. E 79-A, no. 9, pp.1338-1354, Sept. 1996.

[14] MAMBO, Masahiro, USUDA, Keisuke, and OKAMOTO, Eiji, "Proxy Signatures for Delegation Signing Operation," *Proceedings of third ACM Conference on Computer and Communications Security,* New Delhi, Mar. 1996, pp. 48-57.

[15] Kim, Seungjoo, Park, Sangjoon, and Won Dongho, "Proxy Signatures, Revisited," *Information and Communications Security*, Beijing, China, November 1997, pp. 223-232.

[16] Sun, Hung-Min, "An Efficient Nonrepudiable Threshold Proxy Signature Scheme with Known Signers," *Computer Communications,* Vol. 22, pp. 717-722, 1999.

[17] Sun, Hung-Min, "On Proxy (Multi-) Signature Schemes," *2000 International Computer Symposium*, Chiayi, Taiwan, R.O.C., Dec. 6-8, 2000, pp. 65-72.

[18] Sun, Hung-Min and Chen, Biing-Jang, "Time-Stamp Proxy Signatures with Traceable Receivers," *Proceedings of the Ninth National Conference on Information Security,* Taiwan, 1999, pp. 247-253.

[19] Sun, Hung-Min, and Hsieh, Bin-Tsan, "Remark on Two Nonrepudiable Proxy Signature Schemes," *Proceedings of the Ninth National Conference on Information Security*, Taiwan, 1999, pp. 241-246.

[20] Sun, Hung-Min, Lee, N-Y and Hwang T., "Threshold Proxy Signatures," *IEE Proc.-Computers and Digital Techniques*, Vol. 146, No. 5, pp. 259-263, 1999.

[21] Yen, Sung-Ming, Hung, Chung-Pei, and Lee, Yi-Yuan, "Remarks on Some Proxy Signature Schemes", *2000 International Computer Symposium*, Chiayi, Taiwan, R.O.C., Dec. 6-8, 2000, pp. 54-59.

[22] Yeun, C.Y., Mitchell, C. J., and Ng, S. L., "Comment Signature scheme based on discrete logarithm without using one-way hash-function," *ELECTRONICS LETTERS*, Vol. 34, No. 24, pp. 2329-2330, 1998.

[23] Yi, L. Bai, G., and Xiao, G., "Proxy multi-signature scheme: A new type of proxy signature scheme," *Electronics Letters*, Vol. 36, No. 6, pp.527-528, 2000.

[24] Zhang, K., "Threshold proxy signature schemes," 1997 Information Security Workshop, Japan, September 1997, pp. 191-197.