基於(2,2)門檻機制之三重機密影像分享機制

廖惠雯
嶺東科技大學
資訊科技應用研究所
助理教授
e-mail：
hwliao@teamail.ltu.edu.tw

林映秀
嶺東科技大學
資訊科技應用研究所
碩士生
e-mail：
erinlin@ms14.hinet.net

摘要

本文以 Naor 和 Shamir 於 1994 年所提出的視覺密碼學概念為基礎，提出了一個三重機密影像分享機制，傳統的視覺密碼學大多用 1 個機密影像來做加解密的呈現，本文利用分享影像 A 為 2 黑 2 白像素及分享影像 B 為 3 黑 1 白像素，並且運用了旋轉分享影像每個 2x2 區塊的方式來建構一個基於(2,2)具有 3 個機密影像的視覺密碼機制，這是一種不需要複雜的數學計算，利用人類的視覺系統就能達到解密的方法，本文所提出之機制，其分享影像均勻分佈，不會有影像殘留問題，是個安全性高，而且方法簡單之三重機密影像分享機制。

關鍵詞：視覺密碼學、分享影像、視覺系統

Abstract

Visual cryptography, the theme of this research, was first proposed by Naor and Shamir in 1994. Its greatest advantage in decryption requires only superimposing the share images, no complicated computation or cryptology is requires. Most traditional visual cryptology technologies are based on one secret image between two share images. This research utilizes the techniques of rotating each 2*2 block of the ShareA to allow two share images to hold three kinds of confidential messages. The construction scheme handles the ShareA with 2 black-2white pixels and ShareB with 3 black-1 white pixels. Moreover, the technique of triple visual secrets sharing schemes in this study generates the share images distributed uniformly, and the method is easy to achieve information hiding procedure.

Keywords: Visual Cryptography, Share Image, Secret Image

1. 前言

因為資訊科技的發達、網路世界傳遞資料無遠弗屆的功能，造就了“秀才不出門，能知天下事”的生活環境，舉凡工作、消費、休閒…等，都愈來愈離不開電腦的需求，但是網路資源愈發達，有關電腦犯罪或弊端的問題就愈容易產生，因此資訊安全的議題便應運而生，像是密碼學、資訊隱藏、認證機制、數位鑑識及數位簽章的技術等，而視覺密碼學自從被發明之後，因為它不需要複雜計算的特性，被大量的應用在資訊安全的領域上。

2. 文獻探討

視覺密碼學/視覺安全是一種不需要用到電腦大量計算，經由人類的視覺系統就能達到解密的一種方法，這是由 Naor 和 Shamir[2]二位學者在 1994 年提出來的，其原理及概念是依據人類視覺系統對於影像色差的反應，加密時將原始機密分成數張分享影像，等到解密時再將分享影像疊置在一起就可以解密，這種將 n 張的機密影像，分別授權給 k 個成員，然後疊合 k 個以上成員所持有的分享影像($k \leq n$)，就能得到機密訊息的方法，造就了所謂的(k,n)門檻機制，如圖 1 為(2,2)門檻機制之視覺密碼學。

廖惠雯和林秀蓓[3][4]於 2007 年所提出的論文中，利用金鑰推導的觀念及秘密分享(2,2)門檻機制，建立了階層式多重視覺秘密分享交互建構機制，每個成員除僅須保存自己的分享影像，若須兩種機密，管理者僅須將自己的分享影像旋轉 90 度，就可以與使用者多一個機密，原始分享影像並不需要重新計算、成員數具有高度的擴充性，且不因成員數量多而造成金鑰(分享影像)管理的問題及不增加加密的複雜度，如圖 2 為階層式金鑰管理圖，而且此機制不僅適用在黑白視覺密碼學上，亦適用於灰階影像。

廖惠雯和張紋莉[5]於 2008 年提出了不擴展階層式雙重視覺秘密分享技術，這是以固定區塊為加密基本矩陣，每次選取 2x2 區塊作為加密區塊來進行加密判別，將此判別規則應用於階層式多重視覺秘密分享機制，即可建立不擴展階層式多重視覺秘密分享技術，並在還原

機密時，提出分享影像判別方法來提高還原影像之品質，圖 3 為不擴展階層式雙重視覺秘密分享技術的加密模型。

Pei-Fang Tsai and Ming-Shi Wang[6]於 2006 年提出了一個擁有三個隱藏機密資料的(3,3)視覺密碼分享方法，它是利用第一次加密處理產生 Share A 和 Temp Share，第二次加密處理是要從 Temp Share 中產生 Share B 和 Share C，等到要解密時，將 Share A 和做完互斥或(XOR)的 Share B 和 Share C 合成的 Temp Share 疊置，得到第一張機密影像，再利用 Share A 的順時針及逆時針旋轉 90 度後，分別與 Temp Share 疊置便能產生第二張及第三張的機密影像，表 1 為 Tsai 等人所提出之機制，圖 4 為其實驗結果。

由表 1 可看出，Temp Share 由 1 黑 3 白、2 黑 2 白及 3 黑 1 白所組成，黑白點分佈並不均勻，由其實驗結果圖 4 可看出此設計洩露了機密影像。且(3,3)門檻機制用意是設計三張分享影像給三個人共享機密，須三張分享影像正確疊合，才可看出機密，此設計僅將 Share B 及 Share C 疊合，就洩露出機密。

本文提出(2,2)門檻機制之三重機密分享機制，Share A 由 2 黑 2 白所組成，Share B 由 3 黑 1 白所組成(如表 2)，由於其均勻分佈，故由 Share A 及 Share B 完全看不出機密影像。

3.研究方法

本文用 2x2 的區塊為加密基礎，Share A 為 2 黑 2 白的區塊，共 6 種情形(如表 2(a))；Share B 為 3 黑 1 白的區塊，共 4 種情形(如表 2(b))，將 Share A 和 Share B 疊合後的結果以 3 黑 1 白表示為白色，4 黑 0 白為黑色，以此原則來建構本機制，表 3 為本文所提出來的三重機密影像分享機制，三種機密共有 8 種黑白排列，表 3 中分為 6 組，每組有 4 種組合，其餘 2 組，若遇到 3 個機密影像為白白白，則由第 1 組到第 3 組代替，而黑黑黑的組別則由第 4 組到第 6 組代替，各別有 12 種組合。

4.實驗步驟

首先將三張大小為 n x m 的機密影像 S1、S2 和 S3，分別是「嶺東科技大學」、「Ling Tung University」和「資訊科技應用所」，根據機密影像 S1、S2 和 S3 產生二張分享影像 Share A 及 Share B，例如，若 3 張機密影像相對應的像素為 “白黑白”時，則隨機選取表 3 第 2 組中的 4 對組合，假設 Share A 選取  ，而 Share B 為  時，所疊出來的結果為；當要產生第二張機密影像時，只要將 Share A 每個 2x2 區塊順時針旋轉 90 度成為  ，再和 Share B  做疊合，所疊出來的結果為  ；產生第三張機密影像，則再將 Share A 每個 2x2 區塊逆時針旋轉 90 度成為  ，一樣和 Share B疊合，所產生的疊合結果為  。三個機密影像為，即為定義中的“白黑白”，依序完成所有像素，即可產生 Share A 及 Share B。

5.實驗結果及討論

本篇論文所提出的三重視覺秘密分享機制(表 3)，其方法是由機密影像 S1、S2 和 S3 產生分享影像 A(Share A)和分享影像 B(Share B)(圖 5)，解密時，疊置 Share A 和 Share B 會還原第一張的機密影像(圖 6)，然後各別將 Share A 每個 2x2 區塊順時針的旋轉(Share A’)及逆時針 90 度的旋轉(Share A”)，再與 Share B 疊置後會還原第二張機密影像(圖 7)及第三張的機密影像(圖 8)。

本文依照 6 組 Share A 及 4 組 Share B 共 24 組的像素組合設計(2,2)門檻機制之三重機密影像分享機制，Share A 像素分佈為 2 黑 2 白的區塊，Share B 像素分佈為 3 黑 1 白的區塊，機密影像為“白白白”的組別以 2 白 1 黑的組別代替，而完全為“黑黑黑”的組別就用 2 黑 1 白的組別代替，其方法簡單，且此設計使得 Share A 和 Share B 的像素分布得很均勻，而不會產生殘影的現像問題(如圖 5-8)，提高了視覺密碼的安全性，不會有洩露機密的危險。

6.結論

由於資訊科技的進步與發達，讓人類生活在便利快速的環境中，但是資料傳遞愈快速及便利，有關電腦犯罪及弊端的問題就更容易產生，於是乎促使許多科學家發明防範電腦犯罪增加資訊安全的方法，視覺密碼學的優點就在於它不用大量的運算，用人類的視覺系統就能取得機密訊息。

本文以視覺密碼學(2, 2)門檻機制的原理為基礎，配合運用了旋轉分享影像的方式，提出了一個三重機密影像分享機制，不僅方法簡單，而且安全度高，也大大地解決了機密影像會外洩的危機，所呈現出來的效果相當顯著。

參考文獻

[1] 王旭正、柯宏叡、ICCL-資訊密碼暨建構實驗室，***資訊與網路安全秘密通訊與數位鑑識新技法***，博碩文化，2006。

[2] Naor, M and Shamir, A. "Visual Cryptography" ***Proceedings in Eruocrypt'94, Lecture Notes in Computer Science,*** Springer-Verlag, pp.1-12, 1994.

[3] 廖惠雯、林秀蓓，"階層式多重視覺秘密分享機制-傳統分享影像之研究與應用"，***嶺東學報***，Vol. 22, pp. 105-118, 2007.

[4] 廖惠雯、林秀蓓，"階層式多重視覺秘密分享機制於灰階影像之研究與應用"，***資訊科技國際期刊***，Vol. 1, No.1, pp. 56-66, 2007.

[5] 廖惠雯、張紋莉，"不擴展階層式雙重視覺秘密分享技術" ***2008 資訊科技國際研討會***，2008.

[6] Pei-Fang Tsai, Ming-Shi Wang, "An (3,3)-visual Secret Sharing Scheme for H iding Three Secret Data" ***The 9th Joint Conference on Information Sciences, Oct. 8-11, Kaohsiung City, Taiwan***, pp.1007-1010, 2006

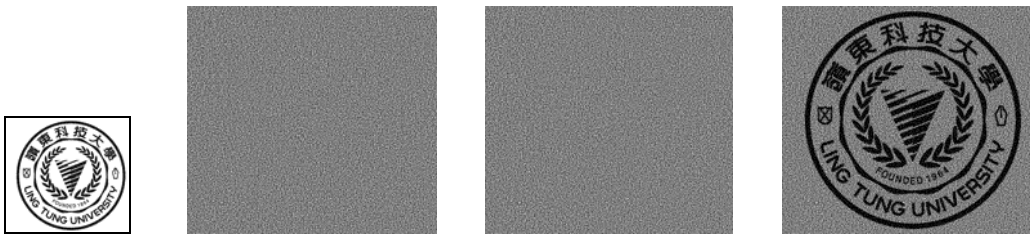


圖 1. (2,2) Naor and Shamir **視覺密碼加密與解密**

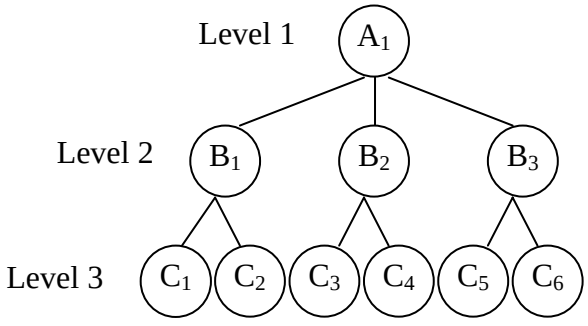
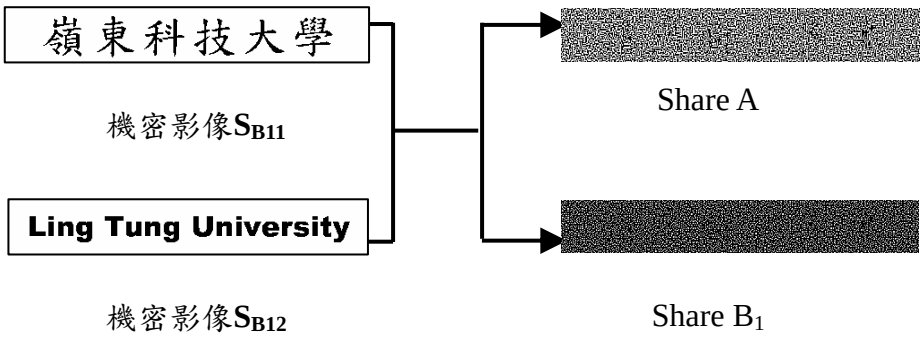
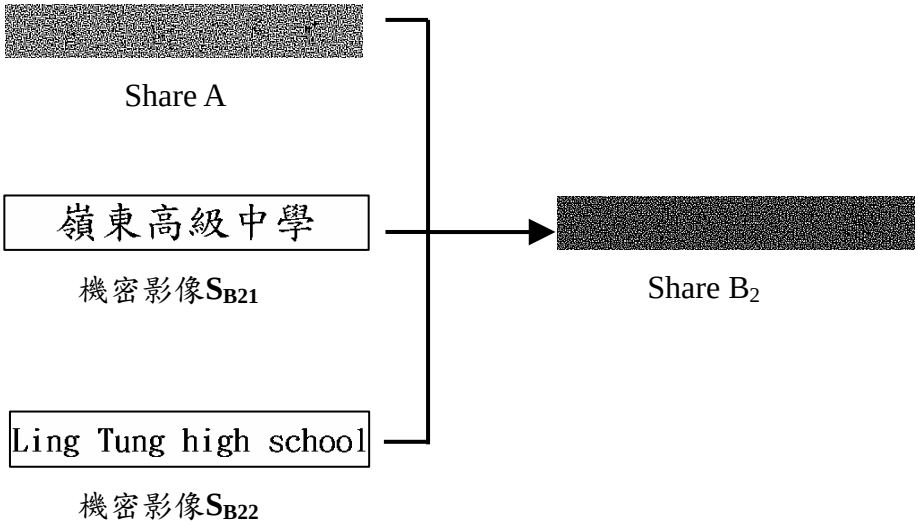


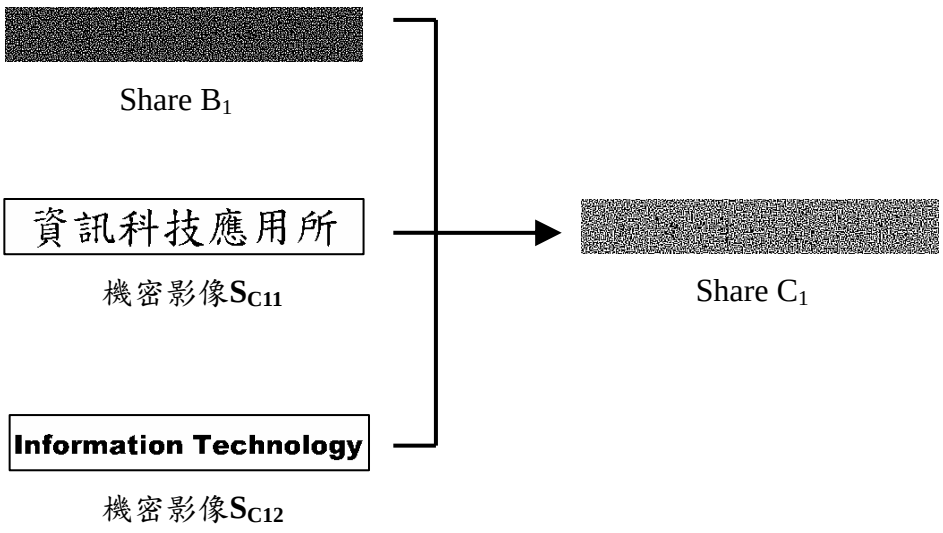
圖 2. 廖惠雯、林秀蓓的階層式金鑰管理



(a)機密影像S_{B11}、S_{B12}加密模型(S_{B11}與S_{B12}為第一層A與第二層B_1之間的機密影像)

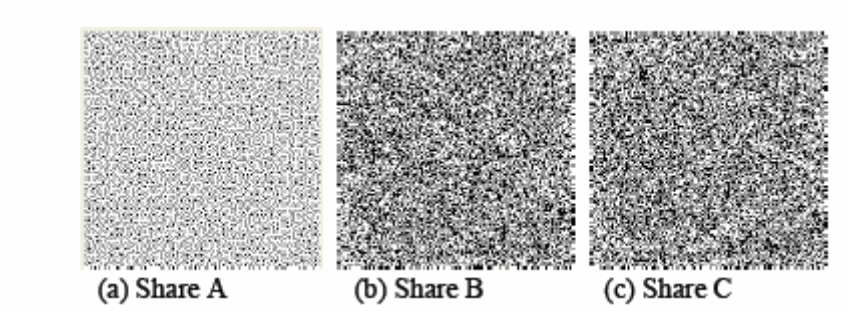


(b)機密影像S_{B21}、S_{B22}加密模型(S_{B21}與S_{B22}為第一層A與第二層B_1之間的機密影像)



(c) 機密影像S_{C11}、S_{C12}加密模型(S_{C11}與S_{C12}為第二層B_1與第三層C_1之間的機密影像)

圖 3. 廖惠雯、張紋莉的不擴展階層式雙重視覺秘密分享技術加密模型



Share Temp = Share B ⊕ Share C

圖 4. Pei-Fang Tsai and Ming-Shi Wang 的實驗結果

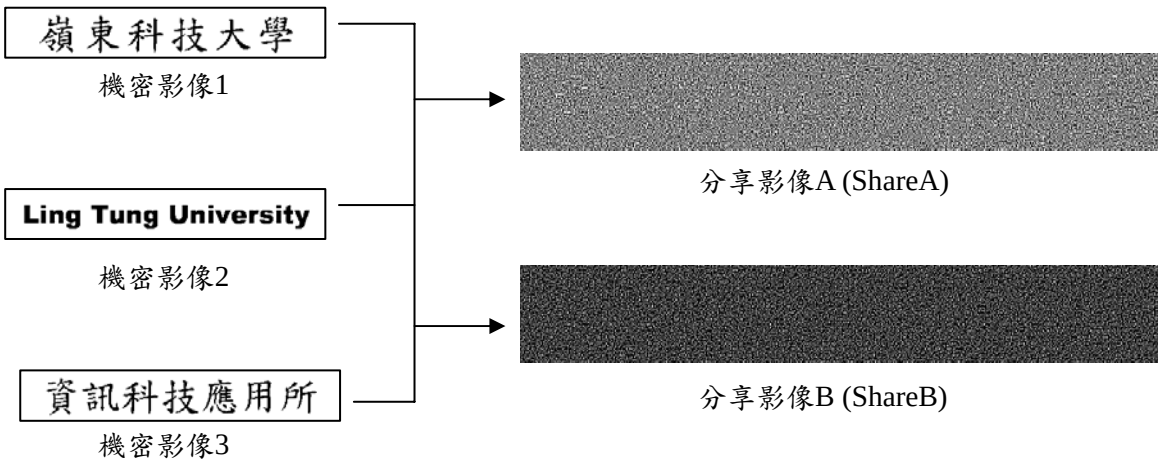
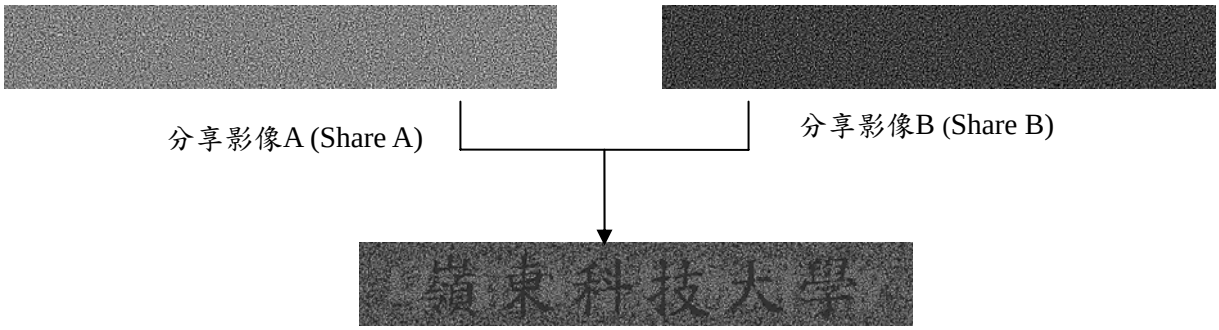
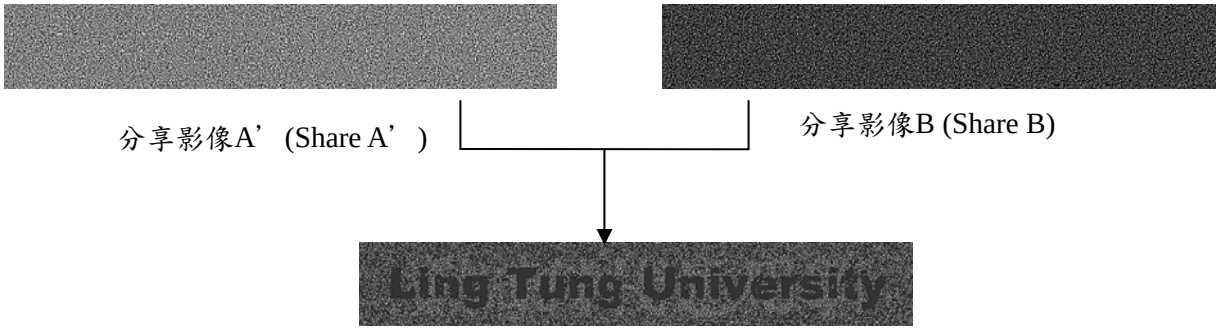


圖 5. 本研究所提出的三重機密影像分享圖



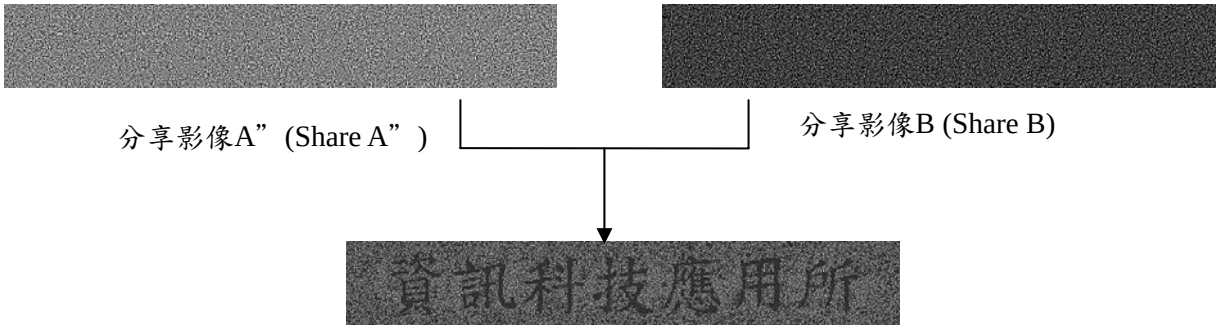
還原影像1

圖 6. 本研究方法還原影像 1



還原影像2

圖 7. 本研究方法還原影像 2



還原影像3

圖 8. 本研究方法還原影像 3

表 1：Tsai and Wang's Scheme

(a)The proposed of the part in first coding processing

Pixel of the first secret image	W	W	W	W	B	B	B	B	W	W	W	W	B	B	B	B
Pixel of the second secret image	W	W	B	B	W	W	B	B	W	W	B	B	W	W	B	B
Pixel of the third secret image	W	B	W	B	W	B	W	B	W	B	W	B	W	B	W	B
2×2 block of Share *A*																
2×2 block of Share *Temp*																
Stacked block by Shares *A* and *Temp*																
Share *A'*																
Stacked block by Shares *A'* and *Temp*																
Share *A"*																
Stacked block by Shares *A"* and *Temp*																

(b)The partial rules of the second encoding process

	1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*
Share *B*										
Share *C*										
Shares *Temp*										

表 2：本研究方法之像素表

(a)分享 A

分享 A						

(b)分享 B

分享 B				

表 3：本研究方法之三重機密影像分享機制

組別	第 1 組				第 2 組				第 3 組			
機密 1	白	白	白	白	白	白	白	白	黑	黑	黑	黑
機密 2	白	白	白	白	黑	黑	黑	黑	白	白	白	白
機密 3	黑	黑	黑	黑	白	白	白	白	白	白	白	白
Share A												
Share B												
Share A’												
Share A”												
Share A +ShareB												
Share A’ +ShareB												
Share A” +ShareB												

組別	第 4 組				第 5 組				第 6 組			
機密 1	白	白	白	白	黑	黑	黑	黑	黑	黑	黑	黑
機密 2	黑	黑	黑	黑	白	白	白	白	黑	黑	黑	黑
機密 3	黑	黑	黑	黑	黑	黑	黑	黑	白	白	白	白
Share A												
Share B												
Share A’												
Share A”												
Share A +ShareB												
Share A’ +ShareB												
Share A” +ShareB												