# 匿名資訊分享與分析之研究

陳正鎔[1]　林文彬[2]　陳鳳美[3]　邱天嵩[4]　尹延齡[5]

[1]萬能科技大學資訊管理學系

[2,3,5]國防大學管理學院資訊管理學系

[4]亞東技術學院工業管理系

## 摘　要

隨著資訊網路之普及與廣泛使用，無形中乃爲大眾資訊交流之媒介，而資訊共享之安全、可靠性與隱私權保護課題益形重要。保護機制欠完善之資料共享系統恐有導致機密資料洩漏之慮，甚至影響供應者分享之意願，相對降低供應鏈資訊整合投資效益。因之，建立一匿名資訊分享供應鏈流程，降低資訊分享風險，爲提高我國資訊戰之關鍵建設之一。職是之故，爲減低前述風險，本研究以群體數位簽章系統原理爲基本架構，藉由離散對數假設之資訊安全基礎，提出一個簽章策略，俾使資訊供應者分享資訊時可獲得完全的隱匿性；同時資訊接收者又得以辨認眞僞，防制有心人員僞冒，確保資訊正確性與人員隱私之保障。研究結果可發現，本架構滿足個人隱密性、來源鑑定性、身分匿名性、資料保護性等安全流程機制，解決各組織成員因互信不足而使資訊無法充份分享之疑慮。因此，可作爲組織與供應鏈夥伴加速資訊分享、建立資訊安全分享系統之推進器，提昇資訊分享供需間之相關效益指標。

**關鍵詞**：資訊戰，資訊分享與分析中心，ElGamal 數位簽章，群體數位簽章。

# A Study of Anonymous Information Sharing

**Jonathan Chen[1]　Wen-Pin Lin[2]　Fun-May Chen[3]**
**Tien-Sung Chio[4]　Yen-Lin Yin[5]**

[1]Department of Information Management, VANUNG University of Science and Technology, Taiwan, R.O.C.

[2,3,5]Department of Information Management, National Defense University, Taiwan, R.O.C.

[4]Department of Industrial Management, Oriental Institute of Technology, Taiwan, R.O.C.

## ABSTRACT

With the popularity and widespread use of network, it is the media by which information is shared and exchanged to each member in a group. The topics such as security, dependability and privacy of shared information become more and more concerned. Without a tight protection, information sharing will take the risks of being intercepted and hence discourage one's willingness to share information with other members in the group. How to build an anonymous system to

hide the sender of shared information is an important factor to the success of information warfare.By means of group digital signature that based on Discrete Logarithms assuming, this research builds a mechanism to let the members not only share information anonymously, but also can identify whether a message comes from a group member or not; hence encourage the desire to share information among partners.

**Key words:** Information Warfare, Information Sharing and Analysis Center, ElGamal Digital Signature, Group Digital Signature

## 壹、前　言

### 一、研究動機

隨著資訊科技與網際網路之蓬勃發展，無形中形成企業提昇組織知識管理之競爭策略。其中，資訊分享爲推廣知識管理不可或缺之過程，故如何提供可靠之匿名資訊共享平台，提昇資訊之信度，進而降低隱私洩密之疑慮。

所謂知己知彼，百戰不殆，資訊分享之手段即是情報戰中洞燭先機不可或缺的重要一環，故情報資訊安全儼然成爲資訊作戰基礎建設（Information War Infrastructure）之關鍵成功因素（Critical Success Factor）。隨著時代的演進，資訊情傳手段已由傳統書信往來，演變爲資訊化的網絡傳遞。然情資來源之可信度攸關情報作戰之成敗，而情資傳送者之忠誠度亦是如此。

職是之故，情資傳遞過程中同時保障所獲情資之正確性及分享者之安全性，是資訊安全值得深思的議題。有鑑於此，本研究旨在針對情資分享者與資訊分享與分析中心（Information Sharing and Analysis Center, ISAC）間，建立一個安全的確認機制，確保組織在未來情報作戰能勝兵先勝。

### 二、研究目的

敏感性資訊傳遞，除注重機密性外，也強調不可受任何僞造或竄改。在機密性部分，任何一種安全性密碼系統如 RSA (Nitaj, 2006)、ElGamal (Duursma and Park, 2006)、DES（Wyseur et al., 2007）、AES（Shang et al., 2006）等均可以達此目的。在防範僞造或竄改則可有賴數位簽章。

傳統數位簽章（Digital signature）技術即是確保電子資料傳遞過程中不受到僞造或竄改，並確認通訊雙方客户身份，作爲事後不可否認的證據，進而確保資料一致性及不可否認性等特性。惟在匿名資訊傳遞上，仍無法同時保障所獲情資之正確性及情報傳送者之安全性。故情報傳遞者在蒐獲情資後，分享給 ISAC 時，除需以密文傳送外，ISAC 可辨識情報來源，惟接收人員解得明文時，亦無法得知情報傳遞者之確切身分。如此，儘管組織內部有心人士預找尋公告人員，亦可確保其人身安全，進而降低資訊洩密風險，提昇資訊分享意願。有鑒於此，爲滿足上述情傳需求，避免危安風險疑慮，本研究嘗試使用 Lee and Chang（1998）所提出之群體數位簽章（Group Digital Signature）系統以同時滿足傳送者匿名與 ISAC 確認之要求。於是，首先綜結上述一個完善的情資傳遞機制至少需滿足下列特性：

(一) 秘密性（Secrecy or Privacy）

防止非法之接收者得知由資訊共享者所傳遞之情報資料明文。

(二) 鑑定性（Authenticity）

確定所獲情資來源之合法性，亦即此情資確由發送方所發送。而非他人所僞

造，或利用以前的訊息來重送。

(三) 完整性（Integrity）

確保情資沒有被有意或無意之竄改，及被部分取代、加入或刪除等等。

(四) 匿名性（Anonymity）

傳送者傳送電子文件，接收者可確定該訊息係合法成員所發出，惟不知是那一位所發送。

(五) 保護性（Protection）

除傳送情資者外，組織內其他成員無法根據所攔截之訊息而整理出該文件係那一位傳遞者所傳送（除非組織中只有二位成員）；組織之部門主管亦無法於多項式時間內計算出發文者之所有秘密金鑰。因之，組織之主管沒有能力以特定傳送者之身分傳輸訊息。

(六) 無關聯性（Unlinkability）

情資接收單位無法追蹤所簽文件與傳送簽章者的關係，日後文件內容與簽署文公布出來，簽章者也無法追蹤文件與當時他所簽屬的文件之間的關係。

(七) 追蹤性（Traceability）

倘若發現可疑情資時，接收單位持該情資之單位主管反映，單位主管可據以查出係由那一位傳送者所發出。

由上述資訊安全分享特性，似符合匿名分享需求，惟前述所提及的 Lee and Chang 之演算法，卻有以下風險：

(一) 攻擊者可偽造合法簽章：

攻擊者僅需使用一個虛構的秘密金鑰，即可偽造有效之群體數位簽章。

(二) 追蹤可疑情資來源時會導致成員傳送者曝光：

在質疑某情資來源之合法性，欲找出發送該情資人員時，需公布一些相關資訊，從而導致被追蹤之傳送者曝光。

(三) 無法有效管理傳送者密鑰：

系統建置時，所遴選之傳送者擇一秘密金鑰，再計算出相對應之公開金鑰集中保管。惟與該傳送者身份資訊毫無關係，因而增加金鑰管理上之困難度。

因此，本研究可改善上述缺失，故以 ElGamal 之密碼系統原理爲基本架構，藉由離散對數之假設作爲安全基礎，提出一個可變式群體數位簽章機制，俾利應用於匿名情資傳遞系統中，確保安全無虞。

## 貳、文獻探討

### 一、資訊戰（**Information Warfare**）

從古至今，「資訊戰」之釋義眾說紛云。自二十世紀末，西方強權國家－美國，掀起了各國重視軍事事務革新之潮流，促進資訊戰及資訊作戰在同一時期迅速發展。至今，大部分國家仍賡續 1980 至 1990 年代美軍對資訊戰與資訊作戰之定義，將資訊作戰（Information Operations, IO）界定爲廣義層面的資訊攻防運用，而將資訊戰（Information Warfare, IW）界定爲專業的軍事行動。然而，美國國防部於 1998 年頒佈之空軍資訊作戰準則中，對資訊作戰及資訊戰的定義（曾章瑞、陳志誠、張榮鋒，2006），如下所述：

(一)資訊作戰（**Information Operations, IO**）

不論平時或戰時，各種影響敵方資訊與資訊系統之手段，並可保護我方資訊與資訊系統之作爲。

(二) 資訊戰（**Information Warfare, IW**）

在危機或衝突階段，對於特殊的敵人，爲達成特定目的，所實施之資訊作戰。

然而，隨著二十一世紀的來臨，美軍新一代作戰型態也納入了資訊作戰，且於 2006 年 2 月 13 日公佈之聯合作戰範疇中，修訂了資訊作戰之定義。另一方面，準則中定義爲資訊作戰的資訊戰名詞也同步刪除，改爲單元化的資訊作戰。換言之，資訊戰已不再是狹義的軍事術語，而是對戰爭類型統稱之廣義名詞。相對而

言，資訊作戰已明確定義爲軍事作戰型態之關鍵元素，不再僅是界定爲網路科技或是安全技術之運用而已。然而，中共則將所謂資訊戰解釋成「訊息戰」，於 2002 年「中國軍事百科全書」（呂文創，2005）中詮釋信息戰就是剝奪、利用、破壞或摧毀敵方信息、信息系統和信息作戰能力，同時保護和充分利用乙方信息、信息系統和信息作戰能力而採取各種行動。其目標在於截取和確保信息優勢，充分掌握信息的獲取、控制權和使用權，並由此取得在戰爭中的主動權和有利地位。若依時間，又可分爲平時信息戰和戰時信息戰。平時信息戰是指和平時期敵對雙方在政治、經濟、科技、外交、文化、軍事等領域普遍進行的信息對抗。戰時信息戰是指在戰爭時期敵對雙方所實施的信息戰，包括運用多種手段攻擊敵方信息和信息系統，破壞或切斷敵方信息流，影響、削弱、摧毀敵信息作戰能力，同時保護乙方信息作戰能力。

相較於美國與中共定義資訊戰之不同見解，參照我國「國軍軍語辭典」之詮釋，整體而言，資訊戰定義可歸納如下：「企圖以防護、利用、破壞、拒絕等手段，影響敵人之資訊、資訊化處理及資訊系統等來源，而防禦本身之資訊、資訊化處理及資訊系統，以取得資訊之優勢及目標所採取之各項行動」。

## 二、資訊分享與分析中心（**Information Sharing and Analysis Center, ISAC**）

資訊分享與分析係一涵蓋領域廣泛且錯綜複雜之概念。1999 年起，美國白宮已主導成立約 14 多個行業別之 ISAC（Sabo, 2004），其推動成效也已引起英國、歐盟等國家均設置其 ISAC。因此，相較於我國日益成熟的數位資訊化社會需求，推動資通安全發展，已是相當值得學習的借鏡。

有鑒於國內資通安全發展現況及未來趨勢，在「建立我國通資訊基礎建設安全機制計畫(2005～2008)」中，訂定的 10 項發展目標之第 2 項即明定：「建置政府及重要基礎建設之資訊分享及分析中心，提昇國家競爭力」。其中，資訊安全防護中心（Security Operation Center，簡稱 SOC）之最終目標即是資訊分享與分析中心（Information Sharing and Analysis Center，簡稱 ISAC）之推廣（樊國楨、林樹國、歐崇明，2006）。因此，行政院自 90 年 1 月 17 日第 2718 次院會通過「建立我國通資訊基礎建設安全機制計畫」（行政院國家資通安全會報，2004）後，相關部門諸如行政院資通安全會報技術服務中心也開始著手執行「資安監控中心」計畫。換言之，若再進一步導入 ISAC 之精神，並參考先進國家之執行成效，相信對於我國防範資通安全犯罪事件之預防應有相當正面的助益。

然而，若某種型態的訊息對於維護資通安全工作特別有價值，而且也較容易由不同的組織或機構間加以分享。政府機構與民間企業則可考量將分享的重要資訊涵蓋其內，例如

(一) 已知的風險評估

假如單位內曾經對其組織本身的危安進行評估並研析評估資料，則此單位必然更可以有效地確保其單位通資系統之安全，同時可將其先前所存在的弱點之性質透過知識管理體系分享給其他子單位，以節?預防的時間及風險：但是，若單位資訊管理部門恐懼缺失的改善不盡完善將面臨檢討時，勢必又將抱持得過且過心態，進而間接影響此種資訊分享的意願。

(二) 已知的威脅攻擊與預防事件

企業資訊管理部門具備科技管理與網路監控之能量，並兼負單位資訊安全維護之最後防線。惟僅限人力資源掌控仍有顧

此失彼之疑慮，加上資訊安全危機意識不足，恐導致危安事件發生。因之，若資訊部門或所屬單位接獲相關資安事件時，應設法對此一資訊加以篩選、分析，然後分送並回報給其他可能會遭受影響之單位。如此，可不提及單位名稱之前提下，適時掌握防護有效契機。

我國行政院資通安全會報技術服務中心爲預防通資安全攻擊事件，已規劃建置國家資通安全監控中心（National Security Operation Center, N-SOC）之 5 年計畫（國家資通安全會報技術服務中心，2002）。惟 SOC 僅是整體資訊安全作爲之一小部份，故若能整合各個產業別之 ISAC，藉以研判可能之攻擊作爲，並建置資訊安全攻防模型，結合各產業之 ISAC 與 N-SOC，則可達事半功倍之綜效。因之，推廣「資訊分享與分析中心」爲刻不容緩的工作。

## 三、群體數位簽章（**Group Digital Signature**）

1991 年，Chaum 及 van Heijst 提出群體簽章（Group Signature）的概念。在群體簽章中，該群體的任何一位成員可以代替整個群體來簽署有效的簽章。而接收單位在驗證該群體簽章時並無法得知眞正個別簽署者爲何。另外，群體簽章必須滿足以下特性。

(一) 不可僞造性（**Unforgeability**）

只有組織中合法的成員才可以代替該單位來簽署有效簽章。

(二) 可辨明性（**Exculpability**）

沒有任何一位組織成員或是群體管理者可以代替其他成員簽署全體簽章。

(三) 無法連結性（**Unlinkability**）

給定許多有效但不同的群體簽章，但無法找出哪些簽章是由一位成員所簽署的。

(四) 匿名性（**Anonymity**）

驗證者沒有辦法從簽章中推導出成員的身分。

(五) 可追蹤性（**Traceability**）

群體管理者可以解開有效群體簽章內的重要訊息來找出眞正的簽署者。

(六) 抗合謀性（**Coalition-resistance**）

群體成員的一個合謀子集不能產生一個有效的不可追蹤之簽署。

## 四、ElGamal 數位簽章

1985 年，ElGamal 提出一個植基於解離散對數（discrete logarithm）之困難度上的數位簽章法。

(一) 系統參數

設系統（或網路中）存在一個很大的質數 $p$ 以及一個 $p$ 模之原根 $g$，使得解離散對數成爲相當困難的問題

1. 私密金鑰：簽章者 A 任選一個整數 $x$，並滿足 $1< x <p-1$，作爲其私密金鑰。
2. 公開金鑰：簽章者 A 計算出其公開金鑰爲 $y = g^x \bmod p$。

(二) 簽署階段

如果傳送者 A 欲簽署訊息，且滿足 $1 \le m \le p-1$，便可執行下列步驟傳送者 A 先任選一個整數 $k$，滿足 $GCD\ (k, (p-1))=1$

步驟一：傳送者 A 計算 $r = g^x \bmod p$

步驟二：傳送者 A 求出

$s = k^{-1}(m-xr) \bmod (p-1)$ 或

$m = xr + ks \bmod (p-1)$

步驟三：傳送者 A 計算出相對應的數位簽章(r, s)

(三) 驗證階段

傳送者 A 將訊息 $m$ 與數位簽章送給接收單位 $B$，當 $B$ 收到 $m$ 與數位簽章(r, s)後，便利用傳送者 $A$ 的公開金鑰 $y$ 來進行驗證步驟，驗證 $g^m ? \equiv y^r r^s \pmod p$，

其中 $(g^m = g^{xr} g^{ks} = g^{xr+ks} \bmod p)$

如果上述成立，接收單位 $B$ 便確定(r.s)確

實爲傳送者 A 對訊息 $m$ 所簽署的數位簽章，反之則屬非法簽署。

## 參、系統架構與建置

本簽章系統架構係闡明 ElGamal 之概念，然亦添加我們之獨特見解，用以說明群體簽章具有資訊分享與分析之功能，而本架構概分爲下列四個部份：

一、系統參數

(一) 系統參與者

1. 註冊中心，爲本系統之最高權限核心中心（Power Authority, PA）。
2. 組織內所有使用本系統實施資訊分享之組織成員 $g_i$（group members），也就是簽章使用者。
3. 資訊分享與分析中心(Information Sharing and Analysis Center, ISAC) 即爲驗證部門 V（Verifier）。

(二) 運作模式

組織成員（使用者）欲回傳情資給資訊分享與分析中心（ISAC），透過取得公開金鑰（public key）將訊息實施加密、簽署及驗證（加解密流程如第三章所述），且運作時透過秘密金鑰（private key）之運用，可協助判別來源之合法性，又兼具確保身分隱私之功能，有效達到安全之匿名資訊分享與分析之目的（運作模式如圖 1）。

二、模式架構

本架構建立，又分爲二個階段

(一) 註冊中心（**PA**）設定：

PA 選取滿足下列式子之大質數 $M$

$$M = 4m_1m_2+1 \quad \text{.....(1)}$$

其中 $m_1$，$m_2$，亦均爲大質數，且 $4|m_k-3$，$k=1,2$

令 $h = m_1m_2$ .....(2)

再選取模(modulo) $M$ 其序(order)爲 $h$ 之一數 $d$，其中 $M, h, d$ 爲 PA 之公開金鑰，而 $m_1$, $m_2$ 爲其秘密金鑰。

(二) 組織成員建立階段：

本階段又再細分爲二部分：

1. 經註冊合格之組織成員向 **PA** 註冊：

經遴選合格之組織成員 $g_i$ 選取二數，計算 $p, q$？ $z_h^*$

$$e \equiv d^q \pmod{M} \quad \text{.....(3)}$$

$$t_1 \equiv d^p \pmod{M} \quad \text{.....(4)}$$

然後進行下列步驟：

(1) 選取一數 $a_1 \in z_h^*$，計算

$$t_2 \equiv d^{p^2} \pmod{M} \quad \text{.....(5)}$$

$$x_1 \equiv d^{a_1} \pmod{M} \quad \text{.....(6)}$$

$$x_2 \equiv d^{pa_1} \pmod{M} \quad \text{.....(7)}$$

$$t_1+t_2 \equiv p(x_1+x_2)+a_1z_1 \pmod{h} \quad \text{.....(8)}$$

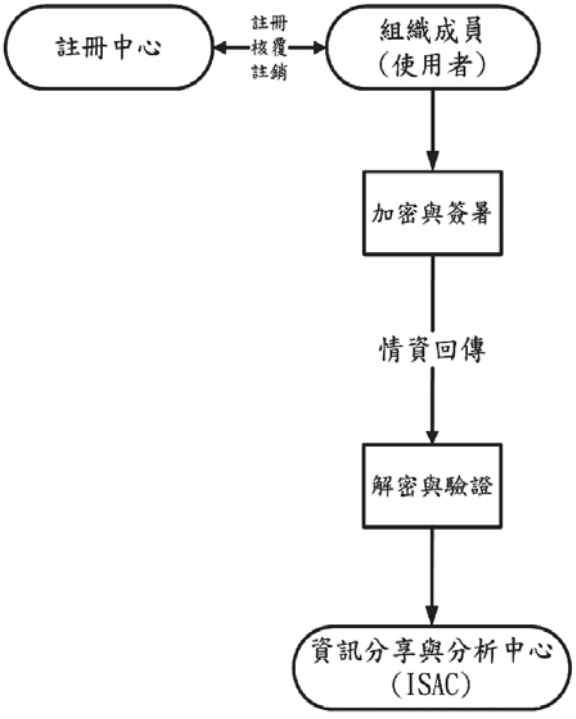


圖 1　系統基本運作模式

(2) 選取一數 $a_2 \in z_h^*$，計算

$$e_1 \equiv d^{q^2} \pmod{M} \quad \text{.....(9)}$$

$$x_3 \equiv d^{a_2} \pmod{M} \quad \text{..... (10)}$$

$$x_4 \equiv d^{q a_2} \pmod{M} \quad \text{.....(11)}$$

$$e+e_1 \equiv q(x_3+x_4)+a_2 z_2 \pmod{h} \quad \text{.....(12)}$$

(3) 選取一數 $a_3 \in z_h^*$，計算

$$t_3 \equiv (t_1 t_2 d)^q \pmod{M} \quad \text{..... (13)}$$

$$x_5 \equiv d^{a_3} \pmod{M} \quad \text{.....(14)}$$

$$x_6 \equiv (t_1 t_2 d)^{a_3} \pmod{M} \quad \text{.....(15)}$$

$$t_3 \equiv q(x_5+x_6)+a_3 z_3 \pmod{h} \quad \text{..... (16)}$$

(4) 計算

$$D \equiv (1+p+p^2)(q+q^2) \pmod{M} \quad \text{.....(17)}$$

傳送 $\{D, e, e_1, t_k, z_k, x_w\}$ 予 PA，其中 $1 \le k \le 3$, $1 \le w \le 6$。

2. **PA** 核覆組織成員之相關金鑰：

PA 收到組織成員 $g_i$ 所傳送之訊息後，進行下列步驟：

(1) 驗證

$$d^{t_1+t_2} \equiv t_1^{x_1+x_2 z_1} x_1 \pmod{M} \quad \text{.....(18)}$$

$$t_1^{t_1+t_2} \equiv t_2^{x_1+x_2 z_1} x_2 \pmod{M} \quad \text{.....(19)}$$

(2) 驗證

$$d^{e+e_1} \equiv e^{x_3+x_4 z_2} x_3 \pmod{M} \quad \text{.....(20)}$$

$$e^{e+e_1} \equiv e_1^{x_3+x_4 z_2} x_4 \pmod{M} \quad \text{.....(21)}$$

(3) 驗證

$$D^{t_3} \equiv e^{x5+x6 z_3} x_5 \pmod{M} \quad \text{.....(22)}$$

$$(t_1 t_2 d)^{t_3} \equiv t_3^{x_5+x_6 z_3} x_6 \pmod{M} \quad \text{.....(23)}$$

如果式子(19)—(23)均成立，則計算

$$U^2 \equiv D \pmod{M} \quad \text{.....(24)}$$

將{u}經由安全管道(secure channel)傳送給組織成員 $g_i$，其中 $p, q$ 爲其秘密金鑰，$u$ 爲其半秘密金鑰(semi-private key)，而 $t_1, e$ 則爲其半公開金鑰(semi-public key)。

三、群體簽章與驗證

(一) 組織成員簽章之產生

假定組織成員 $g_i$ 欲對訊息 $s$ 予以簽章，其演算法步驟如下：

1. 選取一數 $b \in z_h^*$，計算

$$F_1 \equiv (b+1)^2 \pmod{h} \quad \text{.....(25)}$$

在無法將合成數 $h$ 因數分解之前提下，如果 $F_1$ 模 $h$ 之平方根爲可行解，則重覆本小步驟 1.，直至無可行解爲止。

2. 選取一數 $p_1 \in z_h^*$，計算

$$D_1 \equiv d^b \pmod{M} \quad \text{.....(26)}$$

$$D_2 \equiv d^{b^2} \pmod{M} \quad \text{.....(27)}$$

$$E_1 \equiv d^{p_1} \pmod{M} \quad \text{.....(28)}$$

$$E_2 \equiv d^{bp_1} \pmod{M} \quad \text{.....(29)}$$

$$D_1+D_2 \equiv b(E_1+E_2)+p_1 f_1 \pmod{h} \quad \text{.....(30)}$$

3. 選取一數 $p_2 \in z_h^*$，計算

$$D_3 \equiv D_1 d \pmod{M} \quad \text{.....(31)}$$

$$D_4 \equiv d^{F_1} \pmod{M} \quad \text{.....(32)}$$

$$E_3 \equiv d^{p_2} \pmod{M} \quad \text{.....(33)}$$

$$E_4 \equiv d^{(b+1)p_2} \pmod{M} \quad \text{.....(34)}$$

$$D_3+D_4 \equiv (b+1)(E_3+E_4)+p_2 f_2 \pmod{h} \quad \text{.....(35)}$$

4. 選取一數 $b_1 \in z_h^*$，計算

$$F_2 \equiv b_1^2 \pmod{M} \quad \text{.....(36)}$$

如果不能因數分解 $h$，$F_2$ 模 $h$ 之平方根爲可行解則重覆本小步驟 4.，直至無可行解爲止，然後計算

$$u+F_3 \equiv b_1 \pmod{h} \quad \text{.....(37)}$$

5. 選取一數 $p_3 \in z_h^*$，計算

$$D_5 \equiv D_1^p \pmod{M} \quad \text{.....(38)}$$

$$D_6 \equiv D_5^p \pmod{M} \quad \text{.....(39)}$$

$$E_5 \equiv D_5^{p_3} \pmod{M} \quad \text{.....(40)}$$

$$E_6 \equiv D_5^{pp_3} \pmod{M} \quad \text{.....(41)}$$

$$N+D_5+D_6 \equiv p(E_5+E_6)+p_3 f_3 \pmod{h} \quad \text{.....(42)}$$

6. 選取一數 $p_4 \in z_h^*$，計算

$$D_7 \equiv D_1 D_5 D_6 \pmod{M} \quad \text{.....(43)}$$

$$D_8 \equiv D_7^p \pmod{M} \quad \text{.....(44)}$$

$$D_9 \equiv D_8^p \pmod{M} \quad \text{.....(45)}$$

$$E_7 \equiv D_7^{p_4} \pmod{M} \quad \text{.....(46)}$$

$$E_8 \equiv D_8^{p_4} \pmod{M} \quad \text{.....(47)}$$

$$D_8+D_9 \equiv p(E_7+E_8)+p_4 f_4 \pmod{h} \quad \text{.....(48)}$$

7. 選取一數 $p_5 \in z_h^*$，計算

$$D_{10} \equiv D^{bu} \pmod{M} \quad \text{.....(49)}$$

$$D_{11} \equiv D_{10}^{bu} \pmod{M} \quad \text{.....(50)}$$

$$E_9 \equiv d^{p_5} \pmod{M} \quad \text{.....(51)}$$

$$E_{10} \equiv D_9^{bu} \pmod{M} \quad \text{.....(52)}$$

$$D_{10}+D_{11} \equiv bu(E_9+E_{10})+p_5 f_5 \pmod{h} \quad \text{.....(53)}$$

8. 傳送$\{N, F_{k1}, D_{k2}, E_{k3}, f_{k4}\}$予接收者（或驗證者）$g_i$，其中

$1 \le k_1 \le 3, 1 \le k_2 \le 11, 1 \le k_3 \le 10, 1 \le k_4 \le 5$

(二) 組織成員簽章之驗證

ISAC 驗證者，在收到組織成員回傳之訊息時，進行下列驗證之演算法步驟：

1. 計算

$$d^{D_1+D_2} \equiv D_1^{E_1+E_2} E_1^{f_1} \pmod{M} \quad \text{.....(54)}$$

$$D_1^{D_1+D_2} \equiv D_2^{E_1+E_2} E_2^{f_1} \pmod{M} \quad \text{.....(55)}$$

2. 計算式子(31)以及

$$d^{D_3+D_4} \equiv D_3^{E_3+E_4} E_3^{f_2} \pmod{M} \quad \text{.....(56)}$$

$$D_3^{D_3+D_4} \equiv d^{F_1(E_3+E_4)} E_4^{f_2} \pmod{M} \quad \text{.....(57)}$$

3. 計算

$$D_1^{N+D_5+D_6} \equiv D_5^{E_5+E_6} E_5^{f_3} \pmod{M} \quad \text{.....(58)}$$

$$D_5^{N+D_5+D_6} \equiv D_6^{E_5+E_6} E_6^{f_3} \pmod{M} \quad \text{.....(59)}$$

4. 計算式子(43)以及

$$D_7^{D_8+D_9} \equiv D_8^{E_7+E_8} E_7^{f_4} \pmod{M} \quad \text{.....(60)}$$

$$D_8^{D_8+D_9} \equiv D_9^{E_7+E_8} E_8^{f_4} \pmod{M} \quad \text{.....(61)}$$

5. 計算

$$d^{D_{10}+D_{11}} \equiv D_{10}^{E_9+E_{10}} E_9^{f_5} \pmod{M} \quad \text{.....(62)}$$

$$D_{10}^{D_{10}+D_{11}} \equiv D_{11}^{E_9+E_{10}} E_{10}^{f_5} \pmod{M} \quad \text{.....(63)}$$

6. 如果式子(54)—(63)均成立，則表示情資確係發自於組織之成員無誤。

(三) 追蹤可疑情資來源

由於資訊分享時，ISAC 接收人員只能確認訊息來源之合法性而無法知悉發訊者之身分，故組織成員有心人士則可能利用匿名性以發送不實情資，不得不防。因此在發現高度可疑情資時，可由 PA 追查出簽署問題文件之成員。其作法如下：

1. 驗證式子(54)—(63)，如果該等式均成立，則接受仲裁，否則，拒絕接受。
2. 依據式子(25)解出 $b$ 之 4 個根 $y_k$, $1 \le k \le 4$，將此 4 個根分別代入式子(26)，找出正確之根。
3. 依據式子(36)解出 $b_1$ 之 4 個根 $c_k$，將此 4個根分別代入式子(37)，得出 $u$ 之 4 個根 $u_k$，再尋找半秘密金鑰爲 $u_k$ 值之組織成員 $g_k$, $1 \le k \le 4$ 。
4. 依據式子(26)與(38)，計算

$$d^{p} \equiv D_5^{b^{-1} (\mathrm{mod}\, h)} \pmod{M} \quad \text{.....(64)}$$

尋找半公開金鑰 $t_1$，符合式子(64)之組織成員，至此，該筆有爭議之情資係爲那一位內部成員所發出可確定無疑。

## 四、 系統安全性分析

根據 Maurer-Yacobi 之理論（MURAKAMI, 2005），二個質因數係經過審慎的挑選，使得 PA 可對此二質因數做運算，而在不知道合成數 $M$ 之組成因數的狀況下，則無法 $M$ 對做離散對數（Modulos）運算以分解出$r_1$，$r_2$，因爲其困難度等同（或超過）分解因數之困難。很明顯地，企圖破解 PA 秘密金鑰之難度與 *RSA* 之假設相同。以下我們區分爲於組織成員註冊階段時，該成員不誠實註冊其秘密金鑰或進行僞造（Forgery）攻擊等二種情形分別予以研析。模擬幾種可能之攻擊方式，以考驗本系統之安全性：第一種爲組織成員不誠實註冊；第二種爲非成員密謀竄改情資；第三種爲組織成員意圖變更私鑰；第四種乃非成員或組織非法接收人員，嘗試破解組織成員之匿名身份。以上數種攻擊方式對系統之影響分析於後。

攻擊法一：組織成員不誠實註冊。

1. 分析

假定某組織成員，於註冊時不誠實，意圖讓式子(4), (5)之 $p$ 值不相同或式子(3)與(9)之 $q$ 值不相同，俾便日後發送不實情資時免於遭到稽核，此攻擊得逞之可能性趨近於零。

2. 定理 1

式子(4)與(5) $p$ 值相同之機率爲 $1-\frac{1}{h}$

3. 證明

假定 $q$ 值不相同，攻擊者任選與 $p$ 相異之二數 $p', p'' \in z_h^*$，將式子(5), (7), (8)改成下列式子

$$t_2' \equiv d^{p'} \pmod{M} \quad \text{.....(65)}$$

$$x_2' \equiv d^{p''} \pmod{M} \quad \text{.....(66)}$$

$$t_1 + t_2' \equiv p(x_1 + x_2') + a_1 z_1 \pmod{h} \quad \text{.....(67)}$$

解出式子(67) $z_1$ 值之後，我們將式子(67)轉換成

$$p(t_1 + t_2') \equiv p^2(x_1 + x_2') + p a_1 z_1 \pmod{h}$$

.....(68)

將式子(68)全等式右邊之 $p^2$ 以 $p'$ 取代，$p$ 以 $p''$ 取代，則

$$p(t_1 + t_2') \equiv p'(x_1 + x_2') + p'' a_1 z_1 \pmod{h}$$

.....(69)

在式子(69)中，由於所有參數均爲事先律定，非攻擊者所能決定，該式子成立之機率爲$\frac{1}{h}$，同理，在式子(65)與(66)之前提下，式子(67)與(69)能解出相同 $z_1$ 之機率亦爲$\frac{1}{h}$，故式子(4)與(5) $p$ 值相同之機率爲1-$\frac{1}{h}$，由此得證。

由定理 1 知，式子(3)與(9) $q$ 值不同之機率亦爲 $\frac{1}{h}$。綜合上述討論，內部成員不誠實註冊是難以成功的。

攻擊法二：非法人員攔截到回傳情資後，欲竄改訊息內容。

1. 分析

假定敵人欲將式子(42)之 $N$ 值竄改而於網路上攔截內部成員 $g$ 對外所有傳送之訊息，對攻擊者而言在式子(42)中 $p$ 與 $p_3$ 皆爲未知數，要僞造 $N$ 亦將面臨計算離散對數之瓶頸。

攻擊法三：組織成員意圖變更私鑰，規避 PA 追查。

1. 分析

內部成員 $g_0$ 針對式子(17)企圖更改其秘密金鑰 $p$（或 $q$），如果 $D$ 值不變動，要解出對應之 $q$（或 $p$）值需面臨因數分解難題；或任意選取 $p$ 與 $q$ 二數，其所產生之 $D$ 值對其而言仍爲不可控制之變數，因之要解出式子(24) $u$ 之值會有因數分解之困擾，因而無從得逞。

攻擊法四：非法人員或組織內部非合法成員，欲假某組織成員之名發送不實情報。

1. 分析

式子(3)至(7)；(9)至(11)；(13)至(15)均是離散對數的問題，此外，在式子(8)、(12)、(16)與(17)中，每個式子各有二個未知數。因此，*PA* 欲解析內部成員之秘密金鑰 $q$、$p$ 是有困難的。

## 肆、結　論

本文藉由可變式群體數位簽章（Convertible Group Signature）可解決機敏單位資訊分享與分析面臨之難題。且鑑於資訊分享作業之隱私性及匿名性需求，透過學理之安全性分析驗證，可提供一套符合全方位安全需求之資訊分享密碼模組，藉此防堵當前資安防護之嫌隙。然而，儘管近期相關先進學者之研究已不在少數，但對於與時俱進之通資安全需求多有顧此失彼之遺憾。故爲達到「全方位安全」之基本要件，本文導入離散對數與因數分解雙重複雜度之假設，設計出群體數位簽章密碼模組，並應用於 ISAC 情資傳遞作業上，以利建構一個理想的資訊分享與分析平台，進而強化我國資訊戰中之資訊安全基礎建設，以期未來現代化資訊戰中能適時掌握情資，制敵機先。

## 參考文獻

行政院國家資通安全會報，2004。建立我國通資訊基礎建設安全機制計畫（九十四年至九十七年），下載於 http://www.cga.gov.tw/sea/doc/p12_4.pdf（2004 年 3 月 1 日）。

呂文創，2005。1985-2004 年共軍信息戰發展之研究，國防管理學院國防決策科學研究所碩士論文。

國家資通安全會報技術服務中心，2002。e-Taiwan 計畫之建置安全的資訊通信環境計畫摘要，簡報資料。

曾章瑞、陳志誠、張榮鋒，2006。認識資訊戰、資訊作戰及政府應有軍政作爲，資通安全分析專論，T95020。

樊國楨、林樹國、歐崇明，2006。資安監控中心之終極目標：資訊分享與分析中心初探，資通安全專論，T95002。

Chaum, D. and van Heyst, E., 1991. Group Signatures. In: Advances in Eurocrypt' 91, LNCS 547, 257-265.

Duursma, I. M. and Park, S.K., 2006. ElGaal type signature schemes for n-dimensional vector spaces , International Association for Cryptologic Research.

ElGamal, T., 1985. A public key cryptosys-

tem and a signature scheme based on discrete logarithms, IEEE Transactions on Information Theory ,Vol. IT-31, No. 4, 469- 472.

Lee, W. B. and Chang, C. C., 1998. Efficient Group Signature Scheme Based on Discrete Logarithm, IEE Proceedings － Computers and Digital Techniques, Vol. 145, No. 1, 15-18.

MURAKAMI, Yasuyuki. and KASAHARA, Masao., 2005. Murakami-Kasahara ID-based Key Sharing Scheme Revisited－ In Comparison with Maurer － Yacobi Schemes International Association for Cryptologic Research.

Nitaj, Abderrahmane., 2006. Cryptanalysis of RSA with constrained keys, International Association for Cryptologic Research.

Shang, D., F. Burns, and A. Bystrov, 2006. High-security asynchronous circuit implementation of AES, Computers and Digital Techniques, IEE Proceedings, Vol. 153, No. 2, 71-77.

Sabo, J. T., 2004. Managing Trust in Critical Infrastructure Protection Information Sharing System, Highlights of the Information Security Solutions Europe 2004 Conference, 271-280.

Wyseur, B., W. Michiels, P. Gorissen, and B. Preneels, 2007. Cryptanalysis of White-Box DES Implementations with Arbitrary External Encodings, International Association for Cryptologic Research.