增強型的群體導向數位簽章系統
Improved Group-Oriented Digital Signature Scheme

陳正鎔

國防管理學院資訊管理學系
中和市民安街 150 號
jonathan@rs590.ndmc.edu.tw

余平

國防管理學院資訊管理學系
中和市民安街 150 號
ping@rs590.ndmc.edu.tw

摘要

本文提出一個基於離散對數的增強型群體導向數位簽章系統，主要基於 Desmedt 與 Framkel 利用 ElGamal 加解密方法於群組導向之解密，但並無就群組導向數位簽問題予以探討，所以我們提出一種增強型的作法，即不須藉助廣播通道及秘書的協助即可完成群組導向數位簽章，以減少群體導向數位簽章系統的建置成本。
關鍵字：群體導向數位簽章、密碼系統、離散對數

Abstract

A improved group_oriented digital signature scheme is proposed in this paper. Because although Desmedt and Frankel apply ElGamal's cryptosystem, they fail to discuss the issue of group_oriented digital signature. we propose a method in which broadcast channel and clerk are not needed.
Key words: group_oriented digital signature, cryptosystem, discrete logarithm

一、前言

1976 年 Diffie 與 Hellman[6]提出一個公開金匙分配系統(Public Key Distribution System)讓未曾謀面的兩個使用者，可以透過公眾通道，以獲得只有他們兩個人才知道共同金匙，以分享彼此間的秘密通訊。此機密分享的觀念，在 1987 年 Desmedt[4]首先提出一個群體導向的密碼系統(Group_Oriented Cryptosystem)且陸續與 Frankel[5]提出一種依據(t,n)門檻方法分配金匙及依據 ElGAmal[7]加密方法來完成群體導向加密系統的策略。而其他學者[2,3,8,9]亦以此研究爲基礎陸續發表相關文獻。在群體導向密碼系統架構中，群體的主秘密金匙(master private key)，需由內部所規範的特定人數將所持有的秘密金匙(private key or shadow)予以結合成主秘密金匙方能使用。而對於如何避免在結合過程中的欺騙行爲，Brickell & Strinson[1]以及 Tompa & well[13]亦發表許多相關研究。

雖然 Desmedt 與 Frankel[5]將 ElGamal[7]所提出的解密方法運用於群體導向的解密方法，而達到解密的目的。但如何將此方法運用於群體導向數位簽章的問題上，上述學者並無進一步的討論。所謂群體導向數位簽章即指群體中的成員們依事先定義的規則，製作代表此群體的數位簽章，然後將簽章傳送給驗證者加以驗證，有鑑於企業中網路快速發展如 INTRANT，將群體決策藉由電腦網路來時現實有其需求及必要性，針對此點，Harn[9]反覆利用 ElGamal 零知識(zero knowledge)之特性，而達到群體式導向數位簽章的效果，但其系統必須藉由廣播通道(broadcast channel)的設備及秘書(clerk)的協助方能得以實現。

鑑於運用廣播通道的方式將增加網路軟硬體設備建置成本，且在組成群體導向數位簽章過程中每位參與者至少需使用廣播通道一次，將使訊息傳遞過於複雜及頻繁，再加上秘書的採用，均使系統負荷及成本增加。而其後在 Chen 與 Yu[10]所提出論文中僅就如何由 Harn 系統中偵測及阻擋欺騙者的方法予以討論，並無增強其系統，所以本論文提出一種不需藉由廣播通道及秘書，即能達到群體導向數位簽章功能的增強作法，以克服上述缺點。本論文架構如下，第一部份爲前言、第二部份爲我們所提出作法，第三部份爲分析與討論，最後一部份爲結論。

二、我們的作法

假定某一組織有 n 個人，其中需有 w 個人以上方能代表其組織對外傳遞組織訊息，此爲門檻策略(threshold scheme)，系統中心首先選定一個大質數 p，此 p 值具有(p-1)的因數分解存在一個大質數 q 的特性(a prime divisor of p-1)，再選取一數 h 其限制爲 1<h<p，以下式得出 g。

$$g \equiv h^{\frac{p-1}{q}} \pmod{p} \qquad (1)$$

然後選取一個一元(c-1)多項式 f 如下式

$$f(x) \equiv \sum_{i=0}^{c} a_{i-1} x^{i-1} (\mathrm{mod}\, q) \quad (2)$$

其中 $0 \neq a_{i-1} (\mathrm{mod}\, q)$

系統中心以 a_0 爲該組織之主秘密金匙(master private key)，並以其製作主公開金匙(master public key)如下式之 Y

$$Y \equiv g^{a_0} (\mathrm{mod}\, p) \quad (3)$$

組織內部成員 u_i，並假定其身份識別碼爲 $UID_i, 1 \le i \le n$，系統中心再製作其私人秘密金匙 z_i 如下式

$$z_i \equiv f(UID_i) (\mathrm{mod}\, q) \quad (4)$$

今假設組織內有某 w 個人($1 \leqq w \leqq n$)，分別爲 $u_1, u_2, \ldots, u_w$，將以該組織名義，共同對訊息 m 加上群體簽章後傳遞給接收者 u_j，其演算法如下：

步驟一：使用者 u_i 任意選取四個不相同的數 $\varphi_{1,t}, (1 \le t \le 4)$，計算下列式子

$$P_{1,t} \equiv \beta_{1,t} (\mathrm{mod}\, pq) \equiv g^{\varphi_{1,t}} (\mathrm{mod}\, pq) \quad (5)$$

$$Q_{1,1} \equiv Q_{1,1} (\mathrm{mod}\, q) \equiv P_{1,1} P_{1,2} z_1 \left(\prod_{k=1, k\neq 1}^{w} \frac{-UID_k}{UID_1 - UID_k} \right) m - Q_{1,1} Q_{1,2} (\varphi_{1,1} + \varphi_{1,2}) (\mathrm{mod}\, q) \quad (6)$$

$$Q_{1,2} \equiv Q'_{1,2} (\mathrm{mod}\, q) \equiv P_{1,1} \varphi_{1,3} - P_{1,1} \varphi_{1,1} (\mathrm{mod}\, q) \quad (7)$$

$$Q_{1,3} \equiv Q'_{1,3} (\mathrm{mod}\, q) \equiv P_{1,2} \varphi_{1,4} - P_{1,2} \varphi_{1,2} (\mathrm{mod}\, q) \quad (8)$$

$$Q_{1,4} \equiv \varphi_{1,3} - \varphi_{1,4} (\mathrm{mod}\, q) \quad (9)$$

然後將 $(P_{1,1}, P_{1,2}, P_{1,3}, P_{1,4}, Q_{1,1}, Q_{1,2}, Q_{1,3}, Q_{1,4}, m)$ 資料傳送給使用者 u_2。

步驟二：使用者 $u_\sigma (2 \le \sigma \le w)$ 任意選取四個不相同的數 $\varphi_{\sigma,t} (1 \le t \le 4)$ 計算下列式子：

$$\beta_{\sigma,t} \equiv g^{\varphi_{\sigma,t}} (\mathrm{mod}\, pq) \quad (10)$$

$$P_{\sigma,t} \equiv \beta_{\sigma,t} P_{\sigma-1,t} (\mathrm{mod}\, pq) \quad (11)$$

$$Q'_{\sigma,1} \equiv \beta_{\sigma,1} \beta_{\sigma,2} z_\sigma \left(\prod_{k=1, k\neq \sigma}^{w} \frac{-UID_k}{UID_1 - UID_k} \right) m - \beta_{\sigma,1} \beta_{\sigma,2} (\varphi_{\sigma,1} + \varphi_{\sigma,2}) (\mathrm{mod}\, q) \quad (12)$$

$$Q'_{\sigma,2} \equiv \beta_{\sigma,1} \varphi_{\sigma,3} - \beta_{\sigma,1} \varphi_{\sigma,1} (\mathrm{mod}\, q) \quad (13)$$

$$Q'_{\sigma,3} \equiv \beta_{\sigma,2} \varphi_{\sigma,4} - \beta_{\sigma,2} \varphi_{\sigma,2} (\mathrm{mod}\, q) \quad (14)$$

$$Q_{\sigma,1} \equiv \beta_{\sigma,1} \beta_{\sigma,2} Q_{\sigma-1,3} + P_{\sigma-1,1} P_{\sigma-1,2} Q'_{\sigma,1} (\mathrm{mod}\, q) \quad (15)$$

$$Q_{\sigma,2} \equiv \beta_{\sigma,1} Q_{\sigma-1,2} + P_{\sigma-1,1} Q'_{\sigma,2} (\mathrm{mod}\, q) \quad (16)$$

$$Q_{\sigma,3} \equiv \beta_{\sigma,2} Q_{\sigma-1,3} + P_{\sigma-1,2} Q'_{\sigma,3} (\mathrm{mod}\, q) \quad (17)$$

$$Q_{\sigma,4} \equiv \varphi_{\sigma,3} - \varphi_{\sigma,4} (\mathrm{mod}\, q) \quad (18)$$

步驟三：如果 $\sigma = w$，則

(1) $P_t \leftarrow P_{\sigma,t}, 1 \le t \le 4$ (19)

(2) $Q_t \leftarrow Q_{\sigma,t}, 1 \le t \le 4$ (20)

(3)將資料 $(P_1, P_2, P_3, P_4, Q_1, Q_2, Q_3, Q_4, m)$ 傳送給接收者 u_j

(4)進行步驟四

否則

(1)將資料 $(P_{\sigma,1}, P_{\sigma,2}, P_{\sigma,3}, P_{\sigma,4}, Q_{\sigma,1}, Q_{\sigma,2}, Q_{\sigma,3}, Q_{\sigma,4}, m)$ 傳送給使用者 $u_{\sigma+1}$

(2) $\sigma \leftarrow \sigma + 1$ (21)

(3)重複步驟二

步驟四：接收者 u_j 驗證下列式子

$$(P_1 P_2)^{P_1 P_2} g^{Q_1} \stackrel{?}{\equiv} Y^{P_1 P_2 m} (\mathrm{mod}\, p) \quad (22)$$

$$P_1^{P_1} g^{Q_2} \stackrel{?}{\equiv} P_3^{P_1} (\mathrm{mod}\, p) \quad (23)$$

$$P_2^{P_2} g^{Q_3} \stackrel{?}{\equiv} P_4^{P_2} (\mathrm{mod}\, p) \quad (24)$$

$$g^{Q_4} \stackrel{?}{\equiv} P_3 P_4 (\mathrm{mod}\, p) \quad (25)$$

如果上述四個式子皆同時成立，表示所接收訊息 m 具有該組織的數位簽章，如不成立則表示有問題。

三、分析與討論

傳送者（即某組織）於步驟三，將資料傳送給接收者 u_j，而接收者藉由步驟四的驗證程序，即可確知訊息來源之正確性，爲證明其可行性，我們提出 4 個引理及 1 個定理，用以支持我們理論的正確性。

引理一：在式子(1)-(4)的條件下，

$$Y \equiv g^{a_0} (\mathrm{mod}\, p) \equiv \prod_{t=1}^{w} g^{z_t \left(\prod_{k=1, k\neq t}^{w} \frac{-UID_k}{UID_t - UID_k} \right)} (\mathrm{mod}\, p)$$

證明：

$$a_0 \equiv f(0) (\mathrm{mod}\, q) \equiv \sum_{t=1}^{w} z_t \left(\prod_{k=1, k\neq t}^{w} \frac{-UID_k}{UID_t - UID_k} \right) (\mathrm{mod}\, q)$$

根據 Lagrange interpolation method[12]

$$Y \equiv g^{a_0} \pmod p$$

$$\equiv g^{\sum_{t=1}^{w} z_t \left(\prod_{k=1,k\neq t}^{w} \frac{-UID_k}{UID_t - UID_k} \right) \pmod q} \pmod p$$

$$\equiv \prod_{t=1}^{w} g^{z_t \left(\prod_{k=1,k\neq t}^{w} \frac{-UID_k}{UID_t - UID_k} \right)} \pmod p$$

根據美國數位簽章標準[14]，因此，我們得到證明。

引理二：

$a \equiv b \pmod m$ 及 $d \mid m, d > 0$ ，所以

$a \equiv b \pmod d$

證明：請參考 Niven etc.[11]等人所著第 48 頁定理 2.1 之(5)的證明。

引理三：

在式子(5),(6),(10)-(12),(15),(19),(20)的條件下，式子(22)成立。

證明：根據引理一、二及 Chen and Yu[10]的定理，我們得到結論。

引理四：

式子(22)-(25)成立

證明：此處類似於引理三的證明，我們予以省略。

定理一：式子(22)-(25)正確無誤

證明：由引理一至四，本定理得到證明。

四、結論

我們所提出增強型的群體導向數位簽章策略，允許組織內若干成員（即達到門檻值的規定人數）共同參與即可用組織名義對外傳送訊息，接收訊息者只要根據該組織的公開金匙，而不用瞭解組織內部門檻值策略如何運作，即可辯證該訊息是否確實經過該組織的認可。

比起 Harn[9]的論文，我們不需藉助廣播通道與秘書的協助，所以我們的作法不但達成群體導向數位簽章的目的，亦能減少系統建置成本。此外當 Harn 的系統運用於多重數位簽章環境時，有其侷限性。而我們的作法可以允許組織內部任何訊息自由律定先後傳遞順序，且在其後簽章者可以驗證所有前面簽署訊息者的數位簽章，所耗計算量及所需傳輸量始終維持在常數狀態（即 O(1)）為我們作法的另一優點。

在利用離散對數(discrete logarithm)為基礎的群體導向數位簽章形成過程中，組織內部成員如何互相偵測欺騙者，Chen and Yu[10]已有所著墨，因此，我們省略討論內部成員欺騙問題，而假設參與的成員均是誠實的動用其私人秘密金匙。如果以本論文為基礎，結合 Chen and Yu 的偵測欺騙者的策略，將可成為一個比較理想的群體導向數位簽章系統。

參考文獻

1. Brickell, E.F., and Stinson, D.R.,"The detection of cheaters in threshold schemes," Advances in Cryptology-CRYPTO'88, pp.564-577, 1989.
2. Chaum, D., and Heyst, E.V., "Group signature," Advances in Cryptology - EUROCRYPT'91, pp.257-265. 1992.
3. Chen, L., and Pederson, T. P., "New group signature schemes," Advances in Cryptology - EUROCRYPT'94, pp.163-173, 1995.
4. Desmedt, Y., "Society and group_oriented cryptography: A new concept," Advances in Cryptology - CRYPTO'87, pp.120-127, 1988.
5. _____, Frankel, Y., "Threshold cryptosystem," Advances in Cryptology - CRYPTO'89, pp.307-315, 1990.
6. Diffie, W. and Hellman, M. E.," New Directions in Cryptography," IEEE tran. Information Theory, Vol.IT-22, No. 6, 1976, pp.644-654.
7. ElGamal, T., "A public-key cryptosystem and a signature scheme based on discrete logarithms," IEEE Trans. on Information Theory, Vol.II-31, No.4, pp.469-472, 1985.
8. Frankel, Y., "A practical protocol for large oriented networks," Advances in Cryptology - CRYPTO'89, pp.56-61, 1990.
9. Harn, L., "Group_oriented (t,n) threshold digital scheme and digital multisignature," IEE Proc. Comput. Digit. Tech., Vol.141, No.5, pp.307-313, 1994.
10. Jonathan Jen-Rong Chen and Ping Yu ," A Discrete Logarithm_based Multisignatures Scheme ," Proc. of ICS'96 International Computer Symposium , 1996 , pp48-53.
11. Niven, I., Zuckerman, H.S., and Montgometry, H.L., An Introduction to the theory of numbers, John Wiley & Sons, Inc., U.S.A., 1991.
12. Stinson, D.R., Cryptology: theory and practice, CRC Press, Inc., 1995.
13. Tompa, M., and Woll, H., "How to share a secret with cheaters," Journal of Cryptology, vol.1, pp.133-138, 1988.
14. "The digital signature standard proposed by NIST," Communications of the ACM, vol.35, No.7, pp.36-40, 1992.