寫入-讀出法團秘密分享技術

A write-read coterie secret sharing scheme

江振瑞
Jenh-Ruey Jiang

玄奘人文社會學院
資訊管理系
Hsuan Chuang College
Information Management Department

<<摘要>>

在此篇論文中，我們利用**不可超越寫入-讀出法團**(nondominated write-read coterie)來實現**秘密分享技術**(secret sharing scheme)。一個秘密分享技術必須滿足**秘密重建**(reconstruction)特性及**完美**(perfect)特性，我們將證明利用不可超越寫入-讀出法團產生的**存取結構**(access structure)，可以滿足上述之秘密分享技術的二個特性。我們並將所提的技術與一些以**法定人數集合系統**(quorum system)為基礎的方法加以比較，如同我們於論文中指出的，因為寫入-讀出法團比法定人數集合系統更具一般性，這使得我們所提出的秘密分享技術更具有彈性，能夠達成更低的通訊成本(communication cost)及更高的擷取度(availability)。

關鍵字：存取結構，不可超越寫入-讀出法團，秘密分享技術，法定人數集合系統

A write-read coterie secret sharing scheme

Abstract

In this paper, we utilize *nondominated write-read coteries* to implement a *secret sharing* scheme. A secret sharing scheme must satisfy (1)the *reconstruction* property and (2)the *perfect* property. We will prove that the *access structure* derived from a nondominated write-read coterie can satisfy the above-mentioned properties of the secret sharing scheme. We also compare our scheme with the ones utilizing *quorum systems*. As we will show, our scheme is more flexible than related ones since write-read coteries are more general than quorum systems. Thus, our scheme can achieve lower communication cost and higher availability.

Keywords: access structure, nondominated write-read coterie, secret sharing scheme, quorum system

壹、緒論

繼美國各州（猶他州一九九五年五月等）、德國（一九九七年八月）、馬來西亞（一九九七年）、義大利（一九九七年三月）及新加坡（一九九八年六月）等國家完成電子簽章法立法之後，行政院亦於日前（一九九九年十二月）通過電子簽章法草案[37]，提交立法院審查，等待完成立法程序。這顯示政府建立電子交易環境與普及電子商務應用的決心，也揭示一個資訊化、電子化、網路化時代的來臨。但是網路與電子交易環境日益複雜，電子資料在網路傳輸及儲存過程中，容易遭受僞造、竄改或竊取，因此資訊安全技術是建置安全電子交易環境的核心技術之一[38]。

秘密分享技術（secret sharing scheme）是資訊安全技術中的一個重要領域，近來吸引相當多的學者投入研究[2-6, 8-13, 17-18, 22-23, 25-26, 29-34]，在文獻[21,28]中有詳細完整的介紹。秘密分享技術將**秘密**（secret）分割成若干稱爲**分享**（secret share）的部分，並利用分享來組合拼湊成原來的秘密。秘密分享技術可使用於許多與群體運作及控制有關的領域上，如私密金鑰管理（private key management）、會議金鑰（conference key）的產生[36]、安全多方計算（secure multiparty computation）[6, 9, 11]、視覺密碼學（visual cryptography）的應用[23]及網路拍賣安全開標程序（network auction）[35]等。

最基本的秘密分享技術爲(*t*,*n*) threshold scheme [3, 30]，其基本想法爲將秘密分割爲 *n* 個分享，而只要任何 *t* 個（$t \leq n$）分享即可還原原始的秘密，而任何少於 *t* 個以下的分享將無法獲得任何原始秘密的資訊。一個更一般化的秘密分享技術爲**存取結構**（access structure）秘密分享 [2, 13]，在此技術中，僅有授權子集合（authorized subset）中的所有分享才可恢復原始秘密而所有非授權子集合（unauthorized subset）中的分享，均無法獲取任何有關原始秘密的訊息。

近來有研究利用**法定人數集合系統**（quorum system）實現秘密分享技術[6,25]，並將之用於秘密的分散式儲存[25]及安全多方計算[6]上，此種秘密分享

技術需要取得所有分享中的若干個才能恢復原始之秘密，這可降低秘密遭受僞造、竄改或竊取的機會；另外，可以不用取得全部的分享即可計算出原始的秘密，這又賦予秘密存取的容錯（fault-tolerant）能力。

法定人數集合（quorum）是由秘密分享參與者（player）所構成的集合，法定人數集合系統（quorum system）則是由法定人數集合所構成的收集（collection），此收集並滿足任何二個法定人數集合均有交集的條件 [1, 14-16, 19-20, 27]。法定人數集合系統一般應用於容錯分散式控制及管理上，如互斥控制（mutual exclusion）[1, 14, 16, 20, 27]及資料備份控制（data replica control）[7, 15, 19] 等，法定人數集合系統具有低通訊成本（communication cost）及高擷取度（availability）的特性 [24]，將法定人數集合系統應用於秘密分享技術上，可使秘密分享技術亦具有如同法定人數集合系統的特性。

文獻[6]中提出一個一般化的法定人數集合系統秘密分享技術，此技術可適用於所有的法定人數集合系統，除了一般化的法定人數集合系統秘密分享技術之外，文獻[6, 25]亦針對不同的法定人數集合系統提出不同的秘密分享技術，包括階層樹狀（hierarchical tree）法定人數集合系統[1, 19] 秘密分享技術、有限投射平面（finite projective plane）法定人數集合系統[20] 秘密分享技術及爬牆（crumbling wall ）法定人數集合系統 [27] 秘密分享技術等，這些特別的法定人數集合系統秘密分享技術，因爲利用各系統不同的特性，因此比一般化的法定人數集合系統秘密分享技術有更低的通訊成本與更高的擷取度。

一個較法定人數集合系統更一般化的觀念爲寫入-讀出法定人數集合系統(write-read quorum system)[12]，寫入-讀出法定人數集合系統的條件爲(1)寫入法定人數集合必須與其他寫入法定人數集合有交集(2) 寫入法定人數集合必須與讀出法定人數集合有交集。我們可以很容易看出寫入-讀出法定人數集合系統比法定人數集合系統更具一般性。若我們又加入最小化(minimality)的特性於寫入-讀出法定人數集合系統中，則我們可以得到寫入-讀出法團（write-read coterie），而一個不可超越(nondominated)寫入-讀出法團是所有寫入-讀出法團中

具有最佳化(optimality)特性的候選者。

本論文利用不可超越寫入-讀出法團來實現秘密分享技術。我們將證明利用不可超越寫入-讀出法團產生的存取結構，可以滿足秘密分享技術秘密重建(reconstruction)特性及完美(perfect)特性，因爲寫入-讀出法團比法定人數集合系統更具一般性，這使得我們所提出的秘密分享技術更具有彈性及更加有效率。

貳、相關研究

令 $U=\{u_1,...,u_n\}$ 是一個包含所有參與者$u_1,...,u_n$的宇集合 (universal set)，以下我們敘述寫入-讀出法定人數集合系統(write-read quorum system)、寫入-讀出法團結構(read-wrtite coterie)、存取結構(access structure)、寫入-讀出法定人數集合存取結構(write-read quorum access structure) 的定義及其相關的定理及特性。

定義 1：寫入-讀出法定人數集合系統(*write-read quorum system*)

一個**寫入-讀出法定人數集合系統**(*write-read quorum system*)是一由兩個 U 的子集合(subset)的收集(collection)所構成的配對(pair) ($\mathcal{W}$, $\mathcal{R}$)，並且滿足以下之條件：

(P1)寫入-寫入互斥(Write-Write Mutual Exclusion)特性

$\forall X,\forall Y: X,Y\in \mathcal{W}: X\cap Y\neq\varnothing$;

(P2)寫入-讀出互斥(Write-Read Mutual Exclusion) 特性

$\forall X,\forall Y: X\in \mathcal{W}, Y\in \mathcal{R}: X\cap Y\neq\varnothing$;

另外，若最小化(minimality)的特性也可以滿足的話，那麼我們可以得到一個更嚴謹的系統：寫入-讀出法團(write-read coterie)

定義 2：寫入-讀出法團(*write-read coterie*)

一個**寫入-讀出法團(*write-read coterie*)**是一由兩個 U 的子集合(subset)的收集(collection)所構成的配對(pair) ($\mathcal{W}$, $\mathcal{R}$)，並且滿足以下之條件：

(P1)寫入-寫入互斥(Write-Write Mutual Exclusion)特性

$\forall X,\forall Y: X,Y\in \mathcal{W}: X\cap Y\neq\varnothing$;

(P2)寫入-讀出互斥(Write-Read Mutual Exclusion) 特性

$\forall X,\forall Y: X\in \mathcal{W}, Y\in \mathcal{R}: X\cap Y\neq\varnothing$;

(P3)寫入法定人數集合最小化特性

$\forall X,\forall Y: X,Y\in \mathcal{W}, X\neq Y: X\not\subseteq Y$;

(P4) 讀出法定人數集合最小化特性

$\forall X,\forall Y: X,Y\in \mathcal{R}, X\neq Y: X\not\subseteq Y$.

例如，令 $\mathcal{W}=\{\{u_1,u_2,u_3\}, \{u_1,u_2,u_4\}, \{u_3,u_4\}\}$， $\mathcal{R}=\{\{u_1,u_3\}, \{u_1,u_4\}, \{u_2,u_3\}, \{u_2,u_4\}, \{u_3,u_4\}\}$，則 $(\mathcal{W}, \mathcal{R})$ 是一個滿足特性(P1)、 (P2)、 (P3)及(P4)的寫入-讀出法團。

以下我們介紹寫入-讀出法團的超越(*domination*)特性：

定義 3：法團超越(*domination*)性

令 $\mathbb{A}=(\mathcal{W}_A, \mathcal{R}_A)$ 及 $\mathbb{B}=(\mathcal{W}_B, \mathcal{R}_B)$ 是兩個寫入-讀出法團。那麼，我們說 $\mathbb{B}$ **超越** $\mathbb{A}$ 若且唯若 [4]

(1) $\mathbb{A}\neq\mathbb{B}$, i.e., $\mathcal{W}_A\neq\mathcal{W}_B$, or $\mathcal{R}_A\neq\mathcal{R}_B$;

(2) $\forall X: X\in \mathcal{W}_A:[\exists Y:Y\in \mathcal{W}_B:Y\subseteq X]$;

(3) $\forall X: X\in \mathcal{R}_A: [\exists Y:Y\in \mathcal{R}_B:Y\subseteq X]$.

定義 4：法團不可超越(*nondomination*)性

一個寫入-讀出法團稱爲**不可超越**(*nondominated, ND*) 若且唯若沒有其他的寫入-讀出法團可以超越它。

例如，令 $\mathcal{W}_1=\{\{u_1,u_2,u_3\}, \{u_1,u_2,u_4\}, \{u_1,u_3,u_4\}, \{u_2,u_3,u_4\}\}$, $\mathcal{R}_1=\{\{u_1,u_3\}, \{u_1,u_4\}, \{u_2,u_3\}, \{u_2,u_4\}\}$, $\mathcal{W}_2=\{\{u_1,u_2,u_3\}, \{u_1,u_2,u_4\}, \{u_3,u_4\}\}$, and $\mathcal{R}_2=\{\{u_1,u_3\}, \{u_1,u_4\}, \{u_2,u_3\}, \{u_2,u_4\}, \{u_3,u_4\}\}$. 那麼， $(\mathcal{W}_1,\mathcal{R}_1)$ and $(\mathcal{W}_2,\mathcal{R}_2)$ 是寫入-讀出法團，而且，根據定義，$(\mathcal{W}_2,\mathcal{R}_2)$ *超越* $(\mathcal{W}_1,\mathcal{R}_1)$。

根據法團不可超越特性，我們有以下的定理：

定理 1： 令 $\mathbb{C}=(W,R)$ 是一個不可超越寫入-讀出法團，則

$\forall X: X\in W:[\exists Y:Y\in R:Y\subseteq X]$

證明：

假設定理之所求證的命題爲非，即$\exists X: X\in W:[\ \forall Y:Y\in R:Y\not\subseteq X]$。

我們可以重新定義一個寫入-讀出法團(W,R')，其中 $R'=R\cup\{X\}$。我們可以看出(W,R')超越(W,R)，這明顯與(W,R)是一個不可超越寫入-讀出法團的事實相違背，因此定理所求證的命題爲真。 □

在Ibaraki及Kameda的論文中[12], 任何U 的子集合可以表示成一個n-項(n-tuple)向量 $X, X=(x_1,...,x_n) \in \{0,1\}^n$ ，其中 x_i 爲 1(0) 若 u_i 在 (不在) 此子集合中。 令C 是一個 U的子集合所構成的收集。 那麼，集合C的對應布林函數 $f_C : \{0,1\}^n \to \{0,1\}$ 定義爲 $f_C(X) \equiv \bigvee_{G\in C}\{\bigwedge_{u_i\in G} x_i\}$。 函數 f_C 具有以下的特性: $f_C(X)=1$ 若向量 X 表示一個法定人數集合的超集合(super set); 反之， $f_C(X)=0$。一個布林函數的對偶 f^d 定義爲 $f^d=f'(X')$，其中 X' 及 f' 分別是 X 及 f, 的反向 (complement)。 例如，令$U=\{u_1, u_2, u_3\}$, 集合 $\{u_1, u_2\}$ 表示爲 (1,1,0); 而 $\{u_2, u_3\}$ 表示爲 (0,1,1)。令 $C=\{\{u_1, u_2\}, \{u_2, u_3\}\}$， 則 $f_C(X) = (x_1x_2 \vee x_2x_3)$.

$f_C^d(X)= f'(X')=(x_1' x_2' \vee x_2' x_3')' = (x_1' x_2')' (x_2' x_3')' =(x_1 \vee x_2) (x_2 \vee x_3) = x_2 \vee x_1x_3$。

集合 C 的對應布林函數提供一個檢查 C 的特性的簡便方法。 例如，以下的定理 2 及定理 3 實際上是論文[12]裡的 Theorem 2.3 及 Theorem 2.4。它們可用以檢查寫入-讀出法團的特性。

定理 2： 令 $\mathbb{C}=(W,R)$, 其中 W 及 R 是U的非空子集合所構成的滿足最小化特性的收集。那麼， $\mathbb{C}$ 是一個寫入-讀出法團若且唯若 (1) $f_W \le f_W^d$ and (2) $f_W \le f_R^d$。

定理 3： 令 $\mathbb{C}=(W,R)$ 如定理 1 中所定義。 那麼，$\mathbb{C}$ 是一個不可超越的寫入

-讀出法團若且唯若 (1) $f_W \le f_W^d$ and (2) $f_W = f_R^d$。

由定理 2 及定理 3 我們可以得到以下推論：

推論 1： 令$\mathbb{C} = (W,R)$ 是一個寫入-讀出法團。 那麼，$\mathbb{C}$ 不可超越若且唯若 $f_W = f_R^d$。 □

根據推論 1，我們可以得到以下之推論：

推論 2 令 (W,R) 是一個不可超越寫入-讀出法團，且X是U的一個子集合。那麼，$X \in W$若且唯若 $\overline{X} \notin R$ (或等義的說，$X \notin W$若且唯若 $\overline{X} \in R$)。 □

定義 5: **存取結構(access structure)**

一個**存取結構(access structure)**A 是 U 的子集合(subset)所構成的收集(collection)，並且滿足以下之單調遞增(monotone increasing)條件：

若 $X \in A$ 則對於每一個 Y，$Y \supseteq X$，我們可得 $Y \in A$。

定義 6: 寫入-讀出法團存取結構(write-read coterie access structure)

令 $\mathbb{C} = (W,R)$ 是一個寫入-讀出法團，對應於 $\mathbb{C}$ 的寫入-讀出法團存取結構(write-read coterie access structure) $\Gamma(\mathbb{C})$定義爲所有的讀出法定人數集合(read quorum)與所有的寫入法定人數集合(write quorum)的聯集，也就是說：

$\Gamma(\mathbb{C})=\{Z \mid Z \supseteq X, X \in R\} \cup \{Z \mid Z \supseteq X, X \in W\}$。

一個不可超越寫入-讀出法團存取結構實際上與其讀出法定人數集合存取結構相同，意即若 $\mathbb{C}$ 是不可超越寫入-讀出法團，則$\Gamma(\mathbb{C})=\{Z \mid Z \supseteq X, X \in R\} \cup \{Z \mid Z \supseteq X, X \in W\}=\{Z \mid Z \supseteq X, X \in R\}$，因爲根據定理 1，$\forall X: X \in W:[\exists Y: Y \in R: Y \subseteq X]$，因此我們可得$\{Z \mid Z \supseteq X, X \in R\} \supseteq \{Z \mid Z \supseteq X, X \in W\}$，所以$\Gamma(\mathbb{C})=\{Z \mid Z \supseteq X, X \in R\}$。

定義 7：秘密分享技術(secret sharing scheme)

令S是所有可能的秘密所構成的有限集合。一個秘密分享技術是一種對應 $\Pi: S \times E \to S_1 \times \cdots \times S_n$ ，其中E是由隨機字串所構成的集合，S_i是分配給參與者 $u_i (u_i \in U, 1 \le i \le n)$，可能的分享所構成的集合，我們說$\Pi$是實現存取結構$\Gamma$的秘密分享技術，若以下的二個條件可以滿足：

(S1)秘密重建(reconstruction)特性：對應每一個集合X，$X\in\Gamma$，假設$X=\{u_{\sigma(1)},\ldots,u_{\sigma(|X|)}\}$，其中σ爲一個由{1..|X|}對應至{1..n}的函數，則存在一個函數$H_\Gamma: S_{\sigma(1)}\times\cdots\times S_{\sigma(|X|)}\rightarrow S$，使得，針對每一個配對$(s,\varepsilon)\in S\times E$，均滿足若$\Pi(s,\varepsilon)=\{s_1,\ldots,s_n\}$則$H_\Gamma(s_{\sigma(1)},\cdots,s_{\sigma(|X|)})=s$。

(S2)完美(perfect)特性：令 $X\notin\Gamma$，則對於任何兩個屬於S的秘密a與b，必須滿足：對於X的成員可能蒐集到的分享所構成的集合$\{s_i|u_i\in X\}$，

$prob(a|\{s_i|u_i\in X\})=prob(b|\{s_i|u_i\in X\})$

參、秘密分享技術及其正確性證明

以下我們提出一個秘密分享技術，我們稱爲WRC-SSS(Write-Read Coterie Secret Sharing Scheme)技術。考慮一個寫入-讀出法團$\mathbb{C}=(\mathcal{W},\mathcal{R})$, 其中$\mathcal{W}=\{W_1,\ldots,W_p\}$, $\mathcal{R}=\{R_1,\ldots,R_q\}$。令 v 是一個欲分享的秘密值，我們可將v分割爲$v_1,..,\ v_p$，使得$v=\sum_{j=1}^{p} v_j$。我們將 $v_1,\ldots,\ v_p$ 稱爲v 的切割(partition)以免與術語分享混淆，每一個v_j對應至一個寫入法定人數集合W_j，$1\le j\le p$ 。屬於參與者u_i的分享(share) $s_i(v)$ 是包含參與者u_i的寫入法定人數集合相對的切割所構成的集合，明確的說: $s_i(v)\equiv\{v_j|u_i\in W_j,\ W_j\in\mathcal{W},\ 1\le i\le n,\ 1\le j\le p\}$。

<u>定理 4</u>: 令$\mathbb{C}=(\mathcal{W},\mathcal{R})$ 是一個不可超越寫入-讀出法團，WRC-SSS是一個實現$\Gamma(\mathbb{C})$的秘密分享技術。

證明：

(1)秘密重建(reconstruction)特性：由於$\Gamma(\mathbb{C})=\{Z|\ Z\supseteq X,\ X\in\mathcal{R}\}\cup\{Z|\ Z\supseteq X,\ X\in\mathcal{W}\}$，若$X\in\ \Gamma(\mathbb{C})$則根據寫入-讀出法團的寫入-讀出互斥(Write-Read Mutual Exclusion) 特性：$\forall X,\forall Y: X\in\mathcal{W},\ Y\in\mathcal{R}: X\cap Y\neq\varnothing$;即$X$中的參與者可以蒐集到對應到每一個寫入法定人數集合的切割$v_1,\ldots,v_n$，因此得以重建秘密v。

(2)完美(perfect)特性：令$X \notin \Gamma(\mathbb{C})$，且$X=\{u_{\sigma(1)},\ldots, u_{\sigma(|X|)}\}$。由$X \notin \Gamma(\mathbb{C})$，我們可得$X \notin R$；那麼，根據推論 2 可得$\overline{X} \in W$，也就是說存在一個法定人數集合$W_j$，$1 \le j \le p$ ，$W_j \subseteq \overline{X}$ ，$W_j \in W$。因爲只有W_j中的成員擁有v_j，自然的，沒有任何X中的參與者能夠收集到v_j。

令ε^a是一個隨機字串，使得$\Pi\ (s,\ \varepsilon^a)=\{s_1^a,\ldots, s_n^a\}$且$H_\Gamma(s_{\sigma(1)}^a,\ldots, s_{\sigma(|X|)}^a)=a$。那麼，對於任何一個異於$a$的秘密值$b$，存在一個隨機字串$\varepsilon^b$使得$\Pi\ (s, \varepsilon^b)=\{s_1^b,\ldots, s_n^b\}$且$H_\Gamma(s_{\sigma(1)}^b,\ldots, s_{\sigma(|X|)}^b)=b$， $\{s_1^b,\ldots, s_n^b\}$可以由$\{s_1^a,\ldots, s_n^a\}$來建置，其做法是以$v_j+(a-b)$取代對應於W_j的v_j部分即可。因爲剛剛描述的取代動作只僅僅影響W_j的成員，因此我們可以得到X中的參與者蒐集到的分享對應成秘密值a與秘密值b的機率相等，即

$prob(a|\{s_i(v)|u_i \in X\})=prob(b|\{s_i(v)|u_i \in X\})$

這意味著集合 X 中的參與者無法獲取秘密值 v 的任何訊息。 □

肆、比較

在本節中，我們將 WRC-SSS 技術與一些以**法定人數集合系統**(quorum system)爲基礎的秘密分享技術加以比較。

法定人數集合系統的交集特性爲(1)任何二個法定人數集合具有非空之交集而寫入-讀出法團的交集特性爲(1)寫入法定人數集合必須與其他寫入法定人數集合有交集(2)寫入法定人數集合必須與讀出法定人數集合有交集。我們若將法定人數集合系統的法定人數集合看成既是寫入法定人數集合也是讀出法定人數集合的話，那麼，很明顯的，一個具最小化特性的法定人數集合系統就是一個寫入-讀出法團。因此，我們可以看出寫入-讀出法團比法定人數集合系統更具一般性。

一般而言，以法定人數集合系統爲基礎設計的系統具有低通訊成本(communication cost)及高擷取度(availability)。通訊成本與法定人數集合的

尺寸(size)成正比，在寫入-讀出法團中，因爲讀出法定人數集合的交集限制較少(讀出法定人數集合僅需滿足寫入-讀出互斥特性)，因此讀出法定人數集合通常有較小的尺寸；而一個法定人數集合系統的擷取度設定爲在環境有可能出錯的情況下，依然能夠組成法定人數集合的機率，寫入-讀出法團中因爲比法定人數集合系統多出讀出法定人數集合這個種類，因此比較容易組成法定人數集合，這意謂著寫入-讀出法團有較高的擷取度。總而言之，若是以寫入-讀出法團爲基礎來製作秘密分享技術，會比使用法定人數集合系統爲基礎來製作的秘密分享技術具有更低的通訊成本與更高的擷取度。

伍、結論

本論文提出一個利用不可超越寫入-讀出法團（nondominat ed write-read coterie）來實現的秘密分享技術 WRC-SSS。我們已證明利用秘密分享技術 WRC-SSS 產生的存取結構(access structure)，可以滿足秘密分享技術之秘密重建(reconstruction)特性及完美(perfect)特性。我們將 WRC-SSS 技術與一些以法定人數集合系統(quorum system)爲基礎的秘密分享技術加以比較。我們發現 WRC-SSS 技術擁有具有較低的通訊成本與較高的擷取度。

未來我們將著重於研究直接利用一些可以產生不可超越寫入-讀出法團的特定的方法來實現秘密分享技術，如文獻[15]裡的分欄方法(column protocol)及文獻[16]裡使用方格結構(grid structure)的備份控制方法(replica control protocol)，都是我們未來預計用以實現秘密分享技術的基礎。可以預期的，這些特定的不可超越寫入-讀出法團秘密分享技術將具有更好的特性。

參考文獻：

[1] D. Agrawal and A. El-Abbadi, "An efficient and fault-tolerant solution for distributed mutual exclusion," *ACM Trans. Comp. Sys.*, 9(1), pp.1- 20,1991.

[2] J. Benaloh and J. Leich ter, "Generalized secret sharing and monotone functions," In Advances in Cryptology – *CRYPTO'88*, LNCS 403, pp. 27-36. Springer - Verlag, 1988.

[3] G. R. Blakely, "Safeguarding cryptographic keys," In *Proc. AFIPS,* NCC, pp. 313-317, 1979.

[4] C. Blundo and A. D. Santis, "Lower bounds for robust secret sharing schemes," *Information Processing Letters*, Vol.63, pp. 317-321, 1997.

[5] C. Blu ndo, A. D. Santis and Ugo Vaccaro. "On secret sharing schemes," *Information Processing Letters*, Vol. 65, pp.25-32, 1998.

[6] D.Beaver and A. Wool, "Quorum-based secure multi-party computation," In K. Nyberg , editor , Advances in Cryptology *–EUROCRYPT'98* , LNCS 1403 , pp. 375-390 , Espoo , Finland, May 1998.

[7] S.Y. Cheung , M. H. Ammar , M. Ahamad, "The grid protocol: A high performance scheme for maintaining replicated data," *IEEE Trans. Knowledge and Data Eng.*, 4(6):582-592, 1992.

[8] C. Cachin, "On-line Secret Sharing," in *Proc. of 5th IMA Conference*, pp. 190-8; 1995.

[9] R. Canetti, U. Feige, O. Goldreich, and M. Naor. "Adaptively secure multiparty computation," In *Proc. 28th ACM Symp. Theory of Computing（STOC）*, pp. 639-648,1996.

[10] C. Charnes, J. Pieprzyk, R. Safavi-Naini, "Conditionally Secure Secret Sharing Schemes with Disenrollment Capability," *ACM Conference on Computer and Communications Security 1994*, pp. 89-95, 1994.

[11] M. Franklin, S. Haber, "Joint Encryption and Message-Efficient Secure Computation," *J. Cryptology*, vol. 9, pp. 217-232, 1996.

[12] T. Ibaraki and T. Kameda, "A theory of coteries: mutual exclusion in distributed systems," *IEEE Trans. Parall. and Distrib. Syst.*, vol. 4, no. 7, pp. 779-794, July 1993.

[13] M. Ito, A. Saito, and T. Nishizeki. "Secret sharing schemes realizing general access structure," In *Proc. IEEE Global Telecommunication Conf.（Globecomm 87）*,pp. 99-102,1987.

[14] Jehn-Ruey Jiang, "Quorum structures for fault-tolerant distributed mutual exclusion," *Ph.D. Dissertation, Tsing Hua University*, July 1995.

[15] Jehn-Ruey Jiang, "The column protocol: a high availability and low message cost solution for managing replicated data," *International Journal of Information Systems*, 20(8), pp. 687-696, Dec. 1995.

[16] Jehn-Ruey Jiang,"A framework for fault-tolerant distributed mutual

exclusion and replica control using grid structures," in *Proc. Of the 8th International Conference on Parallel and Distributed Systems*, pp.311-315, Chicago, IL, Oct. 1996.

[17] Wen-Ai Jackson, K. M. Martin, and C. M. O'Keefe, "Ideal Secret Sharing Schemes with Multiple Secrets," *J. Cryptology*, vol. 9, pp. 233-250, 1996.

[18] Wen-Ai Jackson, K. M. Martin, and C. M. O'Keefe, "Mutually Trusted Authority-Free Secret Sharing Schemes," *J. Cryptology,* vol. 10, pp. 261-289, 1997.

[19] Kumar, "Hierarchical quorum consensus：A new algorithm for managing replicated data," *IEEE Trans. Comput.*, 40(9), pp. 996-1004, 1991.

[20] M. Meakawa. A $\sqrt{n}$ algorithm for mutual exclusion in decetralized system. ACM Trans. Comp. Sys., 3(2):145-159, 1985.

[21] A. Menezes, P. Oorschot and S. Vanstone, "Secret Sharing," Book Section of *Handbook of Applied Cryptography*, pp. 524-540, CRC Press, 1996.

[22] P. Morillo, C. Padró, G. Sáez, J. L. Villar, "Weighted threshold secret sharing schemes," *Information Peocessing Letters*, vol. 70, pp. 211-216, 1999.

[23] M. Naor, A. Shamir, "Visual Cryptography," in *Eurocrypt'94*, pp. 1-12, 1994.

[24] M. Naor and A. Wool, "The load, capacity and availability of quorum systems," In *Proc. 35th IEEE Symp. Foundations of Comp. Sci.（FOCS）*, pp. 214-225, 1994.

[25] M. Naor and A. Wool, "Access control and signature via quorum secret sharing," *IEEE Trans. On Parallel and Distributed Systems*, Vol. 9, No. 9, pp. 909-922, 1998.

[26] Carles Padró, "Robust vector space secret sharing schemes," *Information Processing Letters*, vol. 68, pp. 107-111, 1998.

[27] D. Peleg and A. Wool. "Crumbling wall：A class of practical and efficient quorum system," *Distributed Computing*, 10(2), pp. 87-98, 1997.

[28] G. J. Simmons, "An introduction to shared secret and/or share control schemes and their application," In *Contemporary Cryptology, The Science of Information Integrity*, pp. 441-497. IEEE Press, 1992.

[29] De Santis, Y. Desmet, Y. Frankel, and M. Yung, "How to share a function securely," In *Proc. 26th ACM Symp. Theory of Computing (STOC)*, pp. 522-533, 1994.

[30] Shamir, A. "How to Share a Secret." *Comm. ACM*, 22(11), pp. 612-613,

1979.

[31] H.-M. Sun and S.-P. Shieh, "Constructing Perfect Secret Sharing Schemes for General And Uniform Access Structures," *Journal of Infomation Science and Engineering*, vol. 15, pp. 679-689, 1999.

[32] H.-M. Sun, "On-line multiple secret sharing based on a one-way function," *Computer Communication*, vol. 22, pp. 745-748, 1999.

[33] K.-J. Tan, H.-W. Zhu, S.-J. Gu, "Cheater identification in （t,n）threshold scheme," *Computer Communications*, vol. 22, pp. 762-765, 1999.

[34] Zhang, K.-Y. Lam, S. Jajodia, "Scalable threshold closure," *Theoretical Computer Science*, vol. 226, pp. 185-206, 1999.

[35] 梁高榮，「農產品交易工程學」，國立交通大學出版社，1999。

[36] 郭仲軒，曾文貴，「具容錯性質的分散式會議金鑰系統」，國立交通大學資訊科學研究所碩士論文， 1999。

[37] 行政院研考會，「電子簽章法草案內容」，http://www.pki.gov.tw/gcasite/dilaw/dilaw2.htm， 1999。

[38] 吳宗成，「電子商務安全技術」，製商整合科技人才培育教學研習營講義，2000。