以密碼技術建構具彈性之群體決策機制－以國軍救災資訊系統為例

作者／陳岳霖上尉、曾健豪少校、蘇品長上校

提要

一、 國軍建軍的目的，主要應付來自外部敵對勢力的威脅，有鑑於近年各國複合式天然災害頻繁，災害防救已是國軍核心任務之一，國軍需在第一時間站在第一線守護人民，展現國軍擁有保家衛國的戰力。

二、 當國軍支援救災任務，通資電部隊配合架設通資電中心，囿於時間急迫，如何快速且正確的決定適切之地點及因應的開設方式，是完備救災通聯機制的關鍵所在。針對上述場景，如何客製化國軍資訊應用平台上運作，且依權責賦予權重，設計具彈性的門檻值代理盲簽章機制，救災應變及密鑰管理的問題應可迎刃而解。

三、 本研究為一創新的應用構想，融合代理盲簽章、門檻式簽章及權重的演算機制，導入橢圓曲線密碼系統運算速度比現行其他非對稱密碼系統快速特性，設計一套具權重之門檻導向代理盲簽章機制，適用於高彈性群體決策的客製化環境，並具有強化安全性、不可預測性等五項優點，期能對未來的數位化戰場及國防管理作為，提出具體可行的安全應用。

關鍵詞：權重、門檻、代理盲簽章、橢圓曲線密碼系統。

前言

國軍通資電部隊主要任務包括資訊、通訊和電子作戰等，本研究著重於通訊中的無線通訊系統部分，在通訊作業單位中，主要任務是維護國軍通資系統，包括所有通信品質管控、通訊維護、軍用網路及視訊系統架設，當重大天然災害發生時，指揮管制通信系統暢通構聯，維護通信品質與架構，更是極為重要[1]。

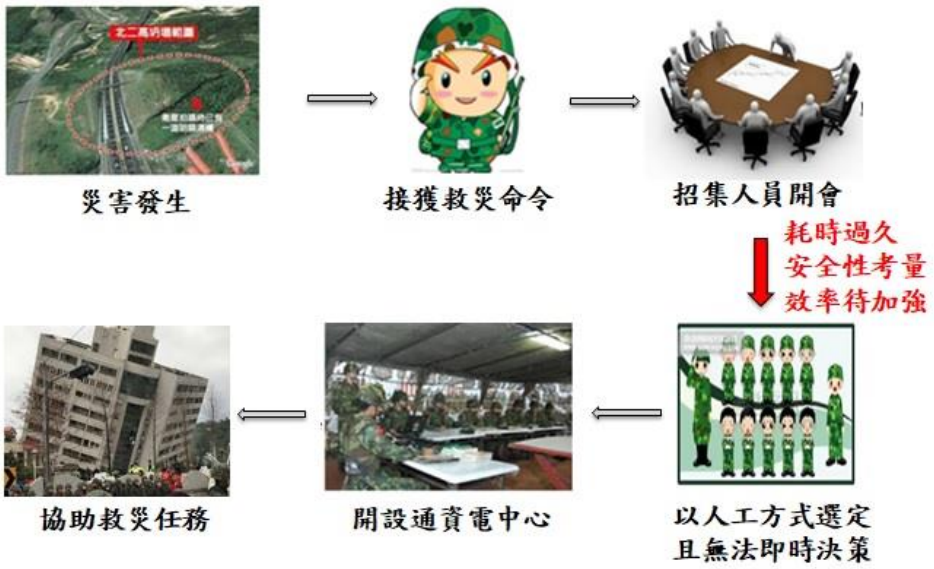
當國軍支援救災任務，通資電部隊配合架設通資電中心，囿於時間急迫，通常由特業(通資電兵科)參謀地圖上直接選定，但地點並非一定理想；或將決定權直接委託各通資電台、組長依據專業立場及現況，判斷可支援的通資電能量來共同商議架設地點。惟各台、組長此時太多分處於各管轄基地，無法集合開會表決(如圖一)，上述因素均勢必影響中心架設速度及救災任務遂行。

另外在安全性的保護上，通常礙於時間考量，均用明文通信，且地點通常不客觀，

[1] 國軍人才招募中心，https://rdrc.mnd.gov.tw/rdrc/iwa/iwa_b.aspx，(檢索日期：2017 年 12 月 28 日)。

無法幫助指揮官迅速掌握能量，其他通資電能量無法有效發揮。效率上，無論是主官決定或集合開會，在命令傳遞上都耗時費力。

圖一 現況分析示意圖



資料來源：作者繪製。

如何客製化設計具權重之門檻式代理盲簽章機制，符合機動性高的救災應變及安全性強的密鑰管理需求，同時解決群體盲思偏誤之疑慮，提升整體決策品質，值得探討與研究。此外，現行簽章機制，基於演算法的設計，導致過多的計算量，直接運用在行動式的資訊平台並不合適，本研究以此為目的，期能對未來的數位化戰場及國防管理作為，提出具體可行的安全應用。

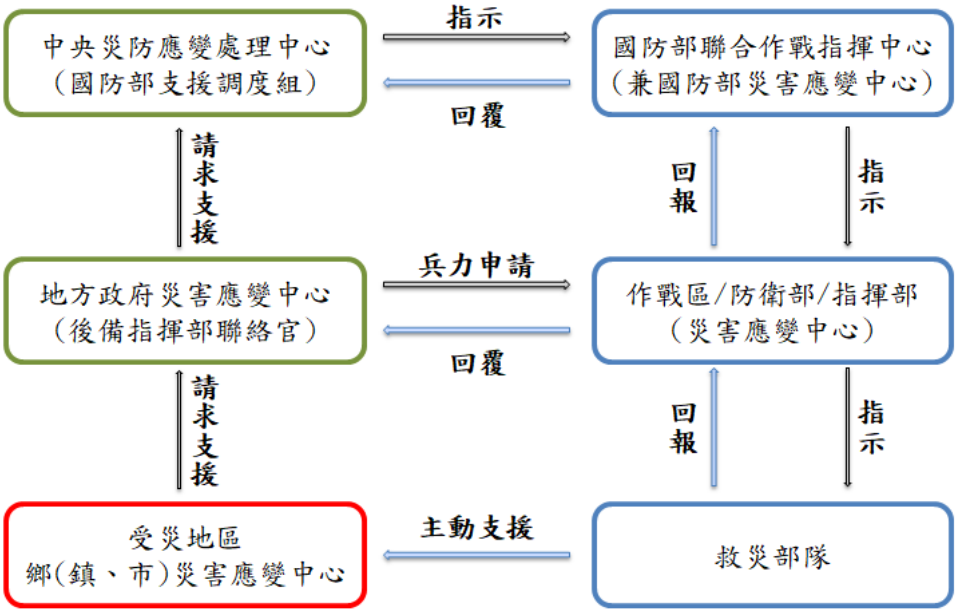
文獻探討

一、現行國軍救災任務處理流程

國軍協助災害防救，由中央災害防救業務主管機關向國防部提出申請；地方由直轄市、縣(市)政府及鄉(鎮、市)公所向所在直轄市、縣(市)後備指揮部轉各作戰區提出申請。但發生重大災害時，國軍應主動派遣兵力協助災害防救，並立即通知直轄市、縣(市)、鄉(鎮、市)及中央災害應變中心。

發生重大災害地區，由作戰區及救災責任分區指派作戰及專業參謀，編成具備勘災能力之災情蒐報小組，掌握災情，並與直轄市、縣(市)政府及鄉(鎮、市)公所首長密切聯繫，適時投入兵力，立即協助救災。直轄市、縣(市)政府及鄉(鎮、市)公所於災害發生期間，緊急申請國軍支援時，作戰區應儘速核定，以電話先行回覆直轄市、縣(市)、鄉(鎮、市)及中央災害應變中心兵力派遣情形，並向國防部回報，流程如圖二。

圖二 國軍災害救援派遣指揮機制圖



資料來源：內政部，〈國軍協助災害防救辦法〉，民國106年4月，頁279。

而國軍面對救災任務，雖均依部頒規定，立即開設各階層之災害應變中心，投入搶救及災後復原等工作，唯內部尚未建置具體且有效的救災資訊系統，除對於緊急接受上級命令及了解即刻災情狀況存有窒礙外，也不利於兵源及人力的分配，致救災任務無法順利遂行。

二、國內救災系統相關研究

(一)國軍防救災地理資訊系統

民國 102 年國防大學管理學院資訊管理學系與中興大學水土保持學系共同研發國軍專屬的防救災地理資訊系統，該計畫搜整國內各相關單位之文獻資料及現有之研究，知悉防救災地理資訊系統的籌建與應用，並結合 GIS(Geographic Information System)方式，透過資料更新、處理、查詢、分析及展示等功能，與災防空間資料相結合，並參考政府部會單位建構防救災之作法，進而完成國軍防救災任務所需地理資訊系統建置，[2]系統之架構如圖三，相關功能如下：

1.結合地理資訊平臺，可作為「空間情報」或「災害防救」等任務之指揮管理或情資服務的基礎，使能清楚了解空間特性與掌握災害態勢。

2.結合全軍產情能量及現行災防任務指管、兵力物資調度機制，可避免延宕救災時效與重複產製之浪費，亦供應即時精確之災防資訊，輔助決策下達。

3.運用 GIS 工具進行決策分析時，可執行多種模擬分析，建立合理的決策模式，並透過個案參數條件的輸入，即可客觀、公正的產生各種決策方案。

[2] 林洋丞、滕春元，〈國軍防救災地理資訊系統實務應用之探討〉《社團法人中華水土保持學會 102 年度年會論文集》，2012 年，頁 3-12。

圖三 國軍防救災地理資訊系統架構示意圖

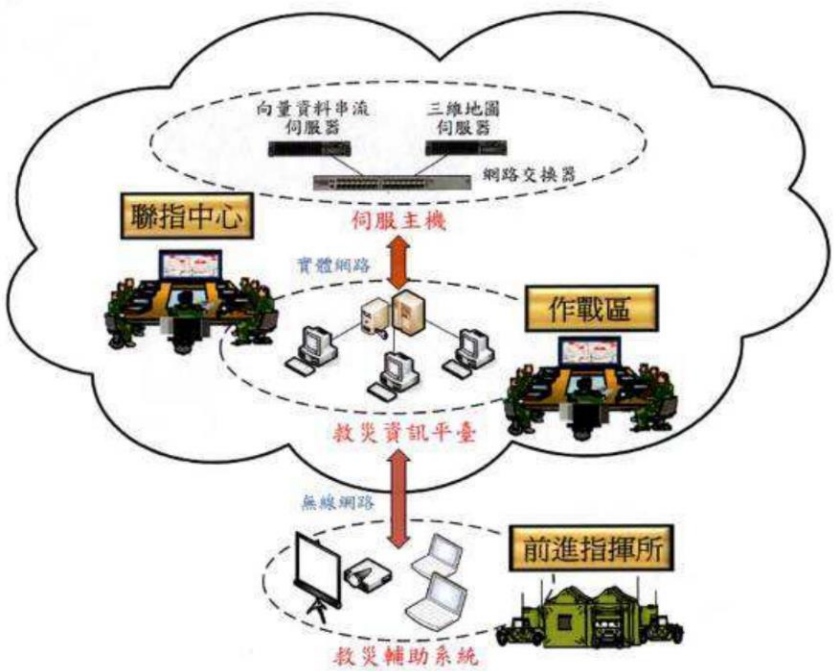
資料來源：林洋丞、滕春元，〈國軍防救災地理資訊系統實務應用之探討〉《社團法人中華水土保持學會 102 年度年會論文集》，2012 年，頁 3-12。

4. 系統架構及功能說明如次(如圖四、五)

(1)三維地圖伺服器(Terra Gate)

將影像與高程資料，融合為三維(3D)地形圖資，發布至網路環境，提供聯指中心、作戰區及前進指揮所之使用者連網使用。另提供協同作業服務，多方網路使用者進行畫面同步、資訊共享與線上對話作業。

圖四 硬體配置及資訊服務示意圖



資料來源：林洋丞、滕春元，〈國軍防救災地理資訊系統實務應用之探討〉《社團法人中華水土保持學會 102 年度年會論文集》，2012 年，頁 3-12。

圖五 系統介面示意圖

資料來源：林洋丞、滕春元，〈國軍防救災地理資訊系統實務應用之探討〉《社團法人中華水土保持學會 102 年度年會論文集》，2012 年，頁 3-12。

(2)向量資料串流伺服器(Terra Gate SFS)

將具有空間資訊之 GIS 向量資料(如 Oracle 空間資料庫、SQL Server 等檔案)，以資料串流方式發布至網路環境，供網路使用者及救災輔助系統使用者運用。

(3)救災資訊平臺

伺服器建構於國防部聯指中心，屬救災資訊於網頁發布之系統介面，網路使用者透過網頁瀏覽器，執行功能與系統操作。

(4)救災輔助系統

針對前進指揮所作業人員，外業任務特性所設計之應用程式介面，可透過瀏覽器連接救災資訊平臺，系統提供使用者運用各項工具執行資訊編輯，執行災害資訊傳遞。

(5)網路使用者

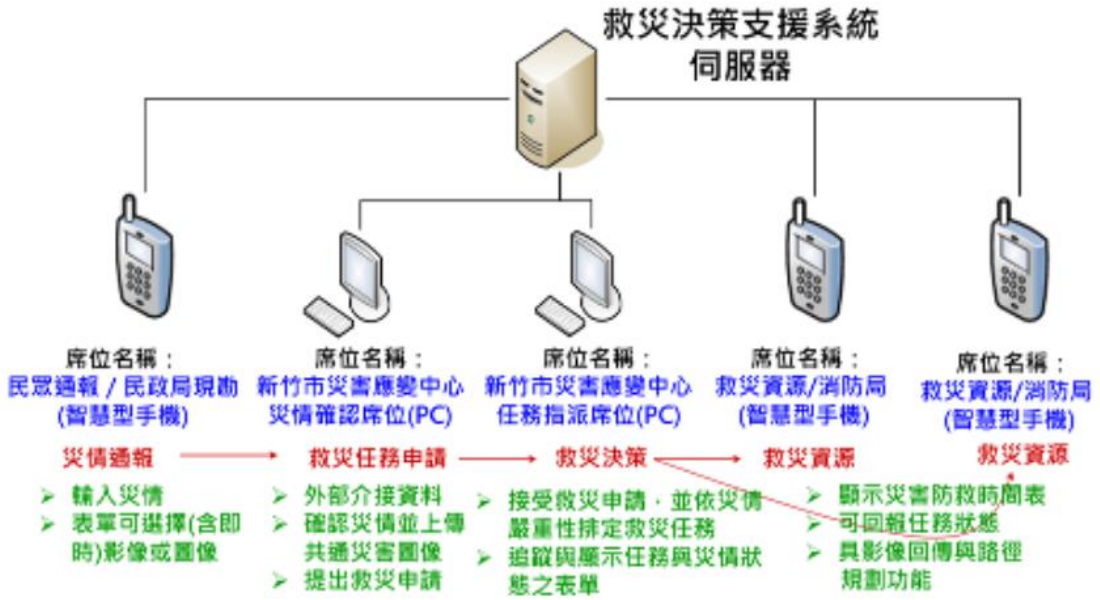
使用者為指揮中心之管理單位，可透過瀏覽器連接救災資訊平臺，並使用系統提供之各項工具，執行災害資訊管理及處置。

(二)救災決策輔助系統

民國 104 年中科院與新竹市消防局共同研發專屬的救災決策輔助系統，該系統具四大功能，分別為整合救災資源與災情資訊、輔助指揮官指派救災任務(決策指派)、即時監控災況與救災單位狀態、自動化產出災況統計與救災成效報表，藉該系統可加速災害應變中心指揮官制定救災計畫與任務、救災人員回報救災狀態，以利完成地方政府的災防工作，[3]系統之架構如圖六，相關功能如下：

[3] 中科院，〈新竹市防救災決策支援系統規劃〉，新竹市政府，2015 年 11 月，頁 8-12。

圖六 災防行動決策支援系統架構示意圖



資料來源：鄒磊，〈智慧防救災系統運用與發展-與新竹市合作建構防救災決策系統〉《陸軍通資半年刊》(桃園市)，第128期，陸軍通信電子資訊訓練中心，2017年9月，頁18-40。

1.具自動化災情通報、勘災任務下達與回傳等功能。

2.具災情總表、任務總表等監控災情與救災任務即時現況等功能。

3.具 8 席位設定及任務指派等功能。

4.具自動化產製災情現況與救災成效之表單等功能。

三、解決群體盲思偏誤

Janis 於 1972 年指出：「團體迷思乃指身處於一高凝聚力的團體內，團體成員對一致性目標的追求凌駕其個人在相關行動方案的實際評估和理性抉擇的一種思維模式」，團體迷思著實代表了團體成員之屈服於從眾壓力，因而造成了其心智能力、事實驗證、道德判斷等方面的退化。[4]

另一方面，團體迷思模式的持續運作無疑地將影響團體決策的效率、效能與能力，與此同時，決策品質亦趨每況愈下。在團體決策過程中，由於成員傾向於讓自己的觀點與群體一致，疏於評估其他可能的選擇方案，令整個群體僅有單方向的思考角度下做出錯誤的決策。

容易發生群體盲思的條件如下：

(一)團體內有高度的凝聚力。

(二)群體隔絕外界資訊與分析。

[4] 陳成宏、粘忠倚，〈學校組織變革的團體決策行為：「艾比里尼弔詭」與「團體迷思」的觀點分析〉《興國學報》，第 7 期，興國管理學院，2007 年，頁 263-273。

(三)群體成員背景和價值觀的相似性很高。

(四)團體剛經歷失敗的打擊。

依據上述論點，軍中環境因獨立於外界資訊，且內部團體亦強調高度凝聚力或服從觀念較深，故群體盲思也易於發生在國軍單位內，而在執行救災任務之時，若因群體盲思的疑慮，以致下達了錯誤決策，延誤救援時機，後果恐不堪設想。為解決此問題產生，本系統設計利用成員權責賦予不同權重，並運用加密投票機制的方式，達到類似匿名性的功能，能以自身最專業的立場判斷事件優劣，以提升決策品質。

相關密碼技術簡介

一、橢圓曲線公開金鑰密碼系統

Miller[5]首先提出了Elliptic Curve Cryptography (ECC)密碼系統，假設一個橢圓曲線是屬於F_q，而A是橢圓曲線$E(F_q)$上的一個點，給定一個屬於橢圓曲線E上的一個點B，若要找出一整數k使得$kQ = B$，因為其特殊的點加法運算，破密者除了逐一的窮舉所有可能的點之外，別無他法，直至目前為止，這個問題仍無法於多項式時間內求出解答，安全度基於離散對數的難題。

ECC 密碼系統的優點是在同樣的安全度之下，相較於現行 RSA 密碼系統(於 1978 年提出，為目前最流行的非對稱式加密演算法，廣為運用於電子商務或資訊系統，其安全度基於極大整數因數分解)，ECC 密碼系統僅需要較小的金鑰長度。相同地，在同樣的金鑰長度下，ECC 密碼系統卻擁有更高的安全性(如表一)，因此運用於使用者將所需使用之服務及權限種類序列值與公享密鑰執行橢圓曲線點加法運算，破解者若想解開這些資訊，將面臨 ECC 密碼系統難題。

表一 RSA 與 ECC 在相同安全度下金鑰長度之比較表

長度 / 項目	金鑰長度(bits)				
RSA	1024	2048	3072	7680	15360
ECC	160~223	224~255	256~383	384~511	512+
金鑰長度比	1:6	1:9	1:12	1:20	1:30

資料來源：NIST, “ Computer Security Division”, NIST Special Publication 800-57, 2012, pp.1-10.

二、門檻式密碼系統

門檻式密碼系統(Threshold Secret Sharing Scheme)是一種簡單且有效的秘密分享

[5] Miller, V. S., 1985, “Use of Elliptic Curve in Cryptography, Advance in Cryptography-Crypto,” New York:Spring-Verlag, pp.417-426-209.

(Secret Sharing)方法；[6]系統中有兩個重要參數：門檻值 *t* (Threshold Value)，以及次密鑰的數目 *n*，一般皆採用(*t*, *n*)來表示，莊家(Dealer)將其所選定的主密鑰 *K* 打造成 *n* 份不同的次密鑰，並讓每一位參與者(Shadow Holder)皆獲得一支次密鑰；(*t*, *n*)門檻式簽章便是結合數位簽章與門檻式密碼系統，提出一種同時將簽章權力與訊息認證分享給團體的機制；[7]門檻式簽章具有二種特性：

(一)當次密鑰的數目超過或等於門檻值*t*的時候可以推導出主密鑰*K*。

(二)當次密鑰的數目小於門檻值*t*的時候，則無法推導出主密鑰*K*。

三、權重式簽章

權重式簽章是一種以權重為基底的群體導向(Group-Oriented)數位簽章技術。現實生活中，群體之間傳遞訊息的問題已愈顯重要，藉由設定個人在這個群體的權重，再依組織的機密性設定群體加解密的授權權重，可運用於線上簽核機制或電子採購等系統；[8]理想的權重式簽章必須具備三種特性：

(一)適用於任何的組織體系，包含階層式及平行式的架構。

(二)最少能滿足三個門檻的架構，將群體分類，分別客製化賦予門檻值及權重，需同時達到門檻才能執行。

(三)群體必須由系統賦予的權重來區分使用者，權重值高為強使用者，權重值低為弱使用者。

本研究基於上述所提及之橢圓曲線公開金鑰密碼系統、門檻式密碼系統及權重式簽章等技術，除導入權重應用的構想，並運用了ECC系統相較於其他非對稱密碼系統，具較高的安全性及效益。設計具高度彈性之群體決策機制，以有效提升系統的執行效率及決策品質，且適合於行動式之國軍通訊資訊網路。

設計具高度彈性之群體決策機制

本研究區分為八個階段：系統初始階段、門檻金鑰分配及認證階段、門檻式簽章產生階段、導入權重分配階段、代理階段、盲化階段、代理盲化驗證階段、門檻驗證階段，以下對本方法各階段進行說明：

一、本系統整體運作流程架構及參數表

運作流程首先由金鑰分配中心(Key Distribution Center, KDC)賦予團體成員身分並完成金鑰驗證及簽章產製，以確認身分別，後續導入權重因子，進而建立代理及盲化

---

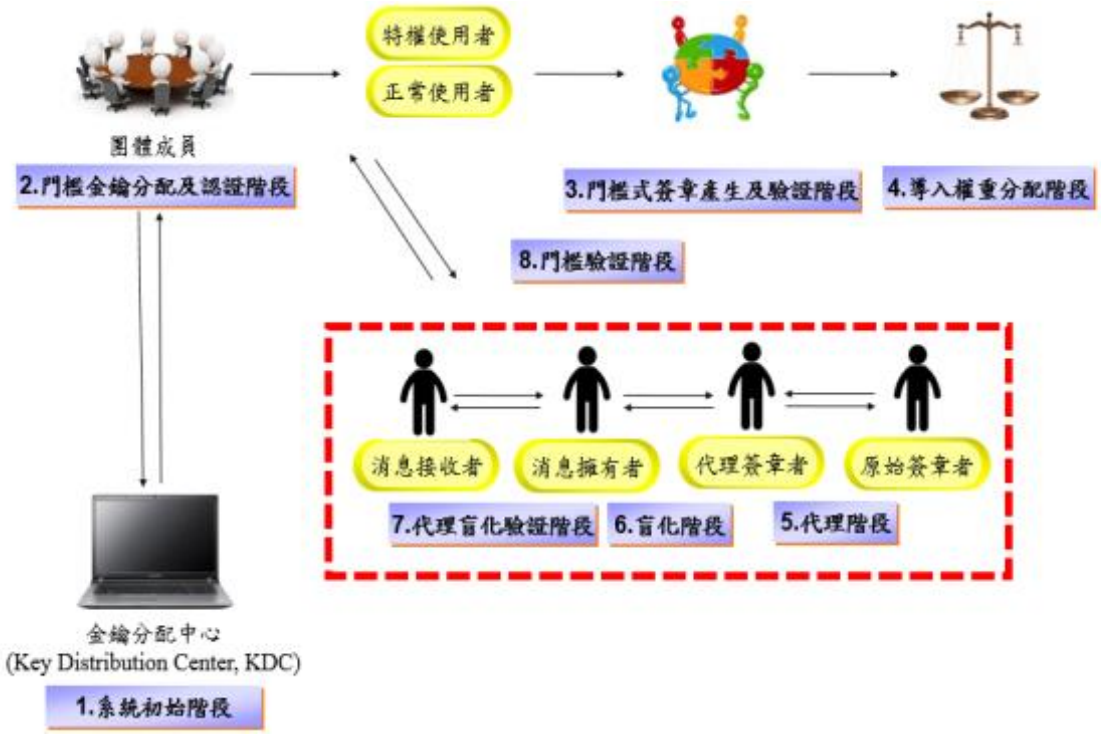
[6] Shamir, A., How to share a secret, Communications of the ACM, (22:11), 1979, pp. 612-613.

[7] Desmedt, Y., and Frankel, Y., 1991, Shared generation of authenticators and signatures, in Proc. of Advances in CRYPTO'91, pp. 457-469.

[8] 蘇品長，〈群體導向的數位簽章技術之研究〉《全國管理碩士論文獎暨研討會論文集》，第 39 卷第 4 期，1996 年，頁 1-9。

機制，使能加快投票速度及提升決策品質，本研究設計構想如圖七、符號說明如表二。

圖七 本研究之設計構想圖



資料來源：作者繪製。

表二 符號說明表

項次	符號	說明	項次	符號	說明
1	$E(F_q)$	有限域F_q中的一條橢圓曲線	14	d	門檻式簽章團體私鑰
2	G	橢圓曲線中的基點	15	Y	門檻式簽章團體公鑰
3	n	橢圓曲線上基點的秩	16	p_i	門檻式簽章團體個別成員
4	q	$q > 2^{224}$之大質數	17	u_i	門檻式簽章莊家為p_i選取隨機參數
5	a_0, b_0	門檻式簽章主密鑰	18	σ_i	門檻式簽章團體驗證p_i參數
6	PK_{KDC}	代理盲簽章主公鑰	19	id_i	門檻式簽章團體p_i成員的身分
7	sk_{KDC}	代理盲簽章主私鑰	20	d_i	門檻式簽章p_i在團體中的私鑰
8	sk_u	代理盲簽章自選之部分私鑰	21	Y_i	門檻式簽章p_i在團體中的公鑰
9	ID_u	用戶身分	22	(r_i, s_i)	門檻式簽章p_i在團體中的個別數位簽章
10	W_u	ID_u由sk_{KDC}所產生部分公鑰	23	(r, s)	門檻式簽章團體數位簽章
11	t_u	ID_u由sk_{KDC}所產生部分私鑰	24	U_z	代理盲簽章隨機因子
12	U_u	ID_u自行運算所產生部分公鑰	25	h_1	代理盲簽章用戶身分ID_u與W_u點轉換成值的雜湊函數

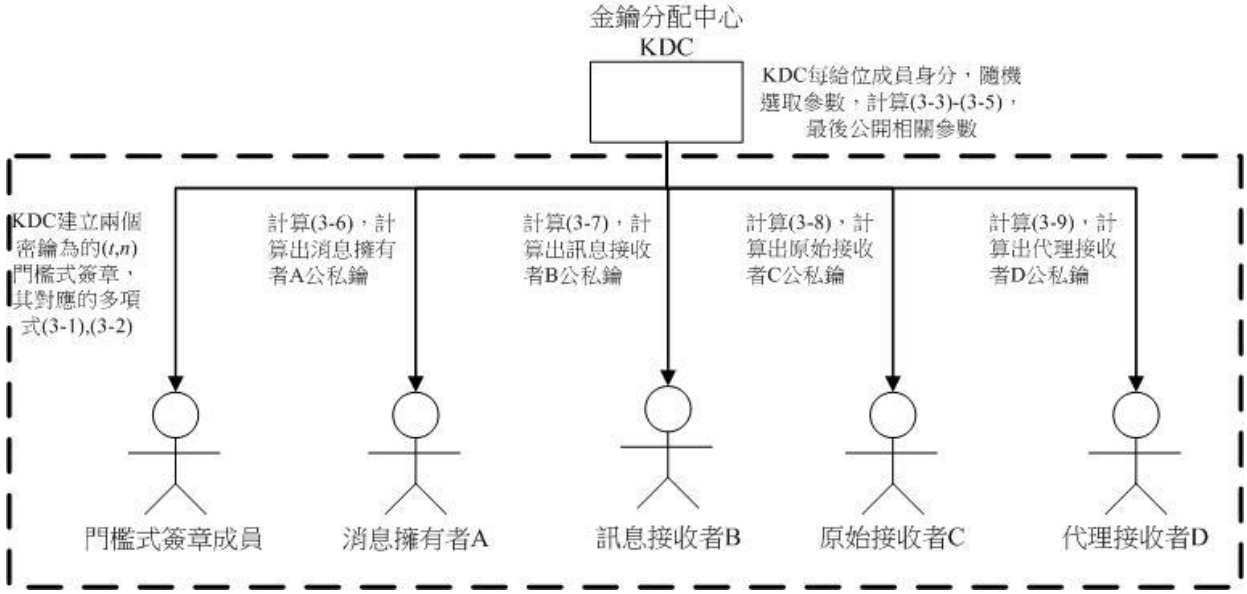
13	r_u	ID_u自行運算所產生部分私鑰	26	h_2	門檻式簽章u_i與id_i共同轉換成值的雜湊函數
27	h_3	門檻式簽章將m轉換成值的雜湊函數	32	k_o	原始接收者 C 隨選之任意值，計算授權公鑰R_o。
28	h_4	將明文序列$(h_3(m), x_i)$點轉換成值的雜湊函數	33	R_o	授權公鑰
29	H_5	將明文序列m_w轉換成點的雜湊函數	34	k_p	代理簽章者 D 隨選之任意值，計算代理私鑰R_P。
30	m_w	代理盲簽章中，原始接收 C 授權給代理簽名者 D 範圍內的認證訊息	34	R_P	代理私鑰R_P。
31	Y_p	簽証公鑰	36	z_1, z_2	代理盲簽章盲因子

資料來源：作者研究整理。

二、系統初始階段

系統在有限域上選取一條安全的橢圓曲線$E(F_q)$，(q 為一個 224bits 以上大質數)，並在$E(F_q)$上選一階數(Order)為n的基點G，使得$n \cdot G = O$，O為此橢圓曲線之無窮遠點，並選取五個單向雜湊函數$\{h_1(), h_2(), h_3(), H_4(), H_5()\}$, $H()$為數值轉點的單向雜湊函數， $h()$為數值轉數值的單向雜湊函數，計算公開參數，示意圖如圖八、計算公式如表三。

圖八 系統初始階段示意圖



資料來源：作者繪製。

表三 計算公式

公式(3-1)	$\boldsymbol{f(x) \equiv a_0 + a_1 x + \cdots + a_{t-1} x^{t-1}}$
公式(3-2)	$f(x) \equiv a_0 + a_1 x + \cdots + a_{t-1} x^{t-1}$

公式(3-3)	$PK_{KDC} \equiv sk_{KDC} \cdot G$
公式(3-4)	$W_u \equiv sk_u \cdot G$
公式(3-5)	$t_u \equiv sk_u + sk_{KDC} \cdot h_1(ID_u, W_u)$
公式(3-6)	$W_A \equiv sk_A \cdot G\ , t_A = sk_A + sk_{CA} \cdot h_1(ID_A, W_A)$
公式(3-7)	$W_B \equiv sk_B \cdot G, t_B = sk_B + sk_{CA} \cdot h_1(ID_B, W_B)$
公式(3-8)	$W_C \equiv sk_C \cdot G, t_C = sk_C + sk_{CA} \cdot h_1(ID_C, W_C)$
公式(3-9)	$W_D \equiv sk_D \cdot G, t_D = sk_D + sk_{CA} \cdot h_1(ID_D, W_D)$
公式(3-10)	$d = (f(0) + g(0))$
公式(3-11)	$Y = d \cdot G(f(0) + g(0)) \cdot G$
公式(3-12)	$R_i = k_i \cdot G$
公式(3-13)	$\sigma_i = h_2(u_i \| \| ID_i)$
公式(3-14)	$Y_i = d_i \cdot G = f(x_i) \cdot G$
公式(3-15)	$d_i = (f(x_i) + g(x_{ij}))$
公式(3-16)	$Y_i = d_i \cdot P = (f(x_i) + g(x_{ij})) \cdot G$
公式(3-17)	$d_i \cdot G = \sum_{j=0}^{t-1} i^j (a_j \cdot G)$
公式(3-18)	$d_i \cdot G = \sum_{j=0}^{t-1} i^j (a_j \cdot G) + \sum_{j=0}^{t_1-1} i^j (b_j \cdot G)$
公式(3-19)	$R_i = k_i \cdot \mathrm{G} = (x_i, y_i)$
公式(3-20)	$r_i = H_4(h_3(m), x_i)$
公式(3-21)	$s_i = (r_i \cdot d_i \cdot C_i + k_i) = (r_i \cdot f(x_i) \cdot C_i + k_i)$
公式(3-22)	$s_i = (r_i \cdot d_i \cdot C_i + k_i) = (r_i \cdot f(x_i) + g(x_{ij}) \cdot C_i + k_i)$
公式(3-23)	$C\_i = (\prod\_(j = 1,\ j \neq 1)\text{\^{}}t \text{▒}〖\ -x\_i\ 〗\ )/(x\_i - x\_j\ )$
公式(3-24)	$R_i = \ s_i \cdot P - r_i \cdot C_i \cdot Y_i$
公式(3-25)	$d_i = w \times b_i(\mathrm{mod}m), i = 1, \dots, n$
公式(3-26)	$j \gg n - j, d_i = e_i \times 2^{n-j} + v_i$
公式(3-27)	$u_i = e_i + t \times v_i, i = 1, \dots, n$
公式(3-28)	$p > \sum_{i=1}^{n} u_i\ , q > \sum_{i=1}^{n} v_i$
公式(3-29)	$A = (a_1, a_2, \dots,\ a_n), 0 \leq a_i \leq pq - 1$
公式(3-30)	$a_i = u_i(\mathrm{mod}p) = v_i(\mathrm{mod}q), i = 1, \dots, n$
公式(3-31)	$(x_{w1}, x_{w2,}\ x_{w3})_2 = \{(x_1, x_2, x_3) \dots (x_{n-2}, x_{n-1}, x_n)\}, x_i \in \{0, 1\}$
公式(3-32)	$c = a_1x_1 + a_2x_2 + \cdots + a_nx_n$
公式(3-33)	$e = u - t \cdot v$
公式(3-34)	$d = e \cdot 2^{n-j} + v$
公式(3-35)	$y = w^{-1} \cdot d(\mathrm{mod}m)$
公式(3-36)	$R_o \equiv k_o \cdot G\ \equiv (R_{o_x}, R_{o_y})$
公式(3-37)	$n_1 \equiv t_C \cdot R_{o_x} + r_C$
公式(3-38)	$N_2 \equiv W_D + PK_{CA} \cdot h_1(ID_D, W_D)$

公式(3-39)	$Y_p \equiv n_1 \cdot U_D$
公式(3-40)	$\lambda_p \equiv t_D \cdot R_o = (\lambda_{p_x}, \lambda_{p_y})$
公式(3-41)	$\sigma_p \equiv r_D \cdot n_1$
公式(3-42)	$T_1 \equiv r_A \cdot H_5(m_w) = r_A \cdot M_w$
公式(3-43)	$T_2 \equiv t_A \cdot G$
公式(3-44)	$T_1 + T_2 \equiv (r_A \cdot M_w) + \left(sk_A + sk_{CA} \cdot H_1(ID_A, W_A)\right) \cdot G \equiv (r_A \cdot M_w) + (W_A + PK_{CA} \cdot H_1(ID_A, W_A)) \equiv r_A \cdot M_w + h_1(ID_A, W_A) \cdot PK_{CA} + W_A$
公式(3-45)	$\alpha \equiv k_p \cdot R_o = (\alpha_x, \alpha_y)$
公式(3-46)	$\beta \equiv t_D \cdot G$
公式(3-47)	$R_p \equiv \alpha \cdot \beta = k_p \cdot R_{o_x} \cdot t_D \cdot G$
公式(3-48)	$U_z \equiv z_1 \cdot G + z_2 \cdot R_p \equiv (U_x, U_y)$
公式(3-49)	$R_z \equiv H_5(m_w) + U_z \equiv M_w + U_z \equiv (R_{z_x}, R_{z_y})$
公式(3-50)	$m_w' \equiv R_{z_x} \cdot z_2^{-1}$
公式(3-51)	$E \equiv z_3 \cdot U_D$
公式(3-52)	$R' \equiv m_w' \cdot G + E$
公式(3-53)	$S' \equiv z_3 \cdot G - r_A \cdot R'$
公式(3-54)	$E \equiv z_3 \cdot U_D$
公式(3-55)	$U_{AD} \equiv r_A \cdot r_D \cdot G$
公式(3-56)	$m_w' \cdot G \equiv R' - E$
公式(3-57)	$s_Z' \equiv k_p \cdot \lambda_{p_x} + m_w' \cdot \sigma_p$
公式(3-58)	$s_z \equiv s_Z' z_2 + z_1$
公式(3-59)	$M_{w_1} \equiv R_Z - s_z \cdot G + R_{Z_X} \cdot Y_p$
公式(3-60)	$s_Z \cdot G \equiv U_Z + R_{Z_X} \cdot Y_p$
公式(3-61)	$R_i = s_i \cdot P - r_i \cdot C_i \cdot Y_i$
公式(3-62)	$s = \sum_{i=1}^{t} s_i$
公式(3-63)	$r = \sum_{i=1}^{t} r_i$

資料來源：作者研究整理。

三、系統建置流程

(一)門檻金鑰分配及認證階段

1. 金鑰分配中心(KDC)利用(3-1)、(3-2)式產生團體私鑰。

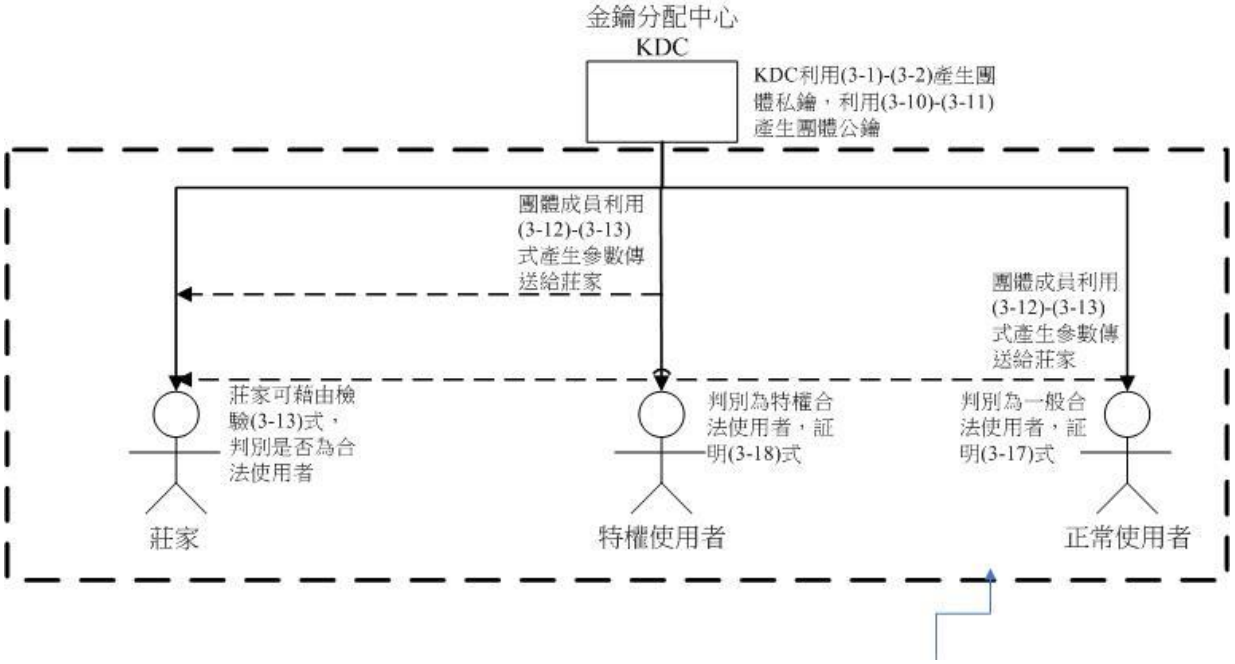
2. 並依照使用者的身分別不同，KDC分配其相對應的私鑰，並透過廣播公布公鑰。(如圖九)

(二)門檻式簽章產生階段

1. 團體成員利用(3-19) ~ (3-22)式產生團體簽章。

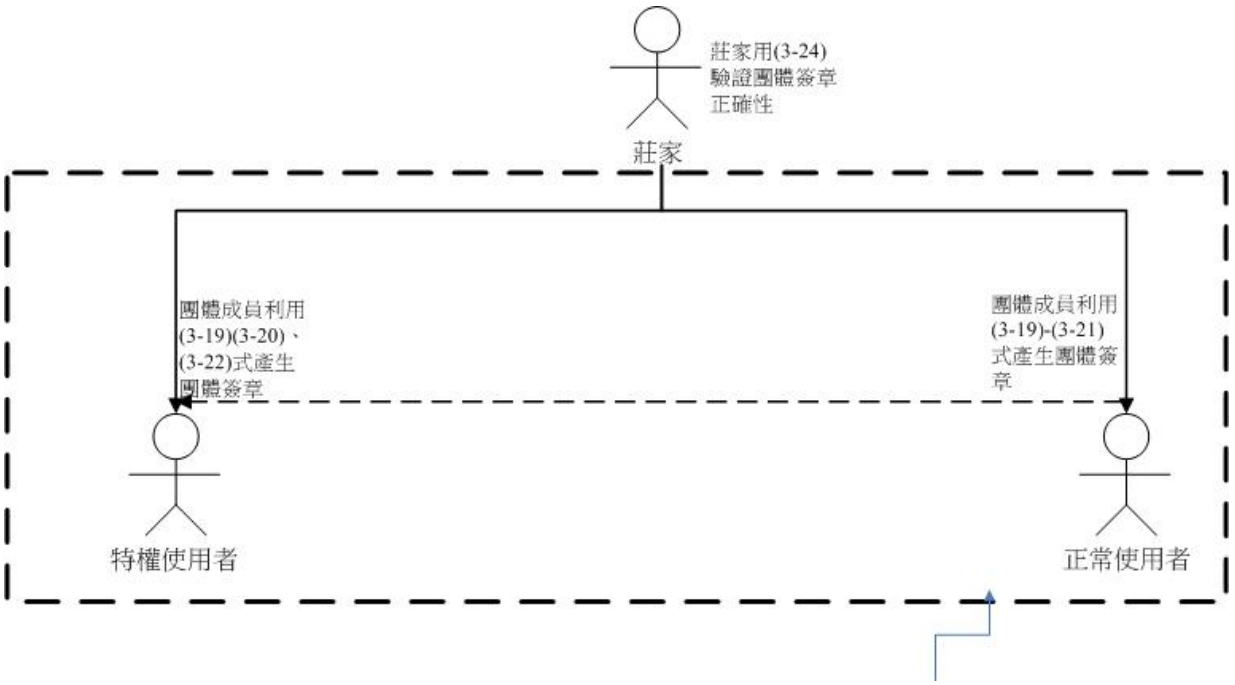
2. 莊家接受個別簽名 s_i，並使用簽章者的公鑰去驗證其正確性。(如圖十)

圖九 門檻金鑰分配及認證階段示意圖



資料來源：作者繪製。

圖十 門檻式簽章產生階段示意圖



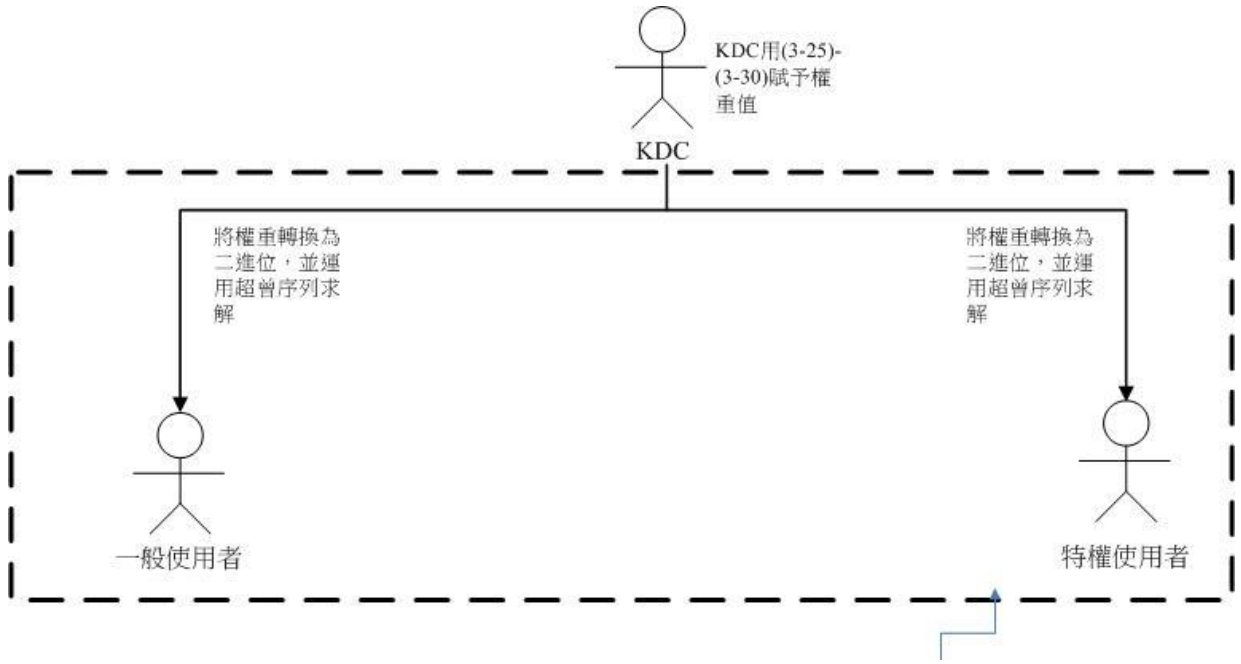
資料來源：作者繪製。

(三)導入權重分配階段

1.針對進入門檻的訊息，依據屬性問題，賦予各成員不同的權重，此權重由KDC客製化分配。

2.將權重轉換為二進位參數，並運用超增序列求解(如圖十一)。

圖十一 導入權重分配階段示意圖



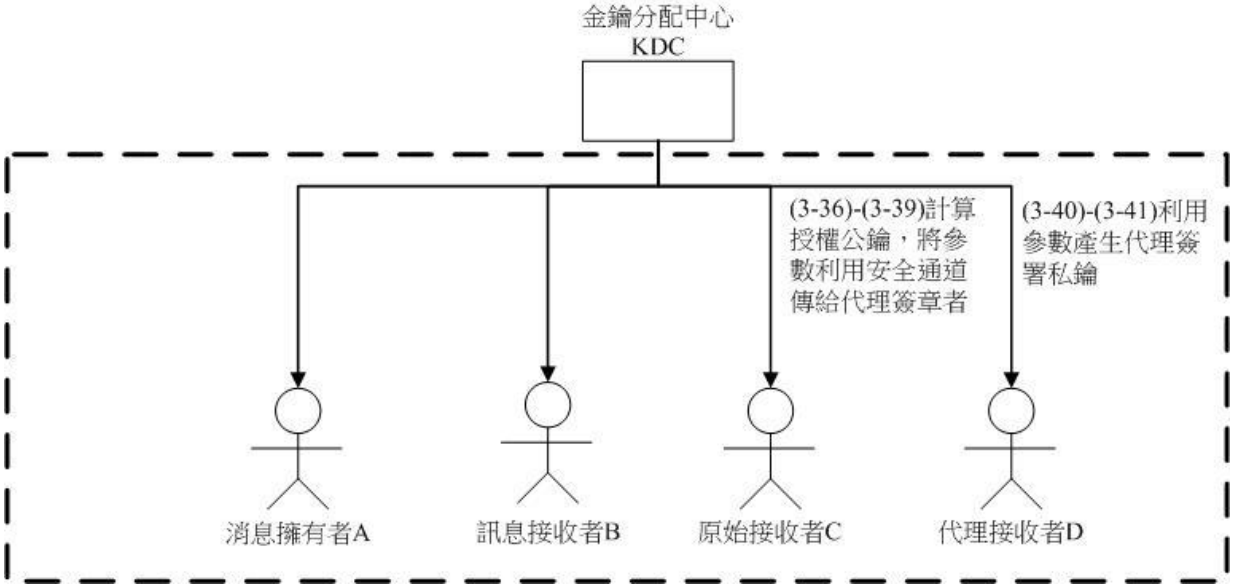
資料來源：作者繪製。

(四)代理階段

1. 若成員有事需代理時，原始簽名者無法親自簽署，必須請代理簽章者代理簽署。

2. KDC利用(3-36)、(3-39)式計算授權公鑰，將參數利用安全通道傳給代理簽章者，並產生代理簽章私鑰(如圖十二)。

圖十二 導入權重分配階段示意圖



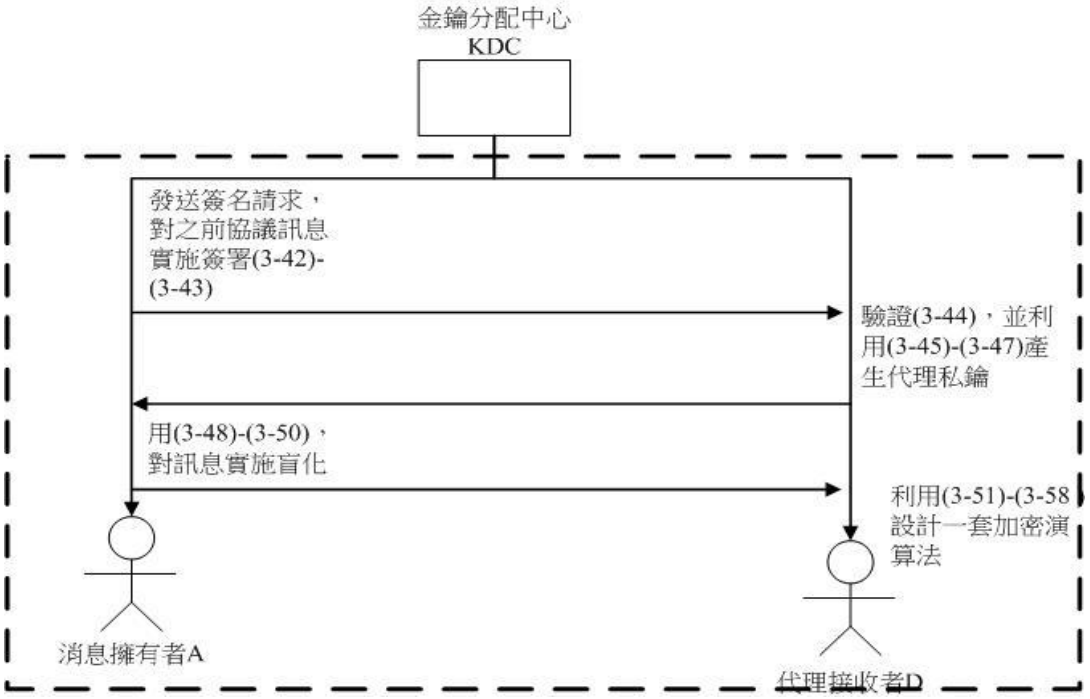
資料來源：作者繪製。

(五)盲化階段

1. 消息擁有者發送簽名請求，要求簽名者對之前協議的訊息 m_w 實施簽署

2. 先驗證(3-44)，利用(3-45)、(3-47)產生代理私鑰，對訊息實施盲化(如圖十三)。

圖十三 盲化階段示意圖



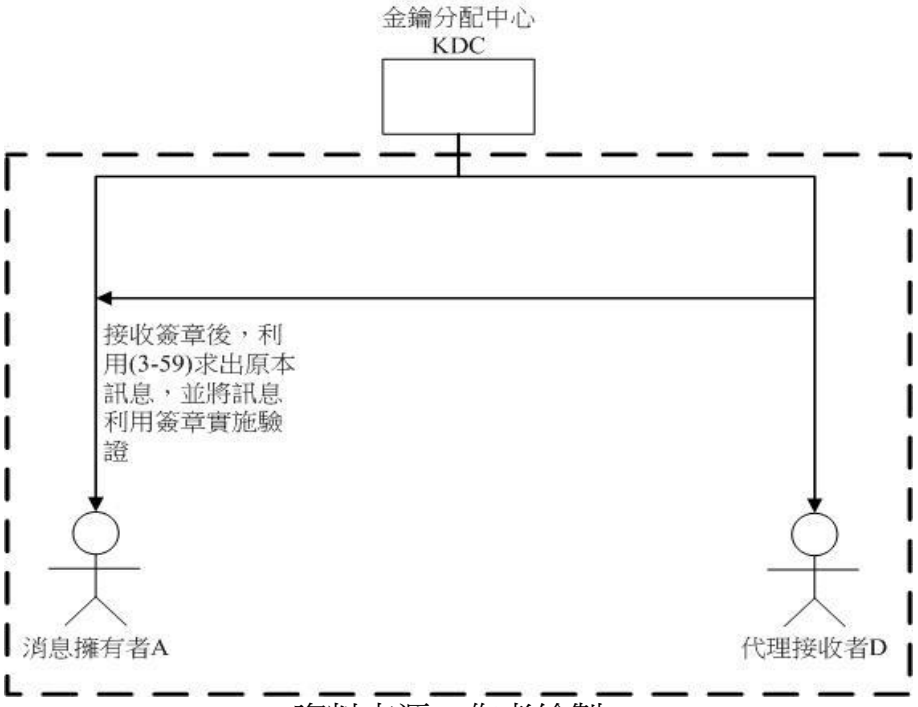
資料來源：作者繪製。

(六)代理盲化驗證階段

1. 接收簽章後，利用(3-59)求出原本訊息，並將訊息利用簽章實施驗證。

2. 將接收到的簽章(U_Z, s_Z)和通過解密得到的訊息M_w代入，若成立，即證明訊息還原正確(如圖十四)。

圖十四 代理盲化驗證階段示意圖



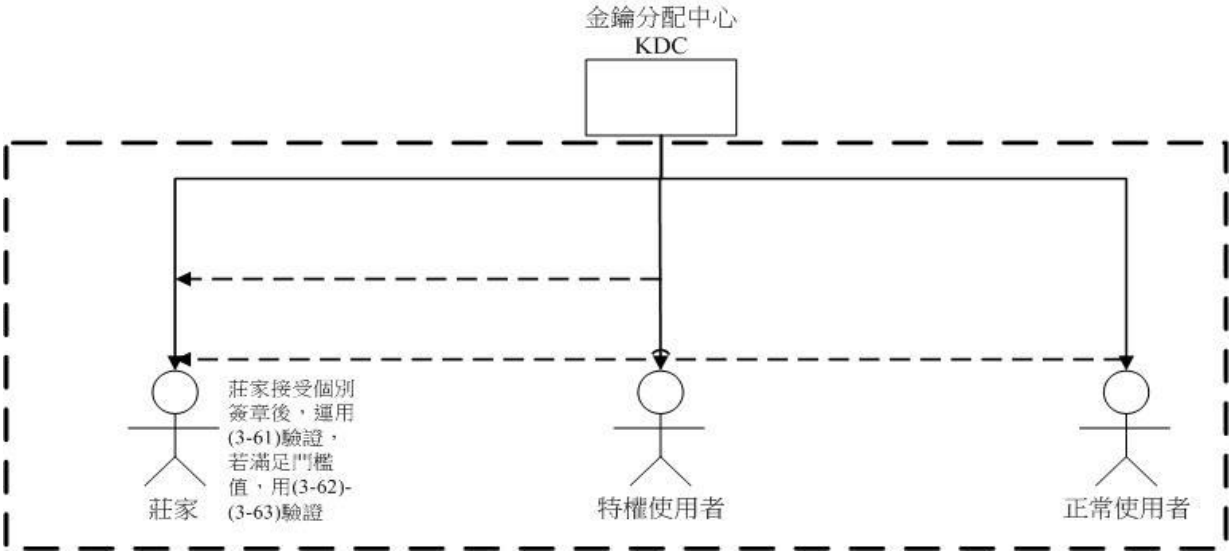
資料來源：作者繪製。

(七)門檻驗證階段

1. 莊家接受個別簽名 s_i，並使用簽章者的公鑰去驗證其正確性。

2. 假設團體中的成員接受個別簽章數滿足(t,n)及(t_1,n_1)的門檻值要求，即可獲得授權(如圖十五)。

圖十五 門檻驗證階段示意圖



資料來源：作者繪製。

安全性及效益分析

本研究為創新的密碼學應用構想，運用 ECC 密碼系統，整合代理盲簽章及(t, n)門檻式密碼系統的基礎架構，並導入可彈性調整權重概念，適合運用於行動式之國軍救災資訊系統，本章節與相關文獻之安全與效益分析比較如后。

一、安全性分析

(一)機密性(Confidentiality)

機密性是指資料不得被未經授權之個人、實體或程序所取得或揭露的特性；[9]本系統中使用橢圓曲線公開金鑰之加密方式。承繼題意，描述本研究符合機密性之特色及如何避免非善意的攻擊手法，詳述如后：

1. 攻擊者想解開訊息m_w，必須得到(t_D,r_D)，消息擁有者D的私鑰，將獲得的(t_D,r_D)透過(3-40)-(3-41)式實施驗證，但攻擊者無法得知(t_D,r_D)，即便是取得公鑰(W_D,U_D)，想取得私鑰(t_D,r_D) 必須面臨解橢圓曲線離散對數的難題(Elliptic Curve Logarithm Problem, ECDLP)，符合機密性的定義。

2. 假設攻擊者想從團體簽章方面著手，攻擊者沒有團體私鑰d，無法通過(3-23)--(3-24)式認證，若想求出團體私鑰d，便面臨解ECC密碼系統離散對數的難題，即便是

[9] Stallings, W., “Cryptography and Network Security Principle and Practices,” Prentice Hall, 2004, pp.203-204.

擁有團體公鑰Y，也無法直接從(3-21)-(3-22)式得到團體私鑰d，故可驗證群體簽章的機密性。

(二)鑑別性(Authenticity)

鑑別性是指確保主體如使用者、程序、系統與資訊等實體或資源之識別，也就是其所聲明者的特性。承繼題意，描述本研究符合鑑別性之特色及如何避免非善意的攻擊手法，詳述如后：

1. 合法接收到的簽章(U_Z, s_Z)並通過解簽章後得到的訊息M，需帶入式(3-60)進行驗證，透過式(3-48)、(3-59)的檢驗，若成功通過驗證，即證明為原訊息M的合法簽章，符合鑑別性的定義。

2. 假設攻擊者偽冒代理簽章者D要獲得消息擁有者A訊息時，必須偽造(R', s')；在(3-52)-(3-54)式，消息擁有者A任選$\{z_3 \in Z_n^*\}$；r_A為消息擁有者A的私鑰，在無法得知的情況下，假設消息擁有者A想要偽造代理簽名者D的簽章，必須偽造(U_Z, S_Z)；在(3-48)、(3-58)式，必須偽造$\{R_p, s_z'\}$；透過(3-45)-(3-47)與(3-57)式，方能通過驗證，由於$\{k_p, \lambda_{p_x}, \sigma\}$僅掌握在代理簽名者D手中，攻擊者必須面臨解ECDLP的難題。

(三)完整性(Integrity)

完整性是指對資料之精確與完整安全保證的特性，也就是確認資料未遭受竄改及破壞。承繼題意，描述本研究符合完整性之特色及如何避免非善意的攻擊手法，詳述如后：

1. 攻擊者想要偽冒原始消息擁有者A發送訊息給代理簽名者D簽署，必須獲得代理簽署私鑰(λ_p, σ_p)，代理簽署私鑰是透過(3-40)-(3-41)式產生的，由式子可知，除了要知道代理簽名者D的私鑰(t_D, r_D)外，也必須得到$\{n_1, N_2, Y_p\}$參數，透過(3-36)-(3-39)式，攻擊者無法任意更改資料，故符合其特性。

2. 假設攻擊者想竄改代理簽名者D簽章訊息而不被發現，透過(3-45)-(3-50)式，將面臨破解單向雜湊函數(One-Way Hash Function, OWHF)難題，無法實施竄改而不被發現，且無法得到代理簽名者D的私鑰(t_D, r_D)，符合完整性需求。

(四)門檻特性(Threshold Characteristics)

門檻特性(Shamir., 1979)將指莊家選定主密鑰K打造成n份不同的次密鑰並讓每一位參與者皆獲得，當次密鑰的數目超過或等於門檻值 t 時，可以導出主密鑰，反之則無法。承繼題意，描述本研究符合門檻特性之特色及如何避免非善意的攻擊手法，詳述如后：

1. 假設攻擊者想通過門檻機制，獲得團體簽章的權力。本研究是基於雙重秘密分享概念，根據(3-1)-(3-2)式，由KDC任意選取兩個多項式，在(3-10)-(3-11)式中，KDC賦予團體私鑰d，在(3-12)-(3-16)式，KDC賦予成員使用者私鑰d_i，根據(3-17)-(3-18)

式，群體內正常的成員若未超過t，具有特權的成員若未超過t_1，便無法實施團體簽章，故滿足其門檻特性。

2.門檻式簽章產生是由(3-19)-(3-20)式構成團體簽章，不論成員p_i是否為具有特權的使用者，必須透過(3-21)-(3-23)式產生，接著運用(3-24)式驗證團體簽章的正確性，故符合其門檻特性。

二、效能分析

為驗證本研究所提出之機制可符合預期目標，本節針對國軍通資電部隊現行救災處理機制與本研究設計之具高度彈性之群體決策機制，比較兩者之各項特色如表四。

(一)運作

每逢天災發生，國軍支援救災任務時，往往時間急迫，通資電部隊如何快速且正確的決定通資電中心適切之架設地點及因應的開設方式，是完備救災通聯機制的關鍵所在。以現行機制而言，是利用參謀人員圖上選定或將決定權直接委託各通資電台、組長依據專業立場及現況，判斷可支援的通資電能量來共同商議架設地點，但通常遭遇地點不適當或耗時過久等問題。故本研究依權責賦予權重，設計具彈性的門檻值代理盲簽章機制，達成快速決策的目的，以利後續救災任務遂行。

(二)安全性及效率

救災任務執行時，通常礙於時間考量，均用明文通信，且地點通常不客觀，無論是主官決定或集合開會，在命令傳遞上都耗時費力，無法幫助指揮官迅速掌握能量，其他通資電能量無法有效發揮。本研究透過由憑證中心發送之訊息，進行團體成員合法性及代理性之認證，除確認身分及訊息的機密性外，妥善應用代理授權的機制，也能加快決策的下達，提高任務執行之效率。

表四 救災應變現行方法與研究機制比較表

運作和安全性	現行方法	本研究
運作	通常由指揮官特業(通資電兵科)參謀地圖上直接選定，但地點通常不甚理想；或將決定權直接委託各通資電台、組長依據專業立場及現況，判斷可支援的通資電能量來共同商議架設地點，惟人員此時太多分處於各管轄基地，無法即時決策。	本研究依權責賦予權重，設計具高度彈性之群體決策機制，供通資作業人員完成地形勘查後，能達成快速決策之目的，以利後續救災任務遂行。
安全性及效率	通常礙於時間考量，均用明文通信，且地點通常不客觀，無論是主官決定或集合開會，在命令傳遞上都耗時費力，無法幫助指揮官迅速掌握能量，其他通資電能量無法有效發揮。	本研究透過由憑證中心發送之訊息，進行團體成員合法性及代理性之認證，除確認身分及訊息的機密性外，妥善應用代理授權的機制，也能加快決策的下達，提高任務執行之效率。

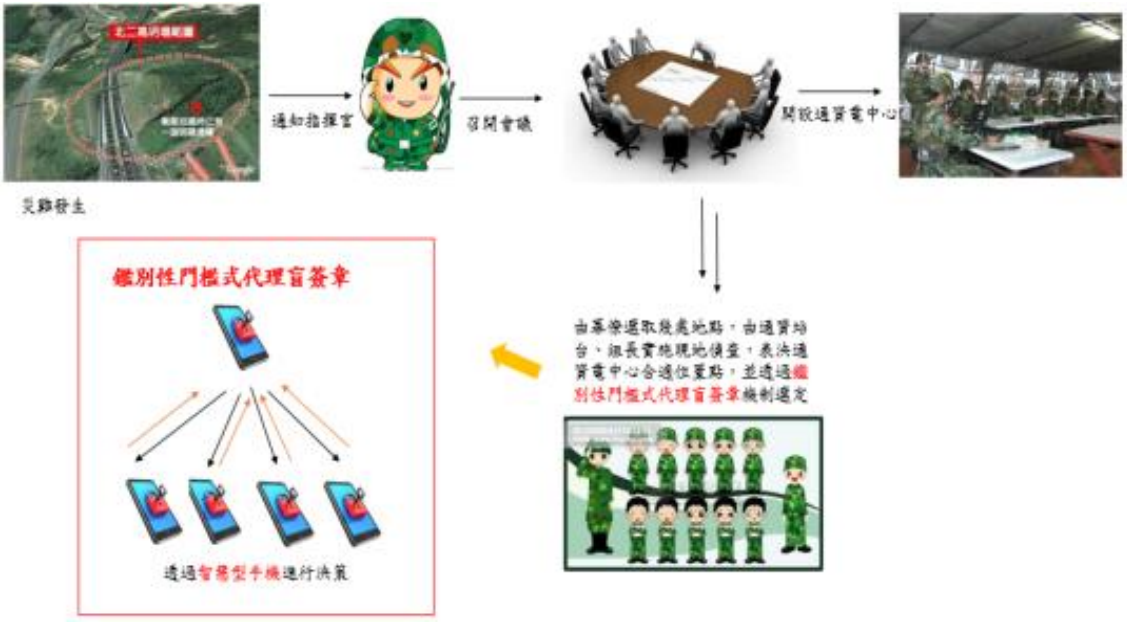
資料來源：作者研究整理。

未來發展建議

一、結合智慧型救災手機

國防應用方面以救災應變為例：突然發生天災人禍，軍團需開設救災指揮所，資電群配合架設通資電中心(如圖一)，有別於以往透過人工方式選定且無法即時討論及決策，如能建立一套機制，使各台、組長能迅速透過智慧型手機，配合權重賦予決定通資電中心合適位置(如圖十六)，便能節省開設通資電中心時間，部隊指揮官也能即時掌握通資電能量，以最快的速度將救災兵力迅速投入災區，減少人員傷亡及財產損失，相關說明如下：

圖十六 救災應變導入客製化示意圖



資料來源：作者繪製。

(一)客製化一套運作於國軍資訊應用平台上，且依權責賦予權重，具彈性的門檻值代理盲簽章機制。

(二)由於運用在手持式資訊平台上，具備有代理盲簽章的安全機制，使主官能在充裕的時間下做出完善的考量，有效掌握通資電能量；且各台長彼此之間不會受到影響，能根據其專業做出決定。

(三)運用手持式資訊平台，可迅速做出決定，避免耗費額外的時間，並立即將命令傳達給各台組長執行。

二、建構完整的災情資訊網

當災害發生時，現行災防法規定是由中央災害防救業務主管機關(內政部所成立的「中央災害應變中心」)向國防部提出申請；地方由直轄市、縣(市)政府及鄉(鎮、市)公所向所在直轄市、縣(市)後備指揮部轉各作戰區提出申請，故如何與民間單位結合，

以建構完整的災情資訊網是極為重要的一環。

目前中科院研製之災害行動決策支援系統(如圖十七)，以先前建構新竹市救災資訊系統之經驗為基礎，預劃導入國軍內部的災情資訊網，系統整合共通災害圖像並具即時提供自動化指派功能建議的行動決策支援功能，可將災情依嚴重性排序、分析需投入多少救災資源、將救災資源與災情進行配對並將災害防救計畫下傳給各式災害防救資源機動人員載台，達到整合救災資源，加速暨提升救災時效、減少救災資源浪費並減少救災人力經費支出的效益，期於未來從地方災害應變中心與所屬國軍的救災分區建構出軍民一致的災情共通圖像，完整的智慧化救災系統，進而推展部署至全國與全戰區，以利因應未來處理複合型災害的需求。

圖十七 災害行動決策支援系統示意圖

資料來源：國家中山科學研究院，〈資訊科技-災害行動決策支援〉，http://www.ncsist.org.tw/csistdup/products/product.aspx?product_Id=63&catalog=12，(檢索日期：2018年12月1日)。

三、強化身分驗證機制

隨著國軍朝向資訊化的目標邁進下，各項戰演訓任務幾乎都採用電腦來遂行戰場訊息傳遞情況下，如何提高系統安全度為現今所面臨到的難題。若能將國軍戰、演訓系統均導入多因子身分認證機制，如帳號密碼、OTP(One Time Password)、智慧卡及生物特徵等驗證方法，並配合橢圓曲線密碼系統、串流加密演算法，使其可抵禦竊聽、重送及偽冒等網路攻擊，未來可實際構改系統，測試其安全性及可行性。

結論

隨著網路技術與通訊科技不斷地推陳出新，無論是公營機關或私人企業，均有可能面臨資訊安全的衝擊，不僅是機關的正常運作、企業的永續經營受到影響，甚或國家的整體基礎建設及安全均面臨挑戰，資訊網路安全對國家的威脅性，已從過去的竊取情報逐漸進化成主動攻擊，沒有安全就沒有一切，在國軍整體發展中安全的議題逐漸成為關鍵。

本研究運用 ECC 密碼系統，整合代理盲簽章及(t, n)門檻式密碼系統的基礎架構，並導入可彈性調整權重概念，可滿足國軍行動式之救災資訊系統需求，縱整本研究，其貢獻如下：

一、 結合門檻式密碼系統，當解密者人數未達到門檻值時無法將密鑰解開，增加一套安全防護機制，為嶄新的秘密分享概念，可增加系統設計的安全性。

二、 利用代理盲簽章機制，當擁有權力者因有事無法行使權力時，可以將權力下授給眾多代理者使用，並運用盲化機制實施表決。

三、 將權重全新的概念導入代理盲簽章架構，使系統可依使用者需求，客製化調整權重，不因組織或任務調整需要重新設計系統，未來可適用於國軍的決策支援系統。

四、 可符合代理盲簽章、門檻式簽章及權重門檻式簽章等三種安全機制要求，從安全性及效益分析，本系統更具實用性。

五、 運用 ECC 密碼系統的特性，由於其運算速度比現行非對稱密碼系統的認證演算法快速，可供結合於手持式資訊設備或通行識別證之認證金鑰上。

綜合上述分析及建議，本研究藉由提出符合國軍特殊需求性之架構，盼能在整體系統之安全上貢獻一己之力，使我軍在提升戰備能量的同時也能夠保障訊息傳送之機密性，並降低系統負擔，提高資源使用率，在有限資源下達到最高的效益。

參考文獻

一、 王健民，〈國軍平時軍事行動之研究－以國軍救災角色定位與執行現況為例〉《黃埔學報》(高雄)，第 69 期，陸軍軍官學校，2015 年。

二、 林洋丞、滕春元，〈國軍防救災地理資訊系統實務應用之探討〉，《社團法人中華水土保持學會 102 年度年會》，第 39 卷第 4 期，1996 年。

三、 陳成宏、粘忠倚，〈學校組織變革的團體決策行為：「艾比里尼弔詭」與「團體迷思」的觀點分析〉《興國學報》，第 7 期，興國管理學院，2007 年。

四、 鄒磊，〈智慧防救災系統運用與發展－與新竹市合作建構防救災決策系統〉《陸軍通資半年刊》(桃園市)，第 128 期，陸軍通信電子資訊訓練中心，2017 年。

五、 蘇品長，〈群體導向的數位簽章技術之研究〉《全國管理碩士論文獎暨研討會論文集》，第 39 卷第 4 期，1996 年。

六、 國軍人才招募中心，https://rdrc.mnd.gov.tw/rdrc/iwa/iwa_b.aspx，2018 年 8 月 28 日。

七、 Desmedt, Y., and Frankel, Y., “Shared generation of authenticators and signatures t,” in Proc. of Advances in CRYPTO’91, 1991.

八、 NIST, “ Computer Security Division”, NIST Special Publication 800-57, 2012.

九、 Miller, V. S., “Use of Elliptic Curve in Cryptography,” Advance in Cryptography-Crypto’85, New York: Spring-Verlag, 1985.

十、 Pierre, J., and Peters., B. G, “Governance”, Politics and the State(New York: St. Martin's Press), 2000.

十一、 Sutikno, S., Effendi, R., and Surya, A., “Design and implementation of arithmetic processor F_2^{155} for elliptic curve cryptosystems,” in: The 1998 IEEE Asia-Pacific Conference on, Vol.32, No146, 1998.

十二、 Shamir, A., “How to share a secret,” Communications of the ACM, Vol.22, No11, 1979.

十三、 Stallings, W., “Cryptography and Network Security Principle and Practices”, Prentice Hall, 2004.

作者簡介

陳岳霖上尉，國防大學管理學院資訊管理學系 107 年班、國防大學管理學院資訊管理學系碩士 108 年班，曾任排長、人事官，現任國防大學管理學院資訊管理學系碩士學員。

曾健豪少校，陸軍官校電機系 95 年班，國防大學管理學院資訊管理學系碩士班 105 年班，曾任排長、有線電官，現任六軍團 584 旅通資連連長。

蘇品長上校，長庚大學電機工程博士，曾任預算財務官、程式設計官、資訊督導官，現任國防大學管理學院資訊管理學系教授。