階層式金鑰產生之方法-以乘法反元素為研究基礎

陳正鎔
萬能科技大學-資訊管理系
桃園縣中壢市萬能路 1 號
Email:jonathan@mail.vnu.edu.tw

郭恆慶
萬能科技大學-理財經營管理系
桃園縣中壢市萬能路 1 號
Email:khckhc@mail.vnu.edu.tw

摘要

隨著人類社會軌跡之發展，密碼系統廣泛地在人們生活中被使用中，在企業組織中運用密碼的範圍隨其組織規模也越來越廣，然也衍生出資訊安全之新問題。假設在組織中每個人皆有一個密碼，用以作為資料加密之用，一般而言，企業組織中包含著層級之因素，若論上司有權對下屬的資料進行存取動作，亦不為過。一個主管要對所屬各單位下屬的密碼，都要全然了解，其龐大數量之密碼，恐會徒然增加主管在管理密碼上之困擾。有鑑於此，研究者提出階層式金鑰指定方法，使得主管只需記得其自己之密碼，而其下屬之密鑰皆可由此(主管)密鑰推導出。此方法對於階層式組織如政府、軍事單位、公司法人在密鑰的指定上有著顯著之助助；在階層式金鑰指定方法之研究課題上，已有相關的基礎研究，然均有其整體效益不足之憾，本論文提出一個不同思考方向之解決方法。

密碼學的發展，與人類之生活經驗相伴行，其為了反映企業組織之需求，例如：為了使電子文件提供如自然人簽名之效果，而運用公開金鑰密碼系統於數位簽署上；思索企業(分支)組織地理位置之分散，遠距會議需求之產生，為此會議金匙的技術於焉發展出來；在企業組織發展中多數為階層式組織，其中必然出現階層式之隸屬關係，則密碼在管理上亦需要能夠配合組織架構，階層式金鑰指定方法被提出來解決階層式組織，上級對下屬密鑰之如何推導問題，使得上級不需要知道下屬之密碼，而可迅速推導下屬密鑰，減少管理密鑰上的繁瑣。1983 年 AKL 與 Taylor 提出利用質數連乘積，解決金鑰推導之問題，為階層式金鑰指定方法之研究濫觴，為往後之研究建立一個方向；在本研究中，將以乘法反元素作為出發點，發展出一套新的階層式金鑰指定方法，並對以往之密鑰產生方法進行探討比較。

考量以中國餘式定理為基礎，完成密鑰之推導作業，並加入對稱式密碼系統的使用，達成使用者更改加密金鑰時，只需改變一個公開參數，在時間複雜度上只需所採用對稱式密碼系統的時間複雜度，該研究對於企業組織中內組織忠誠度較弱之員工，恐有密鑰外洩之虞；在本研究中提出利用乘法反元素之理念，達成階層式金鑰產生方法之模式，雖然已有眾多學術論文相率提出階層式密鑰產生方法，但是其背後所使用的數學原理並不盡然相同，其所衍生之效益與安全性也有其相異之處。我們擬創設一個不同之思考方向，提供往後相關研究於效益比較上，為企業組織之應用者多一個參考方向；本研究所提出之階層式密鑰方法，無論在密鑰推導方式上、數理模式之複雜度上、使用者增減、彼此關係異動、金鑰變動上有其優異之處，提供業界於階層式金鑰產生方法之使用上另一個選擇。

關鍵字：階層式金鑰、乘法反元素、整數論、因數分解、離散對數

壹、前言

隨著人類社會之發展，密碼系統【3, 5, 7-15, 18, 21, 22, 30】普遍地於人們生活中使用中，在組織運用密碼之範圍有越來越廣之趨勢，然也衍生出新問題。吾人設想組織中成員均有其專屬密碼，用以作為資料加密之用，又組織中包含著層級的因素，所以上司有權對下屬的資料進行存取動作，一個主管要對所屬各單位下屬的密碼，都要全然了

解，這龐大數量的密碼，必會徒然增加主管在管理密碼上的困擾，所以便有人提出階層式金鑰指定方法【1, 2, 4, 6, 16, 17, 19, 20, 23-29, 31】，使得主管只需記得自己的密碼，其下屬的密鑰皆可由此密鑰推導出，此方法對於階層式組織如政府、軍事單位、公司法人在密鑰的指定上有著顯著的幫助；在階層式金鑰指定方法的研究課題上，已有相關的基礎研究，然均有其整體效益不足之憾，本論文提出一個另類思考方向之解決方法。

乘法反元素在密碼學中經常被運用，例如公開密碼系統中之 RSA【21】，利用乘法反元素來達成公鑰、私鑰不對稱之情境，建立密碼學之里程碑；本論文就乘法反元素運用於階層式金鑰指定方法進行說明，並與目前所提出利用質數連乘績、中國餘式定理、牛頓內插多項式進行比較。

然後就質數連乘積、中國餘式定理、牛頓內插多項式進行簡單文獻探討，接著以乘法反元素於階層式金鑰指定方法運作模式進行說明，第四章為結論。

貳、階層式金鑰指定方法回顧

階層式金鑰指定方法是一種要達到的目標，但是其背後所進行的數理方法卻不相同，所導致的是產生不同的推導方法、效率與安全性的差異；因此先就目前提出具特色的指定方法稍作簡介；在對各種方法回顧之前，在這裡先定義一些相關變數關係，令使用者為 u ，若 u_1 為 u_2 的上級則以 $(u_1 > u_2)$ 表示。

一、 以質數連乘積為基之指定方法

1983 年 AKL 與 Taylor【23】提出利用質數連乘積，解決金鑰推導的問題，為階層式金鑰指定方法的濫觴，為往後的研究建立一個主題；其系統運作模式由系統管理者選定母金鑰 k_0 與兩大質數 q_1 、 q_2 ，令 $M = q_1 q_2$ ，並為每一個使用者選定一個質數 p_i ，利用式一計算每個使用者的公開參數 t_i ， t_i 為所有 u_i 上級的 p 值連乘積，則 u_i 的金鑰 k_i 可利用式二導出，若 u_a 為 u_i 的上級則 u_a 可利用式三以 k_a 導出 k_i 。

式一： $t_i = \prod_{(u_j > u_i)} p_j$

式二： $k_i = k_0^{t_i} \bmod M$

式三： $k_i = k_0^{t_i} = (k_0^{t_a})^{t_i / t_a} = (k_a)^{t_i / t_a} \bmod M$

本方法雖然擁有直接推導密鑰、推導過程簡單的優點，但是當有參數異動、使用者增減或關係異動時，都要從新計算所有的密鑰與公開參數十分不經濟。

二、 以中國餘式定理為基之指定方法

1997 年吳宗杉提出部分次序集使用者階層架構存取控制方法【[31]】，以中國餘式定理為基礎，完成密鑰的推導作業，並加入對稱式密碼系統的使用，達成使用者更改加密金鑰時，只需改變一個公開參數，在時間複雜度上只需所採用對稱式密碼系統的時間複雜度；系統管理者選取一個大質數 s_{-1} 及一個雙向函數 h 為系統秘密，並在不大於 s_{-1} 的範圍內選定質數給虛擬金鑰 s_0 ，使用者金鑰 s_i ，為每個使用者選取推導金鑰 d_i 使滿足 $\max\{d_1, d_2, d_3, .., d_n\} < \min\{s_0, s_1, s_2, ..., s_n\}$ ，再以下列式子推導公開參數，並對加密金鑰 k_i 加密。

令 $S = \prod_{i=-1}^{n} s_i$

令 $A_i = S / s_i$ ，其中 i=−1, 0, …, n。

令 b_i 滿足 $b_i A_i \equiv 1 \bmod s_i$

令 $e_i = b_i A_i$ ，其中 i=−1, 0, …, n。

令公開參數 $p_i = h(s_i) e_{-1} + d_i \left(e_0 + \sum_{u_i \le u_a} e_a \right) + \sum_{not(u_i \le u_a)} f(i,a) e_a \pmod S$ ，其中 i=−1, 0, …, n； $f(i,a)$ 亂數產生器。

令 $c_i = E_{d_i}(k_i)$ ，其中 i=−1, 0, …, n；函數 E 為對稱式密碼系統的加密函數

在上述的步驟中，將所產生的 c_i 、 p_i 公開，若 u_1 要導出其下屬 u_2 的密鑰，可利用 $d_1 = p_2 \bmod s_1$ 取得 d_1 ，再以函數 E 的解密函數為 c_2 解密取得 k_2 ；本方法在參數的儲存空間上，需要龐大的容量，及當使用者發生增減時，需從新計算所有的參數兩項缺

點。

三、 以牛頓內插方程式為基之指定方法

1992 年 Chang、Hwang、Wu 提出以牛頓內插法解決密鑰推導問題的方法【[1]】，該方法是一種由上而下的指定方法，在參數的設定上，可分為 root 與非 root 兩種，root 為所有節點的上級，非 root 節點除了有下屬外，還有上級的存在，以下就兩種情況分別敘述。

系統管理者先選取一大質數 p ，單向函數 $f(a)$。

狀況一：當節點為 root 時，沒有任何直屬上級。

設 root 共有 k 個直屬單位。

Step1：在 1 到 p-1 的範圍內選一個整數 SK_r 作為金鑰。

Step2：任意建立多項式 $H_r(X)=SK_r+a_1X+a_2X^2+\cdots+a_kX^k(\bmod p)$ ，其中 $a_1,a_2,\ldots,a_k$ 為 1 到 p-1 間的整數。

Step3：在 1 到 p-1 間，任選 k 個相異整數，以 $P1_{r1},P1_{r2},\ldots,P1_{rk}$ 表示，並計算 $P2_{rj}=H_r(P1_{rj})$，其中 j=1, 2, …, k。

Step4：指定 root 直屬單位的金鑰，令 $SK_{rj}=f(a_j)$，其中 j=1, 2, 3, …, k。

狀況二：當節點為非 root 時，有直屬上級。

設這個節點 N_i 共有 k 個直屬單位，N_i 的直屬上級所分派的金鑰為 SK_i。

Step1：在 1 到 p-1 的範圍內選取 k 個相異整數，以 $P1_{i1},P1_{i2},\ldots,P1_{ik}$ 表示。

Step2：在 1 到 p-1 的範圍內選取另一組 k 個相異整數，以 $P2_{i1},P2_{i2},\ldots,P2_{ik}$ 表示。

Step3：建立多項式 $H_i(X)=SK_i+a_1X+a_2X^2+\cdots+a_kX^k(\bmod p)$ ，符合 $(0,SK_i),(P1_{i1},P2_{i1}),(P1_{i2},P2_{i2}),(P1_{i3},P2_{i3}),\ldots,(P1_{ik},P2_{ik})$ 之條件，其中 $a_1,a_2,\ldots,a_k$ 為 1 到 p-1 間的整數。

Step4：指定 N_i 直屬單位的金鑰，令 $SK_{ij}=f(a_j)$，其中 j=1, 2, 3, …, k。

在上述的步驟中，將所產生的 P1,P2 公開作為公開參數，要推導下屬密鑰時，重建該方程式 $H_i(X)$，以其中係數計算獲得所有直屬單位的密鑰。該方法並不能直接推導出非直接下屬的密鑰，需要用遞迴的方式推導，且在推導的過程中需要明瞭組織的隸屬關係，在使用上並不方便；且遇到使用者有增減情況時，需要重新計算全部的參數與密碼。

參、以乘法反元素為基礎之階層式金鑰指定方法

本研究中以乘法反元素擁有的成對特性，達成訊息保護及推導迅速之優點，在本方法中每個使用者為 u_i ，其中 i 為 1, 2, . . , n，由系統管理者分配且安全地送至每位使用者一個質數 p_i 為其辨識碼，透過所公開之計算法而得到公開參數及金鑰，並以該金鑰為加密金鑰加密；當要導出加密金鑰時，先取得公開參數導出金鑰，再以金鑰為加密金鑰解密。以下將整的過程分為兩個階段，一為系統建置階段、一為密鑰推導階段。

一、系統設定階段：

由系統管理者選取兩大質數 q_1 、 q_2 為系統秘密，並令 $M=q_1q_2$ ， $T_A=(q_1-1)(q_2-1)$ ，在不大於 M 的範圍內選取質數 p_i 分配給每個使用者，並進行下列前置計算。

令 x_i ： $x_i=\prod_{not(u_i<u_j)} p_j$

令 p^* ：p mod T_A 之乘法反元素

令 A 為金鑰

$$A_i=g^{\prod_{not(u_i<u_j)} p_j^*} \bmod M \quad \cdots\cdots\cdots\cdots\cdots\cdots(1)$$

，g 為 mod M 之原根

令 $E_{A_i}(k_i)$ 為對稱式加密函數

令 $D_{A_i}(c_i)$ 為 $E_{A_i}(k_i)$ 之解密函數

令 $c_i=E_{A_i}(k_i)$ 為推導金鑰，其中 k_i 為使用者自訂的加密金鑰

以上 x_i 、 p_i 、 c_i 為公開參數。

二、加密金鑰推導階段：

在完成設定階段的各項參數計算後，所有使用者可利用公開參數，直接推導下屬的金鑰，再以金鑰對加密金鑰進行解密。經過以下兩步驟便可得到下屬的加密金鑰。

1. 若 u_1 為 u_2 的上級欲導出 u_2 的密鑰 k_2，先求出金鑰 A_2。

$$A_2 = A_1^{p_1^{'}(p_2^{'})^*} \bmod M \quad \cdots\cdots\cdots\cdots\cdots\cdots(2)$$

證明

$$A_1 = g^{\prod_{not(u_1<u_i)} p_i^*} \bmod M$$

$$A_2 = g^{\prod_{not(u_2<u_j)} p_j^*} \bmod M$$

A_1 由於是 A_2 的上級，所以在 A_1 中包含 A_2，A_1 可表示為

$$A_1 = g^{\left(\prod_{not(u2<u_i)} p_j^*\right)\left(\prod_{(u2<u_i\le u_1)} p_i^*\right)} \bmod M$$

又 p_i^* 為 p_i 的乘法反元素，所以

$$\left(\prod_{(u2<u_i\le u_1)} p_i^*\right)^{x_1 x_2^*} = 1 \bmod T_A$$

故得

$$A_1^{x_1 x_2^*} = \left(g^{\left(\prod_{not(u2<u_i)} p_j^*\right)*\left(\prod_{(u2<u_i\le u_1)} p_i^*\right)}\right)^{x_1 x_2^*} = A_2 \bmod M$$

2. 求取加密金鑰

$$k_2 = D_{A_2}(c_2)$$

肆、結論

本論文結合乘法反元素之特性，達成階層式金鑰指定方法之可行性，與類似論文比較，其背後支邏輯並不完全相同，當然所產生之效益與安全性也就顯出其相異之處，更可凸顯論文之優異性；本研究提出金鑰指定方法，無論其在指定方式上、推導複雜度上、使用者增減、關係異動、金鑰變動上都有其獨特之方法，可提供業界於實務上之參考。

參考文獻

[1] J. M. Atallah, B. Marina, F. Nelly, and B. F. Keith, “Dynamic and efficient key management for access hierarchies, ” ACM Transactions on Information and System Security, Vol. 12, No. 3, 2009.

[2] J. M. Atallah, J. Mikhail, B. F. Keith, and B. Marina, “Dynamic and efficient key management for access hierarchies, ” In Proceedings of the ACM Conference on Computer and Communications Security(CCS), pp. 190–202, 2005.

[3] J. Bethencourt, A. Sahai, and B. Waters. “Ciphertext-policy attribute-based encryption. In Proceedings of the IEEE Symposium on Security and Privacy (S & P), ” pp. 321–334, 2007.

[4] A. Boldyreva, V. Goyal, and V. Kumar. “Identity-based encryption with efficient revocation. In ACM Conference on Computer and Communications Security (CCS), ” pp. 417–426, 2008.

[5] R. Canetti and S. Hohenberger. “Chosen-ciphertext secure proxy re-encryption. In Proceedings of ACM Conference on Computer and Communications Security (CCS), ” pp. 185–194, 2007.

[6] C. C. Chang, R. J. Hwang, and T.C. Wu, “Cryptographic key assignment scheme for access control in a hierarchy,” Information Systems, Vol. 17, No. 3, 1992, pp. 243-247.

[7] J. J.-R. Chen and Y. Liu,2000, “A

Traceable Group Signature Scheme," Mathematical Computer Modelling, pp 147-160.

[8] J. J.-R. Chen and Y. Liu, 2000, Vol. 15, No. 2, March, "An ID-based digital multisignatures scheme with time stamp technique," International Journal of Computer systems Science & Engineering, pp.105-109.

[9] Y.-R. Chen, J. D. Tygar, and W.-G. Tzeng. "Secure group key management using uni-directional proxy re-encryption schemes." In Proceedings of the IEEE International Conference on Computer Communications (INFOCOM), pages 1952 - 1960, 2011.

[10] K.-Y. Chou, Y-R. Chen, and W.-G. Tzeng. "An efficient and secure group key management scheme supporting frequent key updates on pay-tv systems." In Proceedings of the IEEE Asia-Pacific Network Operations and Management Symposium (APNOMS), pp. 1 - 8, 2011.

[11] A. Giuseppe, F. Kevin, G. Matthew, and H. Susan, "Improved proxy re-encryption schemes with applications to secure distributed storag." Security, Vol. 9, No.1. pp.1 - 30, 2006.

[12] M. Green and G. Ateniese. Identity-based proxy re-encryption." In Proceedings of Applied Cryptography and Network Security (ACNS), pp. 288 - 306, 2007.

[13] M. Green, S. Hohenberger, and B. Waters. "Outsourcing the decryption of abe ciphertexts. In Proceedings of the USENIX Security Symposium, 2011.

[14] L. Harn, and H. Y. Lin, "A cryptographic key generation scheme for multilevel database security," Computers and Security, Vol.9, No.6, 1990, pp.539-546.

[15] J. Hur and D. K. Noh. "Attribute-based access control with efficient revocation in data outsourcing systems." IEEE Transactions on Parallel and Distributed Systems, Vol. 22, No. 7. pp. 1214 - 1221, 2011.

[16] D. Knuth, "The Art of Computer Programming: Volume 2 Semi-numerical Algorithms," 2nd edit, Addison-Wesly, 1981.

[17] C. S. Laih, and L. Hwang, "A branch oriented key management solution to dynamic access control in a hierarchy," Proceedings ACM/IEEE 1991 Symposium on Applied Computing, Kansas City, Missouri, U.S.A., pp.422-429, 1991.

[18] S. Luo, Q. Shen, and Z. Chen. "Fully secure unidirectional identity-based proxy reencryption." In Proceedings of International Conference on Information Security and Cryptology (ICISC), pp. 109 - 126, 2011.

[19] S. J. MacKinnon, P. D Taylor, H. Meijer, and S. G. Akl, , "An optimal algorithm for assigning cryptographic keys to access control in a hierarchy," IEEE Transactions on Computers, Vol.C-34, No. 9,1985, pp.797-802.

[20] I. Ray, I. Ray, and N. Narasimhamurthi. "A cryptographic solution to implement access control in a hierarchy and more." In ACM Symposium on Access Control Models and Technologies (SACMAT), pp. 65 - 73, 2002.

[21] R. Rivest, A. Shamir, and L. Adleman, "A method of obtaining Digital Signatures

and Public-key Cryptosystems, ” Communications of the ACM, Vol.21, No.2, pp. 120~126, 1978.

[22] A. Sahai, H. Seyalioglu, and B. Waters. “Dynamic credentials and ciphertext delegation for attribute-based encryption.” In Proceedings of CRYPTO, pp. 199–217, 2012.

[23] G. A. SELIM and P. D. TAYLOR, “Cryptographic Solution to a Problem of Access Control in a Hierarchy, ” ACM Transactions on Computer Systems, Vol. 1, No. 3, August 1983.

[24] R. S. Sandhu, , “Cryptographic implementation of a tree hierarchy for access control, ” Information Processing Letters, Vol.27, No. 2, 1988, pp.95-98.

[25] A. D. Santis, A. L. Ferrara, and B. Masucci. “Efficient provably-secure hierarchical key assignment schemes.” Theoretical Computer Science, Vol. 412. No. 41, pp. 5684–5699, 2011.

[26] J. Shao, P. Liu, Z. Cao, and G. Wei. “Multi-use unidirectional proxy re-encryption.” In Proceedings of IEEE International Conference on Communications (ICC), pp. 1–5, 2011.

[27] S. Yu, C. Wang, K. Ren, and W. Lou. “Achieving secure, scalable, and fine-grained data access control in cloud computing.” In Proceedings of the IEEE International Conference on Computer Communications (INFOCOM), pp. 534–542, 2010.

[28] Y. Sun and K. J. R. Liu, “Scalable Hierarchical Access Control in Secure Group Communications, ” IEEE INFOCOM 2004.

[29] H. Wang, Z. Cao, and L. Wang. “Multi-use and unidirectional identity-based proxy re-encryption schemes.” Information Sciences, Vol. 180, No. 20, pp. 4042–4059, 2010.

[30] 陳正鎔(民八五年三月),「植基 ElGamal 密碼系統之多重簽章策略」,第四屆國防管理學術暨實務研討會論文集，國防管理學院，pp.639-645。

[31]吳宗杉，管理資訊系統中安全控管機制之設計與應用，博士論文，1997。