行政院國家科學委員會補助專題研究計畫成果報告

※※※※※※※※※※※※※※※※※※※※※※※※※※※※
※ ※
※ **代理簽章法群體導向化與驗證加密化之設計研究(2/2)** ※
※ ※
※※※※※※※※※※※※※※※※※※※※※※※※※※※※

計畫類別：☑個別型計畫　□整合型計畫

計畫編號：NSC90-2213-E-032-025

執行期間：90 年 8 月 1 日至 91 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：　黃鈺惠　朝陽科技大學資管系　研究生

陳秋錦　朝陽科技大學資管系　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　九十一　年　六　月　七　日

行政院國家科學委員會專題研究計畫成果報告

代理簽章法群體導向化與驗證加密化之設計研究(2/2)

The Design of Group-Oriented Proxy Signature Schemes and
Proxy Authenticated Encryption Schemes

計畫編號：NSC90-2213-E-032-025
執行期限：90 年 8 月 1 日至 91 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：黃鈺惠 朝陽科技大學資管系 研究生
陳秋錦 朝陽科技大學資管系 研究生
Eamil: sjhwang@mail.cyut.edu.tw

一、中英文摘要

在本報告中，我們充分利用驗證加密式的精神，設計一種的新的代理簽章法，此方法具備了代理簽章可驗證的基本特性，同時加密隱藏了代理簽章者的身份。雖然代理簽章者是匿名的，但是原始簽章者還是無法偽造代理簽章，而事後可以確認真正代理簽章者的身分。

關鍵詞：驗證加密式代理簽章、代理簽章、數位簽章。

Abstract

Utilizing the authenticated encryption function, a new type of proxy signature scheme is proposed in this project: Adaptable proxy signature scheme. In this new scheme, the proxy signer is anonymous but the original signer still cannot forge proxy signatures. Finally, the actual proxy signer can be identified.

Keywords: Proxy signature, authenticated encryption, digital signature.

二、緣由與目的

在數位化時代中，數位簽章代替了原本手寫簽章的需求，數位簽章具有了防止偽造及防止否認的特性，但數位簽章無法提供代理的需求。在 1996 年，Mambo 等學者[3, 4]提出了代理簽章的概念，原始簽章者可以授權予代理簽章者，而代理簽章者為執行代理的功能所簽署的簽章，稱之為代理簽章，自 Mambo 等學者提出後，許多的代理簽章法陸陸續續被提出[1-2, 5-11, 13-17]，但是所提出方法中，如果代理簽章者是匿名的，就無法防止原始簽章者偽造代理簽章。在本報告中，我們充分利用驗證加密式的精神，設計一種的新的代理簽章法，此方法具備了代理簽章可驗證的基本特性，同時加密隱藏了代理簽章者的身份，故在驗證代理簽章的同時，是無法得知代理簽章者的身份。在本方法中，也提供確認代理簽章者的身份的方法，另一方面，方法中也提供了對原始簽章者與代理簽章公平的保護。

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]

這個階段需公開一些系統參數，p 與 q 是兩大質數滿足 q|p-1，g 是 Z_q^* 的次序為 q 的生成子，另外 h 為一公開的單向赫序函數。原始簽章者 A 的秘密金匙為 $x_A \in Z_q^*$，公開金匙為 $y_A = g^{x_A} \bmod p$。代理簽章者 B 的秘密金匙為 $x_B \in Z_q^*$，及公開公匙 $y_B = g^{x_B} \bmod p$。

[授權階段]

在這個階段中，原始簽章者 A 授權代理簽章者 B 為代理人，授權過程如下所示：

步驟一：原始簽章者 A 選擇一個亂數值 $k \in Z_q^*$ 符合 gcd(k, q)=1，計算 $DH \equiv (y_B)^k \pmod$

p)及 $r=g^{-k} DH \pmod p$，並且計算 s 滿足

$$s \equiv k - r x_A h(m_w) \pmod q \quad (1)$$

，此處 m_w 是指代理授權書，其中記錄著代理的細節，例如：原始簽章者的公開公匙，代理期間等資訊。原始簽章者並私下記錄代理簽章者的資訊(ID_B, r, s, m_w)。

步驟二：原始簽章者 A 將（r, s, m_w）送給代理簽章者 B。

步驟三：代理簽者 B 收到後，利用 $g^s y_A^{rh(m_w)} r \equiv (g^s y_A^{rh(m_w)})^{x_B} \pmod p$驗證（r, s, m_w）的正確性。

步驟四：當步驟三的驗證式子正確後，代理簽章者 B 計算$\alpha \equiv g^s y_A^{rh(m_w)} \pmod p$，並儲存(r, s, m_w, α)。

[代理簽章的產生及驗證階段]

假設代理簽章者 B 欲代理原始簽章者 A 簽署一個文件 m 時，代理簽章的產生及驗證步驟如下所示：

步驟一：選擇一個亂數 $t \in Z^*_q$，計算 $T= \alpha^t \bmod p$ 並且從下列等式中求出 U。

$$h(m\|r\|s)= Tx_B+tU \pmod q \quad (2)$$

步驟二：代理簽章者傳送代理簽章((m_w, r, s), (m, T, U))給驗證者。

步驟三：驗證者驗證代理簽章時，首先計算$\alpha \equiv g^s y_A^{rh(m_w)} \pmod p$及 $DH \equiv \alpha^r \pmod p$。接著利用$\alpha^{h(m\|r\|s)} \equiv T^U DH^T \pmod p$驗證代理簽章的正確性。

[確認代理簽者的身份]

當需確認代理簽章身分時，原始簽章者 A 可以藉由記錄(ID_B, r, s, m_w)，找出代理簽章是那一位代理簽章者所簽署，再透過公正第三者進行下列步驟以確認代理簽章者的身份。在不失一般性的情況下，假定該代理者為代理簽章者 B。原始簽章者 A 傳送(m_w, r, s)予公正第三者，並告知代理簽章者 B 的身份。

步驟一：公正第三者計算$\alpha \equiv g^s y_A^{rh(m_w)} \pmod p$及 $DH \equiv \alpha^r \pmod p$。

步驟二：公正第三者選擇兩個亂數值 $e_1 \in Z^*_q$, $e_2 \in Z^*_q$，計算 $c = DH^{e1} y_B^{e2}$ 並傳送 c 值給 B。

步驟三：B 計算 $d=c^{x_B^{-1} \pmod q} \pmod p$傳送 d 值給公正第三者。

步驟四：公正第三者驗證 d 值是否等於 $\alpha^{e_1} g^{e_2} \pmod p$，如果相等，則證明代理簽章者為 B；如果不相等，公正第三者再選擇亂數值 $f_1 \in Z^*_q$, $f_2 \in Z^*_q$，計算 $C = DH^{f1} y_B^{f2}$ 並傳送 C 值給 B。

步驟五：B 計算 $D= C^{x_B^{-1} \pmod q} \pmod p$並傳送給公正第三者。

步驟六：公正第三者驗證 D 值是否等於 $\alpha^{f_1} g^{f_2} \pmod p$，如果不相等，則公正第三者驗證$(dg^{-e_2})^{f_1} \equiv (\mathbf{D} g^{-f_2})^{e_1} \pmod p$，如果相等，則證明代理簽章者不為 B。

底下進行安全分析。在新方法中，驗證者無法得知真正簽署代理簽章者的身份，因為 Nyberg 和 Ruppel 的論文[12]指出要從 DH 中得知代理簽章者的身份是不可行的。另外，雖然代理簽章者所使用的生成子為α，但不會因此而降低了系統的安全性，因為 gcd(k, q)=1，並且$\alpha = g^k \bmod p$，所以生成子α的次序仍為 q，不會降低了系統的安全性。我們的方法主要是架構在離散對數的困難上，由等式(1) 中，攻擊者無法得知原始簽章者的秘密金匙 x_A，在等式(2)中，欲得知代理簽章者的秘密金匙 x_B 同樣也是不可行的。在新方法中，提供了對原始簽章者與代理簽章者的保護，因為在簽署代理簽章時，由於系統中不只使用了代理金匙，更利用了代理簽章者的秘密金匙，所以原始簽章者無法任意偽造代理簽章。

四、計畫成果自評

在第二年度的計劃中，我們提出了一個安全而有效的驗證加密式代理簽章法，此簽章法可提供不指明代理簽章者的功能，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。因此本計畫第二年度的結果，符合了當時計畫書所提的目標與要求。

五、參考文獻

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

[2] 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.

[3] 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, Sept. 1996, pp.1338-1354.

[4] 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.

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

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] Hwang, S. J. and Chen, Chiu-Chin: "Cryptanalysis of nonrepudiable threshold proxy signatures with known signers," Information Security Conference 2001, Taichung, Taiwan, R.O.C. May, 2002.

[12] Nyberg, K., and Rueppei, R.A.: "Message recovery for signature schemes on the discrete logarithm," Pre-proceeding of Eurocrypt'94, Perugia, Italy, 9-12, May 1994, pp. 175-190.

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

[14] 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.

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

[16] 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.

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