國立交通大學

資訊科學與工程研究所

碩 士 論 文

針對以 PHF 為基礎之臨界密碼系統的有效安全廣播模組

An Efficient Secure Broadcast Model for PHF-based Threshold Cryptosystems

研 究 生：甘家兆

指導教授：葉義雄　教授

中 華 民 國　九 十 五　年 七 月

針對以 PHF 為基礎之臨界密碼系統的有效安全廣播模組

An Efficient Secure Broadcast Model for PHF-based Threshold Cryptosystems

研 究 生：甘家兆　　Student：Chia-Chao Kan

指導教授：葉義雄　教授　　Advisor：Yi-Hsiung Yeh

國 立 交 通 大 學

資 訊 科 學 與 工 程 研 究 所

碩 士 論 文

A Thesis

Submitted to Institute of Computer Science and Engineering

College of Computer Science

National Chiao Tung University

in partial Fulfillment of the Requirements

for the Degree of

Master

in

Computer Science

June 2006

Hsinchu, Taiwan, Republic of China

中華民國九十五年七月

針對以 PHF 為基礎之臨界密碼系統的有效安全廣播模組

學生:甘家兆　指導教授:葉義雄 博士

國立交通大學資訊科學與工程學系碩士班

摘要

本篇論文主要是針對在無線網路上，以 PHF(Perfect Hash Family)為基礎的臨界(threshold)密碼系統，在安全廣播(broadcast)上面的特定需求，所設計的一個解決方案。

以 PHF 為基礎的臨界密碼系統有一個特色,即是各個 user 可由其所分享到的 share,來組成不同的 group。在這樣的觀點下，group 與 group 間的安全傳輸以及各個 group 內部的安全傳輸,便是一個需要解決的問題。如果這個問題能夠解決,那麼將可以用作 share renewal 等方面的應用。並且，考量無線網路傳輸上的特性，若是能以廣播的方式來做安全的傳輸，那麼將可以大量的減少所需要的傳輸量。

[1]提到了一個一般化的安全廣播模組，它需要一個TA(trust authority)來做pre-key的分配。然而，在某些無線網路架構上(舉例:Mobile Ad-hoc Network[2])，假設TA的存在往往有些不切實際。因此，在這篇論文中，我們提出了一個針對以PHF為基礎之臨界密碼系統的安全廣播模組，它不需要任何TA，並且，於安全廣播時所需要的訊息傳輸量也較 [1]來的少。

關鍵字：PHF,臨界密碼系統,安全廣播

An Efficient Secure Broadcast Model for PHF-based Threshold Cryptosystems

Student: Chia-Chao Kan Advisor: Dr. Yi-Hsiung Yeh

Institute of Computer Science and Information Engineering National Chiao Tung University

Abstract

The thesis targets for the particular requirement of secure broadcast on PHF (Perfect Hash Family)-based threshold cryptosystems on wireless networks, and we propose a method for doing such secure broadcast.

There is a property on PHF-based threshold cryptosystems: The users in the system can be partitioned into groups by the shares they keep. In such perspective, the secure communication between groups and within groups will be an issue which is needed to be solved. If such issue has been solved, then we can play applications of "share renewal", etc. Moreover, consider the native property of communication on a wireless network. If we apply broadcast technique, then we can reduce the communication cost greatly.

The paper in [1] gave a general secure broadcast scheme. It needs a TA (trust authority) to do the distributions of pre-key. However, in some wireless networks (Ex:Mobile Ad-hoc Network[2]), the existence of a TA is not practical at all. In the thesis, we propose a secure broadcast model on PHF-based threshold cryptosystems. It needs not a TA, and also, the communication cost while doing secure broadcast is less than [1].

Keywords: PHF, Threshold Cryptosystems, Secure Broadcast

致謝

能夠完成這篇論文，要感謝的人真是太多了。首先，我想感謝的是我的父母，感謝他們時常給予我信心與鼓勵，讓我能夠沒有後顧之憂的作研究。我非常感謝指導我的葉義雄教授，不僅在研究領域，老師也在做人、做事、做學問的態度上，給予我無形的身教，俾使我能夠見賢思齊。

我想要特別感謝實驗室的學長高銘智，在整篇論文的研究與寫作過程中，他幫助尋找論文的研究方向，給予許多極具前瞻性及中肯的建議，並且，容忍我的小小偷懶。

實驗室的同學們，包括常常與我一起研究論文的鴻祥、清大科管高材生的昇哥、台柱小白、以及總管兼神的接班人英宗，我很感謝你們。你們在我有疑惑的時候不吝嗇地回覆，在我灰心的時候予我鼓勵，我很開心能與你們作同學。

可愛的學弟妹們，包括美食鑑賞家 Gobby、跑起來不輸任何人的 Qting、以及跟我一樣瘋過惡靈古堡 4 的伯昕，我也很感謝你們，很珍惜與你們相處的快樂時光。

謝謝老哥、謝謝表哥，謝謝你們常常關心我，並且大方地提供我精神糧食。

最後，謝謝老天爺，賜與我足夠的勇氣與運氣，以完成這篇論文。

謝謝！

甘家兆

2006 年 7 月 19 日

目錄

表目錄

圖目錄

一、 簡介

1.1 網路安全需求

在現代資訊化的社會裡，網路安全越來越受到人們的重視。由於讓未加以保護的資料直接在網路上傳輸是危險的，因此，我們考慮將於網路上傳輸的資料加密，以防止被任何非授權者得知資料的內容。一般來說，我們必須考慮的網路安全需求有下列六項[3]：

- 機密性(Confidentiality)
- 確認性(Authentication)
- 完整性(Integrity)
- 不可否認性(Nonrepudiation)
- 存取控制(Access control)
- 可得性(Availability)

每一項需求都有它的獨特性以及重要性，皆是缺一不可。下面分別對此六項需求一一簡單介紹。

(1) 機密性(Confidentiality)

僅有傳送方和特定的接收方能夠了解傳輸的資料內容。竊聽者或許可以截取到經過加密的資料，但無法將該資料解密進而得知原始的資訊。

(2) 確認性(Authentication)

傳送方和接收方在通訊過程中都應該能夠互相證實，雙方的確具有他們所向對方宣稱的身分，即任何人無法冒充他人的身分進行通訊。

(3) 完整性(Integrity)

通訊的資料在產生、傳輸與儲存的過程中未被非法地竄改，即確保訊息沒有遭到複製、修改以及重複傳送等問題。

(4) 不可否認性(Nonrepudiation)

在接收方收到傳送方的資料後，接收方能夠證實資料確實是由傳送方所送出。傳送方不能在訊息傳送之後否認自己曾經傳送過訊息。同樣地，傳送方也能夠證實接收方已經接受過訊息，接收方無法否認。

(5) 存取控制(Access control)

未被授權的人員有可能透過網路存取對應的網路資源，這將危害到網路資訊安全。為防止這種情形發生，網路資源管理者必須對使用者設計不同的規範，以限制他們的行為。管理者必須先確認使用者的身分，才能進而給予適當的授權。

(6) 可得性(Availability)

有許多攻擊會造成網路系統的癱瘓，使它的有效性降低。因此需要一些處置來預防

或彌補這種損害，讓擁有權限的使用者可以隨時得到所想要的資源以及服務。

1.2 密碼理論基礎

密碼理論是達到網路安全的不可或缺的要素，網路安全的各種需求就是透過各種密碼演算法來完成。

密碼理論中的加密演算法，是一種數學函式的運算，從傳送端的角度，透過金鑰，我們可以將資料從原始的明文轉變為密文，而接收端在收到密文後，可以使用對應的演算法和金鑰，將密文轉變為原始的明文。

各種加密演算法根據其運算過程或機制的不同，主要可分為對稱式密碼學(Symmetric Cryptography)，非對稱式密碼學(Asymmetric Cryptography)，以及單向雜湊函數(one-way hash function)。

1.2.1 對稱式密碼學

使用相同的秘密金鑰來做加密與解密動作的演算法，稱為對稱式加密演算法，其典型的演算法有DES[3][4]、AES等。此類演算法最主要的問題是：由於加解密雙方是使用相同的秘密金鑰，因此在傳送資料之前，必須秘密地作金鑰的交換。但是，各種基本的手段均很難同時確保安全及高效率地完成此項工作，此為對稱式加密演算法的一大缺點。而它的優點是效率較好，速度較快。

下圖簡單地描述對稱式加密法。傳送方利用金鑰將明文加密為密文，然後再將密文傳送出去。在接收方收到密文後，便可使用同一把金鑰將密文解密還原為明文，以得知原始的訊息。

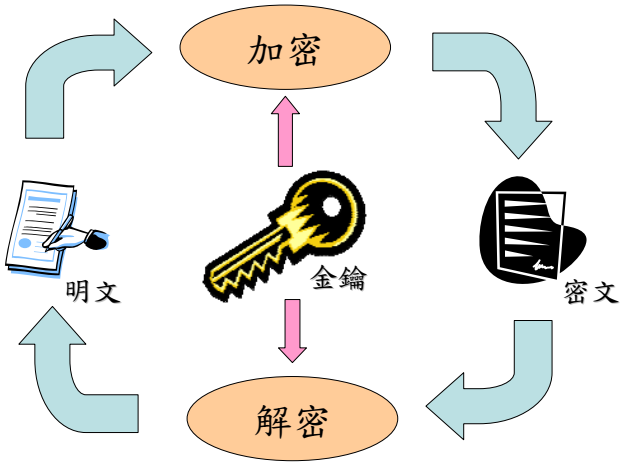

圖 1　　對稱式密碼系統

1.2.2 非對稱式密碼學

傳統的對稱式加密演算法遭遇到了一個難題：秘密金鑰的分發管理。如果秘密金鑰在分發時被洩漏了，那麼即使是最優秀的演算法也無法再確保安全。Diffie與Hellman在 1976 年提出公開金鑰密碼方法的概念[7]，它有效地避免了分發管理秘密金鑰的難題。

使用不同的秘密金鑰來做加密與解密，這種加密演算法一般稱為非對稱式加密演算法。在非對稱式演算法中，有一對秘密金鑰，一把金鑰稱為公開金鑰(public key)，另一把金鑰則稱作私密金鑰(private key)。因此這種演算法亦稱為公鑰加密演算法，其典型的演算法有RSA[3][4]、ECC[5][6]等。

使用公開金鑰加密後的密文只能用與其對應的私密金鑰解密，反之，用私密金鑰加密後的密文只能用與其對應的公開金鑰解密。我們的做法是把公開金鑰向外界公開，私密金鑰則交由自己保管。如果 Alice 要傳送一份機密文件給 Bob，則 Alice 應可以輕易取得 Bob 的公開金鑰，以加密此機密文件。Bob 在取得文件後，使用自己的私密金鑰將其解密，進而得知文件內容。如此即使被他人截取，其原始內容也不可能被得知。除了文件機密得以被確保外，非對稱式加密演算法也避開了資料傳送前秘密金鑰交換的問題。

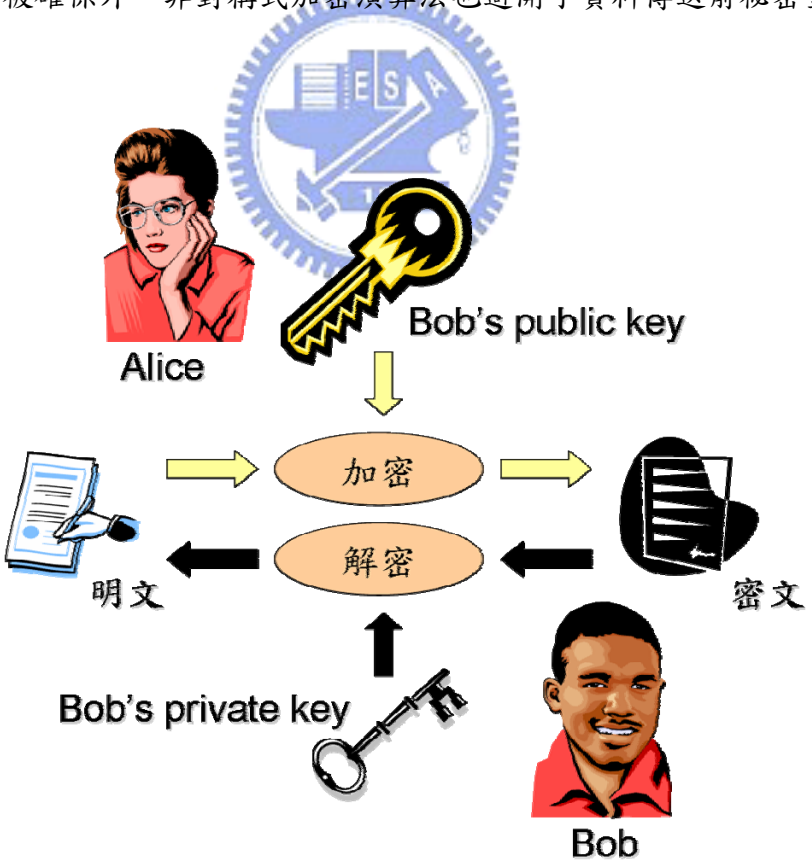

圖 2　　非對稱式密碼系統

以圖 2 為例，黃箭頭代表Alice送出文件前的加密流程，在加密過後，Alice將產生的密文送給Bob; 黑箭頭代表Bob收到密文後的解密流程，在解密過後，Bob可以得到明文。若相反地Alice是用自己的私密金鑰加密，而Bob是使用Alice的公開金鑰解密，則可以用來證明此文件為Alice本人所發，好似現實生活中本人的簽章，因為Alice的私密金鑰只有本人才能擁有。

雖然非對稱式加密演算法有效地避開了分發管理秘密金鑰這一難題，但是，其演算法相較於對陣式演算法複雜，因此資料加密時的速度較慢，效率較差。

1.2.3 單向雜湊函數

單項雜湊函數(One-way hash function)演算法的作用在於，對一段資料進行一次運算，然後得到一段長度固定的訊息摘要。任意兩個不同的資料，會得到兩個不同的訊息摘要，即使這兩個資料只有單一個位元的不同，生成的訊息摘要(message digest)依然會截然不同。我們可以透過訊息摘要來檢查訊息是否被修改，以達到資料完整性的確認。典型的單向雜湊函數演算法有MD5[3]、SHA、SHA-1、SHA-2 等。

1.3 相關設計理論基礎

設計理論(Design Theory)在各項工程領域都扮演了極重要的角色，其中的PHF(Perfect Hash Family)可用作網路安全應用中的臨界秘密分享(Threshold Secret Sharing)。於本篇論文內，我們將會使用到以下的設計理論產物：affine plane 以及PHF，而於本節，我們將簡單地介紹這些組合式物件。

1.3.1 Affine Plane

定義 1.3.1：(*Pairwise Balanced Design(PBD)*)

一個 pairwise balanced design(PBD)是一個有序對(S, B)，其中 S是一個符號的有限集合，裡頭的元素稱作點，而 B是一個以 S中的子集合為元素的集合，裡頭的元素稱作區塊。並且，任兩點恰會一起出現在同一個區塊。

□

以下我們稱 PBD 內的一個區塊為一條線。如果兩點在同一條線，我們稱該兩點為共線。如果兩條線不共點，則我們稱該兩線為平行。

定義 1.3.2：(*Affine Plane*)

一個 affine plane 是一個滿足下列兩性質的一個 PBD(P, B)：

(1) 存在至少一個四點的集合 S包含於 P，滿足 S中的任三點不共線。

(2) 給定一線 l 與一不在 l 上的點 p，則恰有一條線包含 p 且與 l 平行。

□

定義 1.3.3：(*order of an affine plane*)

一個 affine plane 是一個 PBD(P, B)，若 $|P|=n^2$，則稱 n 為該 affine plane 的 order。

□

另外，一個 order 為 $n, n\geq 2$ 的 affine plane(P, B)必滿足下列性質：

(a) $|B|=n^2+n$

(b) $\forall b \in B, |b|=n$

(c) B 可組成 $n+1$ 個 P 的分割，其中每個分割皆有 n 個元素

1.3.2 Perfect Hash Family

定義 1.3.5：(*Perfect Hash Family(PHF)*)

一個(A, B, w)-perfect hash family(PHF)是一個由 A 到 B 的函式的集合 F。並且，對於任何大小為 w 的 A 的子集合 X，都存在至少一個 $f\in F$，使得當限制函式輸入屬於 X 時，f 為一對一函式。並且若 $|F|=N$，則我們表示該 PHF 為 PHF$(N; A, B, w)$。另外，若 $|A|=n$，$|B|=m$，則這樣的 PHF 又可稱為 PHF$(N; n, m, w)$，本篇論文將採用 PHF$(N; n, m, w)$這樣的表示法。

□

範例 1.3.6：PHF(4;9,3,3)

	1	2	3	4	5	6	7	8	9
f_1	1	1	1	2	2	2	3	3	3
f_2	1	2	3	1	2	3	1	2	3
f_3	1	2	3	3	1	2	2	3	1
f_4	1	2	3	2	3	1	3	1	2

圖 3　　PHF(4;9,3,3)

□

一個 PHF 除了上述的定義外，還可以其他的方法的表示之，我們稱之為 PHF 的區塊表示法。使用區塊表示法的主要原因在於，我們不在意 B 集合內元素的實值，而在意的是 B 集合內的元素被哪些 A 集合內的元素所對應。

定義 1.3.7：(*PHF 的區塊表示法*)

對於任一個 PHF$(N; n, m, w)$，都可以將其轉換成 N 個 A 的分割以及 N 個由$\{A_i / A_i \subseteq A\}$

到 B 的函式。轉換方法如下：對於每個 $f_i \in F$ ，我們將對應到同一 B 集合元素的 A 集合元素，收集到同一集合。則很顯然地，這些集合將構成一個 A 的分割 P_i 。並且，可針對每一 f_i 定義一函式 b_i ，稱作區塊對應函式，其輸入是 P_i 中的任一元素(為一 A 的子集合)，其輸出是該集合成員所對應到的 B 集合元素。另外，本篇論文中將另稱 A 集合內的一個元素為一個點，分割 P_i 內的一個元素為一個區塊。

□

範例 1.3.8：PHF(4;9,3,3)的區塊表示法

對於範例 1.3.6 的 PHF(4;9,3,3)，我們可以區塊表示法表示為 4 個分割以及 4 個區塊對應函式，如下：

P_1={{123},{456},{789}}
P_2={{147},{258},{369}}
P_3={{159},{267},{348}}
P_4={{168},{249},{357}}
b_1({123})=1, b_1({456})=2, b_1({789})=3
b_2({147})=1, b_2({258})=2, b_2({369})=3
b_3({159})=1, b_3({267})=2, b_3({348})=3
b_4({168})=1, b_4({249})=2, b_4({357})=3

□

定義 1.3.9：((λ=1)-PHF)

首先定義 λ 為一個 PHF 中，任兩點在各個分割恰屬於同一區塊的個數，則由 PHF 的定義可知，λ 不見得在任一個 PHF 皆能夠被定義。而(λ=1)-PHF 是指一個 PHF 其 λ 值為一，故其必滿足任兩點在各個分割恰屬於單一個區塊。

□

範例 1.3.10：(λ=1)-PHF

範例 1.3.6 的 PHF(4;9,3,3)是一個(λ=1)-PHF，因為在此 PHF(4;9,3,3)中，任兩點再各個分割恰屬於一個區塊。任舉幾對點如下：

1,2 只在 P_1 屬於同一個區塊
6,8 只在 P_4 屬於同一個區塊
4,7 只在 P_2 屬於同一個區塊
3,9 只在 P_2 屬於同一個區塊

□

定義 1.3.11：(balanced PHF)

一個 balanced PHF 為一個滿足下列特性的 Perfect Hash Family，” 任一分割所含

區塊個數，等同於任一區塊所含點個數”。

□

範例 1.3.12：balanced PHF

範例 1.3.6 的 PHF(4;9,3,3)是一個 balanced PHF，因為其任一分割所含區塊個數，等同於任一區塊所含個數，皆為 3。

□

1.4 秘密分享

秘密分享是指我們將原始的秘密分為許多部分，再將單一個部分傳給單一個人。不過，沒有任何人能夠僅僅憑自己的部分，就獲得原始的秘密。只有當集合足夠多的部分時，原始的秘密才能被還原。

於本節，我們將介紹秘密分享中的 Shamir-秘密分享，它是一種(n,k)-臨界秘密分享；並且，我們也會另一種(n,k)-臨界秘密分享：PHF-based 臨界秘密分享，它利用到了 Perfect Hash Family 的概念。

1.4.1 (n,k)-臨界秘密分享

當我們將秘密分為 n 個部分，每個部分都稱做一個 share。當收集 k 個 share 時，k 小於等於 n，則秘密可被還原。滿足上面特性的秘密分享機制叫做(n,k)-臨界秘密分享((n,k)-Threshold Secret Sharing)。

(n,k)-臨界秘密分享是由Adi Shamir所提出[11]，他使用了多項式來分享一個秘密，使用多項式的內插法來還原回秘密。假設秘密為S，並且n個參與者分享這個秘密，我們命名這n個參與者為$id_1,id_2,...,id_n$。以下是(n,k)-臨界秘密分享的執行流程。

首先，我們需要一個公正的分配者，來負責分配 share 予各個參與者。

(1) 取一個質數 p，滿足 $p>\max(S,n)$。

(2) 選取一個多項式 $f(x)=a_0+a_1x+...+a_{k-1}x^{k-1}$，滿足 $a_0=S$ 且 a_i, $i=1,2,\cdots,k-1$ 屬於 Z_p。

(3) 對於 $i=1,2,\cdots,n$，計算 share $S_i=f(id_i)(\mathrm{mod}\ p)$。

(4) 對於 $i=1,2,\cdots,n$，分配 share S_i 予 $id_i,id_2,...,id_n$。

還原回秘密的方法，是透過 Lagrange 內插法來達成。並且，必定需要大於或等於個 $f(x)$才能還原回 $f(0)$，也就是 S。

以下是 Lagrange 內插法的公式：

$$f(x)=\sum_{i=1}^{k} Si\cdot\prod_{j=1,j\neq i}^{k}\frac{x-id_j}{id_i-id_j}(x)(\mathrm{mod}\ p)$$

1.4.2 PHF-based 臨界秘密分享

S.Blackburn在[12]提出了一個擴充的方法：在不改變臨界值(threshold)的情形下，我們可以一個針對秘密K以及m個參與者的秘密分享機制，擴充為一個同樣針對秘密S，不過有$n, n>m$個參與者的秘密分享機制，我們稱之為PHF-based臨界秘密分享。這是藉助了Perfect Hash Family的概念，而非另外找一個新的秘密分享機制。

以下將證明一個定理以及舉一個實例來說明PHF-based臨界秘密分享的運作流程[9]。

定理 1.4.1：

假設我們有一個 PHF$(N; n, m, w)$和 N個獨立的(m, w)-秘密分享機制，則我們可以建構一個(n, w)-秘密分享機制，其中每個參與者會從(m, w)-秘密分享機制接收到 N個 share。

證明：

假設$F = \{f_1, f_2, ..., f_N\}$是一個$(n, m, w)$-PHF，$S = \{S^1, S^2, ..., S^N\}$是一個收集$(m, w)$-秘密分享機制的集合，其所分享的秘密為 K。並且，S^i 分派給各個參與者的 share 為 $s^i_1, ..., s^i_m$，表示為$S^i = \{s^i_1, ..., s^i_m\}$。則我們可以產生出一個新的秘密分享機制 $T = \{t_1, ..., t_n\}$，如下：

對於任何 j 滿足$1 \le j \le n$，

$$t_j = \{s^i_{f_i(j)} : 1 \le i \le N\}$$

任何 w-1 個參與者在每一個(m, w)-秘密分享機制最多只能擁有 w-1 個 share。因此，這 w-1 個參與者無法得知原始秘密 K。而任何 w 個參與者至少擁有一組(m, w)-秘密分享機制中的 w 個不同 share，這是倚靠了 Perfect Hash Family F 的性質。因此，這個參與者能夠獲得原始秘密 K。

Q.E.D.

範例 1.4.2：PHF-based 秘密分享機制

假設 K=10 為原始的秘密，並且假設我們已經建構出四個在 Z_{13} 中的(3, 3)-秘密分享機制，如下：

$$S^1 = \{s^1_1 = 3, s^1_2 = 5, s^1_3 = 2\}$$
$$S^2 = \{s^2_1 = 2, s^2_2 = 2, s^2_3 = 6\}$$
$$S^3 = \{s^3_1 = 1, s^3_2 = 5, s^3_3 = 4\}$$
$$S^4 = \{s^4_1 = 2, s^4_2 = 11, s^4_3 = 10\}$$

則由 圖 3 所示的PHF$(4; 9, 3, 3)$，我們可以建構一個(9, 3)-秘密分享機制

T={ $t_1,...,t_9$ }，如下：

$$t_1 = (s^1{}_{f_1(1)}, s^2{}_{f_2(1)}, s^3{}_{f_3(1)}, s^4{}_{f_4(1)}) = (s^1{}_1, s^2{}_1, s^3{}_1, s^4{}_1) = (3,2,1,2)$$
$$t_2 = (s^1{}_{f_1(2)}, s^2{}_{f_2(2)}, s^3{}_{f_3(2)}, s^4{}_{f_4(2)}) = (s^1{}_1, s^2{}_2, s^3{}_2, s^4{}_2) = (3,2,5,11)$$
$$t_3 = (s^1{}_{f_1(3)}, s^2{}_{f_2(3)}, s^3{}_{f_3(3)}, s^4{}_{f_4(3)}) = (s^1{}_1, s^2{}_3, s^3{}_3, s^4{}_3) = (3,6,4,10)$$
$$t_4 = (s^1{}_{f_1(4)}, s^2{}_{f_2(4)}, s^3{}_{f_3(4)}, s^4{}_{f_4(4)}) = (s^1{}_2, s^2{}_1, s^3{}_3, s^4{}_2) = (5,2,4,11)$$
$$t_5 = (s^1{}_{f_1(5)}, s^2{}_{f_2(5)}, s^3{}_{f_3(5)}, s^4{}_{f_4(5)}) = (s^1{}_2, s^2{}_2, s^3{}_1, s^4{}_3) = (5,2,1,10)$$
$$t_6 = (s^1{}_{f_1(6)}, s^2{}_{f_2(6)}, s^3{}_{f_3(6)}, s^4{}_{f_4(6)}) = (s^1{}_2, s^2{}_3, s^3{}_2, s^4{}_1) = (5,6,5,2)$$
$$t_7 = (s^1{}_{f_1(7)}, s^2{}_{f_2(7)}, s^3{}_{f_3(7)}, s^4{}_{f_4(7)}) = (s^1{}_3, s^2{}_1, s^3{}_2, s^4{}_3) = (2,2,5,10)$$
$$t_8 = (s^1{}_{f_1(8)}, s^2{}_{f_2(8)}, s^3{}_{f_3(8)}, s^4{}_{f_4(8)}) = (s^1{}_3, s^2{}_2, s^3{}_3, s^4{}_1) = (2,2,4,2)$$
$$t_9 = (s^1{}_{f_1(9)}, s^2{}_{f_2(9)}, s^3{}_{f_3(9)}, s^4{}_{f_4(9)}) = (s^1{}_3, s^2{}_3, s^3{}_1, s^4{}_2) = (2,6,1,11)$$

□

PHF-based 臨界秘密分享也是(n, k)-臨界秘密分享的一種，不過，相較於在 1.4.1 所介紹的(n, k)-臨界秘密分享，PHF-based 臨界秘密分享可以較快地作秘密還原的動作，然而，其缺點便是每個節點要儲存較多的 share。

1.4.3 Proactive 秘密分享

如同在 1.4.2 小節所提及的，我們已經知道如何去分享一個秘密。假設所有的參與者皆為無線網路上的節點，那麼經過時間的推移，很有可能攻擊者可以一個接著一個地入侵參與的節點。當超過個k-1 節點被入侵時，攻擊者將有能力還原回秘密。為了避免被入侵超過k-1 節點，一個定期更新share的機制將被採用，這個機制稱作Proactive秘密分享(Proactive Secret Sharing)[10]。

我們必須在攻擊者成功入侵 k-1 節點之前，對 share 進行更新。而在兩次的 share 更新中，兩 share 是完全不相關的，亦即任何人無法由前次 share 預測或推算下一次的 share。換言之，在每次更新 share 的時間區間裡，需要確保攻擊者無法成功入侵 k-1 節點，

首先，我們針對 $f(x)$，產生一個多項式 $f^{(i)}(x)$。更新 share 的方法如下所示：

$f(x) = (a_0 + a_1 x + ... + a_{k-1} x^{k-1}) \bmod p$

$f^{(i)}(x) = (b_{i,1} x + ... + b_{i,k-1} x^{k-1}) \bmod p$ ， $b_{i,1}, \ldots, b_{i,k-1}$ 是隨機取得。

$$f'(x) = (f(x) + \sum_{i=1}^{k} f^{(i)}(x)) \bmod p$$

$$= (a_0 + (a_1 + \sum_{i=1}^{k} b_{i,1})x + ... + (a_{k-1} + \sum_{i=1}^{k} b_{i,k-1})x^{k-1}) \bmod p$$

每一個更新後的 share 可依 $f'(id_j), j = 1,2,...,k$ 來計算。並且，每一個參與者須負責

計算多項式 $f^{(i)}(id_j)$ 的 share，並將其安全地傳送給其他參與者。每一個參與者將收到的多項式 $f^{(i)}(id_j)$ 的 share 加到自己原本的 share，便可獲得更新後的 share。

1.5 研究動機

以 PHF 為基礎的臨界密碼系統有一個特色，即是各個 user 可由其所分享到的 share，來組成不同的 group。在這樣的觀點下，group 與 group 間的安全傳輸以及各個 group 內部的安全傳輸，便是一個需要解決的問題。如果這個問題能夠解決，那麼將可以用作 share renewal 等方面的應用。並且，考量無線網路傳輸上的特性，若是能以廣播的方式來做安全的傳輸，那麼將可以大量的減少所需要的傳輸量。

因此，在這篇論文中，我們提出了一個針對以PHF為基礎之臨界密碼系統的安全廣播模組，它不需要任何TA。。並且，於安全廣播時所需要的訊息傳輸量也較一個一般化的機制 [1]來得少。

1.6 論文編制

在第一章，除了說明研究動機與論文編制之外，我們也針對相關的背景知識作簡單的介紹，這包括了設計理論、秘密分享，以及Proactive秘密分享。於第二章，我們會詳細闡述與通篇論文有直接關聯的背景知識，主要是設計理論中的affine plane以及PHF。第三章是說明我們提出的架構*ESBM(the Efficient Broadcast Scheme)*，並對此架構作正確性、安全性以及容錯能力的分析。在第四章，我們將提出一些理論上的數據作為結果，並與一個一般化的架構 [1]作相關的比較。而第五章，我們為通篇論文作結論並且展望未來可改進的地方。另外，我們也給予幾個改良ESBM的建議方向。

二、 相關背景知識

於本章，我們會介紹一個建構 affine plane 以及一個建構 PHF 的方法。並且，針對在第一章所定義的 balanced (λ=1)-PHF，我們會探究幾個它所擁有的重要性質。另外，我們也會介紹由 Fiat 與 Naor 所提出的一個一般化的安全廣播模組，並說明其所具有的特性及性質。

2.1 相關設計理論細節

於本節，我們將稍加深入並延伸討論第一章所簡介的設計理論物件。我們會提出一個建構 affine plane 以及一個建構 PHF 的方法，並且舉出一實際的例子，希冀能有助於各位對於相關建構方法的了解。

2.1.1 建構 Affine Plane

我們將從一個finite field出發，經過一些特定的演算法，最終獲得一個affine plane。這裡所採用的建構方法在[8]有詳細地證明了正確性，而於本論文將只針對這些建構方法作介紹。另外，這裡假設閱讀者對finite field有一定程度的認識。

假設我們已經有了一個基數為 n 的 finite field $(F,+,\cdot)$，其中 n 為 prime power。則我們作下列程序，最終將獲得一個 affine plane。

$\circ(k)$	n	1	2	…	n-1
n	$n\cdot k+n$	$n\cdot k+1$	$n\cdot k+2$	…	$n\cdot k+(n-1)$
1	$1\cdot k+n$	$1\cdot k+1$	$1\cdot k+2$	…	$1\cdot k+(n-1)$
2	$2\cdot k+n$	$2\cdot k+1$	$2\cdot k+2$	…	$2\cdot k+(n-1)$
⋮	⋮	⋮	⋮	…	
n-1	$(n-1)\cdot k+n$	$(n-1)\cdot k+1$	$(n-1)\cdot k+2$	…	$(n-1)\cdot k+(n-1)$

圖 4　　$\circ(k)$的運算

1. 將$(F,+,\cdot)$中的 $n-1$ 個非零元素 rename 為 $1,2,3,\cdots,n-1$，將零元素 rename 為 n。

2. 依據$(F,+,\cdot)$對於+與·的二元運算表，對於每個非零元素k，我們做$\circ(k)=i\cdot k+j$的運算，其中$i,k\in F$。如 圖 4 所示：

運算後的結果可組成一個nxn的方陣L_k，由$n-1$ 個非零元素，我們可獲得n-1 個方

陣L_1, L_2, L_3, …, L_{n-1}，如圖 5 所示。

$n\cdot k+n$	$n\cdot k+1$	$n\cdot k+2$	…	$n\cdot k+(n-1)$
$1\cdot k+n$	$1\cdot k+1$	$1\cdot k+2$	…	$1\cdot k+(n-1)$
$2\cdot k+n$	$2\cdot k+1$	$2\cdot k+2$	…	$2\cdot k+(n-1)$
⋮	⋮	⋮	…	
$(n-1)\cdot k+n$	$(n-1)\cdot k+1$	$(n-1)\cdot k+2$	…	$(n-1)\cdot k+(n-1)$

圖 5　　nxn 方陣 L_k

3. 定義 $P=\{(i, j)\mid 1\le i, j\le n\}$，將 P 中 n^2 個有序對依特定次序(見下圖)放入一個 nxn 方陣 A：

(1,n)	(2,n)	(3,n)	…	(n,n)
⋮	⋮	⋮		⋮
(1,3)	(2,3)	(3,3)	…	(n,3)
(1,2)	(2,2)	(3,2)	…	(n,2)
(1,1)	(2,1)	(3,1)	…	(n,1)

圖 6　　nxn 方陣 A

4. 定義一個以 P 的子集合為元素的集合 B，其中每個元素皆包含 n 個有序對，B 所收集的元素如下所列出：

(1) A 的每一行的 n 個有序對所形成的集合收集到 B。

(2) A 的每一列的 n 個有序對所形成的集合收集到 B。

(3) 對於每一個 L_i, 每個元素 $1, 2, 3, \cdots, n$ 可決定 n 個於 A 中對應位置的有序對，將此 n 個有序對所形成的集合收集到 B。

則(P, B)是一個基數為 n 的 affine plane。

現以基數為 4 舉例如下：

1. 由質數多項式 $1+x+x^2$ 所生成的 finite field 之二元運算表如下：

+	0	1	x	$1+x$
0	0	1	x	$1+x$
1	1	0	$1+x$	x
x	x	$1+x$	0	1
$1+x$	$1+x$	x	1	0

·	0	1	x	$1+x$
0	0	0	0	0
1	0	1	x	$1+x$
x	0	x	$1+x$	1
$1+x$	0	$1+x$	1	x

圖 7　$1+x+x^2$所生成的 finite field 之二元運算表

將 0, 1, x 以及 $1+x$ rename 為 4, 1, 2, 以及 3，可得到新的二元運算表如下：

+	4	1	2	3
4	4	1	2	3
1	1	4	3	2
2	2	3	4	1
3	3	2	1	4

·	4	1	2	3
4	4	4	4	4
1	4	1	2	3
2	4	2	3	1
3	4	3	1	2

圖 8　$1+x+x^2$所生成的 finite field 之二元運算表(rename 後)

2. 由非零元素 1, 2, 3，我們分別做○(1), ○(2), ○(3)的運算，可獲得三個 4x4 方陣 L_1, L_2, L_3，如下：

○(1)	4	1	2	3
4	4	1	2	3
1	1	4	3	2
2	2	3	4	1
3	3	2	1	4

$i \cdot 1 + j$

○(2)	4	1	2	3
4	4	1	2	3
1	2	3	4	1
2	3	2	1	4
3	1	4	3	2

$i \cdot 2 + j$

○(3)	4	1	2	3
4	4	1	2	3
1	3	2	1	4
2	1	4	3	2
3	2	3	4	1

$i \cdot 3 + j$

圖 9　○(1), ○(2), ○(3)的運算

4	1	2	3
1	4	3	2
2	3	4	1
3	2	1	4

L_1

4	1	2	3
2	3	4	1
3	2	1	4
1	4	3	2

L_2

4	1	2	3
3	2	1	4
1	4	3	2
2	3	4	1

L_3

圖 10　4x4 方陣 L_1, L_2, L_3

3. $P=\{(i, j) \mid 1 \le i, j \le 4\}$，將 P 中 4^2 個有序對依特定次序(見下圖)放入 4x4 方陣 A：

14	24	34	44
13	23	33	43
12	22	32	42
11	21	31	41

圖 11　4x4 方陣 A

4. B 中的元素為 P 的子集合，且其大小為 4。其所收集到的元素如下：

(1) {11, 12, 13, 14}
{21, 22, 23, 24}
{31, 32, 33, 34}
{41, 42, 43, 44}

(2) {14, 24, 34, 44}
{13, 23, 33, 43}
{12, 22, 32, 42}
{11, 21, 31, 41}

L_1 {14, 23, 32, 41}
{13, 24, 31, 42}
{11, 22, 33, 44}
{12, 21, 34, 43}

L_2 {14, 21, 33, 42}
{12, 23, 31, 44}
{11, 24, 32, 43}
{13, 22, 34, 41}

L_3 {14, 22, 31, 43}
{11, 23, 34, 42}
{13, 21, 32, 44}
{12, 24, 33, 41}

則(P, B)是一個基數為 4 的 affine plane。

2.1.2 建構 balanced (λ=1)-PHF

一個balanced (λ=1)-PHF可由一個affine plane建構出來。且order為q的affine plane可建構出balanced (λ=1)-PHF$(q+1; q^2, q, w)$，滿足$q+1 > \binom{w}{2}$。並且，於接下來的論文中，我們將表示該PHF為PHF(q, w)。這裡所採用的建構方法在[9]有詳細的證明，而本篇論文僅就建構的方式作介紹。

假設我們已有了一個 order 為 q 的 affine plane(P, B)，則經由執行下列流程，我們可獲得一個 PHF(q, w) ，滿足 $q+1 > \binom{w}{2}$。

假設 $P=\{1, 2, \cdots, n^2\}$，定義 $A=\{1, 2, \cdots, n^2\}$以及 $Z=\{1, 2, \cdots, n\}$，對於 affine plane 的所有分割 P_i, i=1, 2, …, $q+1$，做下列動作。

定義一函式 f_j 由 A 到 Z 滿足以下性質：

(a) 對於 P_i 中的任一區塊 B_j ，以 B_j 中的點輸入到 f_j 皆得到同一 Z 中的值。

(b) 對於任屬於 P_i 中不同區塊的任兩點 a, b，皆有 $f_j(a) \neq f_j(b)$。

則 $F=\{f_1, f_2, \cdots, f_{q+1}\}$為一 PHF$(q, w)$。

以下同樣以基數為 4 來舉例：

承 2.1.1 小節所得到的 affine plane(P, B)，為了方便，我們可將 P 中 16 個 4x4 的二維元素(i, j)轉換為一維元素 k。以下是經由 $k=4(i-1)+j$ 做轉換後的 affine plane。

P = {1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16}

B = {

{1, 2, 3, 4}, {5, 6, 7, 8}, {9, 10, 11, 12}, {13, 14, 15, 16},
{4, 8, 12, 16}, {3, 7, 11, 15}, {2, 6, 10, 14}, {1, 5, 9, 13},
{4, 7, 10, 13}, {3, 8, 9, 14}, {1, 6, 11, 16}, {2, 5, 12, 15},
{4, 5, 11, 14}, {2, 7, 9, 16}, {1, 8, 10, 15}, {3, 6, 12, 13},
{4, 6, 9, 15}, {1, 7, 12, 14}, {3, 5, 10, 16}, {2, 8, 11, 13} }

觀察 B 中的元素，我們發現從第一個開始，每四個元素可組成一個 P 的分割，我們可針對每一分割定義一個函式，使得該分割所含元素中的點，會依序對應到 Z 中的每一個元素，也就是 1, 2, 3, 4。

例如，由第一個分割{{1, 2, 3, 4}, {5, 6, 7, 8}, {9, 10, 11, 12}, {13, 14, 15, 16}}，我們可以定義 f_1，使得

$f_1(1) = f_1(2) = f_1(3) = f_1(4) = 1$,
$f_1(5) = f_1(6) = f_1(7) = f_1(8) = 2$,
$f_1(9) = f_1(10) = f_1(11) = f_1(12) = 3$,
$f_1(13) = f_1(14) = f_1(15) = f_1(16) = 4$.

同理，我們可定義 f_2, f_3, f_4, f_5 如下：

$f_2(4) = f_2(8) = f_2(12) = f_2(16) = 1$,
$f_2(3) = f_2(7) = f_2(11) = f_2(15) = 2$,
$f_2(2) = f_2(6) = f_2(10) = f_2(14) = 3$,
$f_2(1) = f_2(5) = f_2(9) = f_2(13) = 4$;
$f_3(4) = f_3(7) = f_3(10) = f_3(13) = 1$,
$f_3(3) = f_3(8) = f_3(9) = f_3(14) = 2$,
$f_3(1) = f_3(6) = f_3(11) = f_3(16) = 3$,
$f_3(2) = f_3(5) = f_3(12) = f_3(15) = 4$;
$f_4(4) = f_4(5) = f_4(11) = f_4(14) = 1$,
$f_4(2) = f_4(7) = f_4(9) = f_4(16) = 2$,
$f_4(1) = f_4(8) = f_4(10) = f_4(15) = 3$,
$f_4(3) = f_4(6) = f_4(12) = f_4(13) = 4$;
$f_5(4) = f_5(6) = f_5(9) = f_5(15) = 1$,
$f_5(1) = f_5(7) = f_5(12) = f_5(14) = 2$,
$f_5(3) = f_5(5) = f_5(10) = f_5(16) = 3$,
$f_5(2) = f_5(8) = f_5(11) = f_5(13) = 4$.

於是，$F=\{f_1, f_2, f_3, f_4, f_5\}$為 PHF$(q, w)$，如下：

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
f_1	1	1	1	1	2	2	2	2	3	3	3	3	4	4	4	4
f_2	4	3	2	1	4	3	2	1	4	3	2	1	4	3	2	1
f_3	3	4	2	1	4	3	1	2	2	1	3	4	1	2	4	3
f_4	3	2	4	1	1	4	2	3	2	3	1	4	4	1	3	2
f_5	2	4	3	1	3	1	2	4	1	3	4	2	4	2	1	3

圖 12　PHF(4,3)

2.1.3 balanced（λ=1)-PHF 的性質

對於我們於本篇論文即將提出的架構，balanced（λ=1)-PHF 所具有的性質扮演了很重要的角色，於本節，我們將歸納並證明這些重要的性質。

一個 balanced（λ=1)-PHF 擁有下列的性質：

定理 2.1.1：

任兩點剛好於某一分割內屬於同一區塊。

證明：

由(λ=1)-PHF 的定義可以得知。

Q.E.D.

定理 2.1.2：

對於任一分割的任一區塊，其內的各點，在其他分割皆屬於不同區塊。

證明：

假設 B 為分割 P_i 的一個區塊。考慮 B 中各點在分割 $P_j, j \neq i$ 的情況，假設 B 中存在兩點 a, b 於 P_j 屬於同一區塊，則 a, b 於 P_i，P_j 皆屬於同一區塊，此與定理 2.1.1 的敘述矛盾。

故原假設有誤，即不存在 B 中的兩點，於其他分割 P_j 屬於同一區塊。也就是說，B 中的各點在其他分割皆屬於不同區塊。

Q.E.D.

定理 2.1.3：

承上，若扣除該區塊中的各點，則其他分割將無任何完整的區塊。

證明：

假設 B 為分割 P_i 的一個區塊，由定理 2.2，可得知 B 在其他分割 P_j 皆屬於不同區塊。由 balanced PHF 的定義可知 P_j 所含區塊個數，等同於 B 所含點個數。故若移除 B 中各點，其他分割 P_j 必無完整的區塊。

Q.E.D.

2.2 一個一般化的安全廣播模組

Fiat和Naor於[1]提出了一個廣播加密(Broadcast Encryption)方法，對於n個參與者的網路當中，此機制保證可以對任何n個參與者的子集合T作廣播，並且除T外的不超過k個參與者集合起來，也無法得知該廣播的訊息。除此之外，我們定義：對於一個廣播加密機制，考慮其所有可作廣播的集合T，若聚集除T外的不超過k個參與者，也無法解密該廣播的訊息，則稱這樣的一個機制為*k-resilient*。

定義 2.2.1：(*k-resilient*)

對於一個廣播加密機制，考慮其所有可作廣播的集合 T，若聚集除 T 外的不超過 k 個參與者，也無法解密該廣播的訊息，則稱這樣的一個機制為 *k-resilient*。

□

在 Fiat 和 Naor 的廣播加密方法中，於系統初始時，需要一個 TA 來產生並分派金鑰給所有的參與者，這些金鑰稱作 *prearranged key*，我們簡稱為 *pre-key*。利用這些 pre-key，每個參與者可以廣播(加密過後的訊息)給包含自己的任意數量的參與者，並且解密任何廣播給包含自己的子集合的訊息。

依不同的密碼學假設，Fiat 和 Naor 首先提出了不同的 *1-resilient* 機制。其中各個 *1-resilient* 機制會因為其假設的強弱不同，而需要在各個節點儲存不同的 pre-key 量。如表 1 所示，當不作任何密碼學的假設時，$w=n+1$，在各個 *1-resilient* 機制中，它需要在各個節點需要儲存最多的 pre-key；當假設單向雜湊函數存在時，$w=\log n$；當假設 extracting root modulo composite 很難時，$w=1$，此時各個節點需要儲存最少的 pre-key。

Fiat 和 Naor 提出了兩個 *k-resilient* 機制的廣播加密方法：One Level 機制以及 Multi-Level 機制。兩者都是由 *1-resilient* 機制所生成，並且，都需要在每次作安全廣播時，傳送額外的訊息(*1-resilient* 機制則否)。另外，One Level 機制及 Multi-Level 機制皆是採用了 PHF 的概念，其中 PHF($N;n,m,w$)可以用作產生一個滿足 *w-resilient* 的機制。

以下歸納整理此兩種機制於 n 個參與者，滿足 *k-resilient* 時，每個參與者所需要儲存的 pre-key 量，以及每個參與者為了廣播單一訊息所”實際”需要廣播的訊息量。

表 1　One Level 與 Multi-Level 的比較

	所需儲存的 pre-key 量	廣播所需的訊息量
One Level	$O(k \log n \cdot w)$	$O(k^3 \log n)$
Multi-Level	$O(k \log k \log n \cdot w)$	$O(k^2 \log^2 k \log n)$

資料來源：[1]

說明：當不預作任何密碼學假設時，$w=n+1$；當假設單向雜湊函數存在時，$w=\log n$；當假設 Factoring 很難時，$w=1$。

於本節剩下的部分，我們將簡單介紹One Level機制的運作方式，並且證明其滿足 *k-resilient*的特性。這裡的介紹是參考自 [1]。

假設我們有一個 PHF$(l;n,m,k)$ F: $f_1,...,f_l$, $f_i:U\to\{1,\cdots,m\}$，以及 $l\cdot m$ 個適用於 n 個參與者的 *1-resilient* 機制：$R(i,j), 1\le i\le l, 1\le j\le m$。則以下的建構方式可以產生 n 個參與者的 *k-resilient* 機制，稱之為 One Level 機制。

對於每一個參與者 $x\in U$，我們都給予其在 $R(i,f_i(x)), 1\le i\le l$ 所應獲得的 pre-key。當要傳送訊息 M給一個 U的子集合 T時，傳送端自行生成亂數字串 $M^1,...,M^l$，滿足 $\oplus_{i=1}^{l} M^i = M$。爾後，對於 $1\le i\le l, 1\le j\le m$，傳送端利用 $R(i,j)$傳送 M^i給一個擁有特殊權限的集合 $\{x\in T \mid f_i(x)=j\}$。

則每一個參與者 $x\in T$，都可以獲得 $M^1,...,M^l$，並且經由 XOR 運算來獲得原始訊息 M。

定理 2.2.2：

以上所述的機制(One Level 機制)為一個 *k-resilient* 機制。

證明：

對於所有收集不超過 k 個參與者且不含 T中參與者的集合 S來說，我們可以找到一個在 S上具有一對一特性的函式, $f_i, 1\le i\le l$。

在 *1-resilient* 機制 $R(i,j), 1\le j\le m$ 中，S最多只擁有一個參與者所擁有的 pre-key。故對於 $R(i,j), 1\le j\le m$，S皆無法得知 M^i。

因此，即使所有的 $M^{i'}, i'\ne i$ 都被取得，S仍然無法獲得原始的訊息 $M=\oplus_{i=1}^{l} M^i$。

Q.E.D.

由以上的討論可知，若 $R(i,j)$ 需要每個參與者儲存 w 的 pre-key 量，則 One Level 機制需要每個參與者儲存 $l\cdot w$ 的 pre-key 量，並且需要廣播的訊息量為 $l\cdot m\cdot R(i,j)$ 所需傳送的訊息量$=l\cdot m\cdot 1=l\cdot m$。

Fiat 和 Naor 證明了一個機率式的建構 PHF 方式，其中若 $m=2k^2$, $l=k\log n$，則

成功建構出 PHF($l;n,m,k$)的機率大於等於$1-\frac{1}{n^k}$。

總結 One Level 機制，它需要每個參與者儲存$O(k\log n\cdot w)$的 pre-key 量，需要廣播的訊息量則為$O(k^3\log n)$。

若想要了解Multi-Level機制的運作過程，請見[1]。

三、 ESBM（the Efficient Secure Broadcast Model）

於本章，我們將介紹一個適用在 PHF-based 臨界密碼系統的安全廣播模組：ESBM。於 3.1 節，我們介紹 ESBM 於 share renewal 時所扮演的作用與角色。在 3.2 以及 3.3 節，我們分別以文字描述與演算法的方式，說明 ESBM 的運作過程。3.4 節，我們針對 ESBM 作安全性分析，而 3.5 節，我們針對 ESBM 作容錯能力分析。其中安全性是指除了 ESBM 找到的 renewable subset 外，沒有其他任何一點能夠解密該 renewable subset 之間傳送的加密訊息；而容錯能力則是試著去找到一個下限，滿足若少於該下限的點發生錯誤或不存在，則 EBSM 將不會失敗，亦即可傳回一組 renewable subset 及其 common key。

3.1 應用層面考量

在 1.4.3 小節我們曾經介紹過 Proactive 秘密分享的概念。這個概念是著眼於一般的秘密分享中，各個參與者所擁有的 share，無論時間的遞嬗，並不會有所改變。這顯現了一個危機：攻擊者擁有無限的時間來想辦法一一獲取足夠多的 share，一旦攻擊者得到了超過臨界值的量，他便能夠還原回原始的秘密。

在 Proactive 秘密分享中，各個參與者所擁有的 share 會被定期更新，於是乎，攻擊者若是在兩次更新的時間區間內未能獲取足夠多的 share，在下一次作更新後，之前所獲得的 share 便沒有任何作用。藉此，可以達到更安全的秘密分享。

考量 PHF-based 臨界秘密分享的情形，也就是多個參與者可能被分配予相同的 share。此時，為了更新 share，我們需要於各個擁有相同 share 的 group 中，各選出一個 header node 出來，由這些 header node 之間的安全溝通，我們可以產生一組更新過後的 share(舉例：Proactive 秘密分享中，利用多項式同構的觀念來產生新的 share)。而由於 header node 需要將此更新的 share 安全地傳給同 group 的成員，所以同 group 成員之間的安全溝通也是需要的。

ESBM 提供了一個於更新秘密時，選擇 header node 的方法，並且，這個方法保證 header node 之間可以透過安全的廣播來決定新的 share，以及 header node 可以安全地將新的 share 傳給同 group 的成員。

3.2 ESBM 協定

ESBM 是一個針對 PHF-based 之臨界密碼系統的有效安全廣播模組。於本節，我們將會說明 ESBM 的運作環境及流程。

3.2.1 定義與表示法

如前所述，一個 balanced (λ=1)-PHF 可表為 PHF(q, w)，而 ESBM 將會運作在這樣的一個 PHF(q, w)上面。為了說明與分析時的簡便，在這篇論文內，我們將使用以下的定義及表示法。

定義 3.2.1：(*share*)

對於一個 PHF 中任意點 p，在各個分割都可以找到一個包含 p 的區塊 B，我們可經由區塊對應函式唯一對應到一個對應域的值，稱此值作該點於該分割的 share。

□

定義 3.2.2：(*renewable subset*)

對於一個 PHF 的任意分割，從每一個區塊各取出一點所形成的集合，稱作該分割的一個 renewable subset。

□

範例 3.2.3：share 與 renewable subset

對於以下 PHF(4;9,3,3)，我們列出幾個 share 與 renewable subset 的例子：

	1	2	3	4	5	6	7	8	9
f_1	1	1	1	2	2	2	3	3	3
f_2	1	2	3	1	2	3	1	2	3
f_3	1	2	3	3	1	2	2	3	1
f_4	1	2	3	2	3	1	3	1	2

點 4 的 share：f_1-2, f_2-1, f_3-3, f_4-2
點 6 的 share：f_1-2, f_2-3, f_3-2, f_4-1
點 7 的 share：f_1-3, f_2-1, f_3-2, f_4-3

f_1 的 renewable subset：{147}, {247}, {347}

□

定義 3.2.4：(*pair key*)

對於一個(λ=1)-PHF，任兩點會唯一擁有某一分割的相同 share，稱該 share 為該兩點間的 pair key。

□

定義 3.2.5：(*common key*)

對於一個 renewable subset，考慮其內的各點，若這些點於某一分割內擁有相同 share，則稱該 share 為此 renewable subset 的 common key。

□

範例 3.2.6：pair key 與 common key

對於以下 PHF(4;9,3,3)，我們列出幾個 pair key 與 common key 的例子：

	1	2	3	4	5	6	7	8	9
f_1	1	1	1	2	2	2	3	3	3
f_2	1	2	3	1	2	3	1	2	3
f_3	1	2	3	3	1	2	2	3	1
f_4	1	2	3	2	3	1	3	1	2

3,4 的 pair key：f_3-3
6,8 的 pair key：f_4-1
1,9 的 pair key：f_3-1

{147}是一個 f_1 的 renewable subset，其 common key 為 f_2-1
{267}是一個 f_1 的 renewable subset，其 common key 為 f_3-2
{123}是一個 f_4 的 renewable subset，其 common key 為 f_1-1

□

定義 3.2.7：(*完整區塊*)

若一個區塊內的點皆存在，則我們稱該區塊為一完整的區塊。

□

定義 3.2.8：(*n-pair key*)

對於一個點集來說，若其中有 n 個點在某分割擁有相同 share，則我們稱該點集於該分割有一個 n-pair key。

□

範例 3.2.9：n-pair key

對於以下 PHF(4;9,3,3)，我們列出幾個幾個點集，以及這些點集所含有的 n-pair key：

	1	2	3	4	5	6	7	8	9
f_1	1	1	1	2	2	2	3	3	3

f_2	1	2	3	1	2	3	1	2	3
f_3	1	2	3	3	1	2	2	3	1
f_4	1	2	3	2	3	1	3	1	2

{23456}在 f_1 有一個 2-pair key，以及一個 3-pair key
{6789}在 f_1 有一個 1-pair key，以及一個 3-pair key
{12457}在 f_1 有一個 1-pair key，以及兩個 2-pair key

□

3.2.2 ESBM 的運作流程

ESBM 的運作環境是一個 balanced (λ=1)-PHF，其目的是對於任意分割，都能夠找到至少一組擁有 common key 的 renewable subset，以讓該 renewable subset 可以藉此作安全的廣播。

以下我們將對 ESBM 的運作流程作一個簡單的概述。

考慮一個 PHF(q, w)，其可視為 q + 1 個{1, 2, …, q^2}的分割，假設為 P_1, P_2, …, P_{q+1}，每個分割有 q 個區塊，且每個區塊的大小為 q。對於任一分割 P_i，我們做下列動作，以找到 P_i 的一個擁有 common key 的 renewable subset：

(1) 依次探訪分割 P_{i+1}、P_{i+2}、…、P_{q+1}、P_1、P_2、…、P_{i-1}。

(2) 在目前探訪的分割中，依次探訪其內所有的區塊。

(3) 對於每一個探訪的區塊 B，需要決定其是否完整存在。若 B 是完整區塊，則我們找到了 B 為 P_i 的 renewable subset，其 common key 為 B 的 share，否則繼續探訪下一個區塊或分割。

在 ESBM 成功的執行後，會傳回 pair(S, k)，其中 S 是一個 renewable subset，k 是 S 的一個 common key。故 S 可以 k 利用來作安全的廣播。並且，如果有需要的話，S 中的每一個成員 s 也可以利用在 P_i 中的 share，來對其於 P_i 的同區塊成員作安全的廣播。

3.3 ESBM 演算法

為了實現 ESBM 的運作，我們設計了 ESBM 演算法。ESBM 演算法由兩個函式所構成，Is_Alive()以及 ESBM()。其中 ESBM()是 ESBM 演算法的主函式，而 Is_Alive()則是一個會被 ESBM()呼叫到的副函式。

於 3.3.1 小節我們介紹 Is_Alive()，並對其作相關討論；於 3.3.2 小節我們介紹 ESBM()，並對其作正確性的分析。

3.3.1 Is_Alive()函式

Is_Alive()是一個會被 ESBM()呼叫到的副函式，它接受的輸入是一個區塊，而演算法的內部是在對區塊內的每一點作測試，如果每一點都存在，會傳回 TRUE，否則就傳回 FALSE。

以下便是 Is_Alive()的演算法：

```
1   Procedure Is_Alive (B)
2   輸入：區塊 B
3   輸出：TRUE or FALSE
4
5   for (所有 B 中的點 b)
6       if (b 仍存在)
7           ;
8       else
9           return FALSE
10  return TRUE
```

而實際測試一個節點是否存在的方法，可透過 TCP/IP 中的網路層(Network Layer)或傳輸層(Transport Layer)所提供的服務來達成。舉例來說，我們可依據 TCP protocol 傳給一個節點的封包 Timeout 與否，來判斷該節點是否存在。

3.3.2 ESBM()函式

ESBM()的輸入為 PHF(q, w)中所有的分割，以及欲找 renewable subset 及其 common key 的分割的索引，其目的是找到該分割的一個 renewable subset 及其 common key，以便用在 share renewal 等的安全應用上。

以下是 ESBM()的演算法：

```
1   Procedure ESBM (P1, P2, …, Pq+1, i)
2   輸入：分割 P1, P2, …, Pq+1 ,    //來源是一個 balanced (λ=1)-PHF
3         i                          //欲作安全廣播的分割之索引 i
4   輸出：Pi 的一個 renewable subset B 及其 common key
5
6   for (Pj=Pi+1、Pi+2、…、Pq+1、P1、P2、…、Pi-1)
7       for (所有 Pj 中的區塊 B)
8           if (Is_Alive(B))    //B 為完整區塊
9               return (B, Share_Of(B))
10  return "FAIL"
```

ESBM()可能傳回的結果有二：順利傳回一個 pair(S, k)，其中 S 是一個點集，k 是一個 common key；以及”FAIL”字串，說明 ESBM()執行失敗，意味著它找不到任何的完整區塊。那麼，我們如何確知 S 的確是分割 P_i 的一個 renewable subset？如何確知 k 是此 renewable subset 的一個 common key 呢？以下我們將證明(S, k)的確是 P_i 的一個 renewable subset 及其 common key。

定理 3.3.1：

由 ESBM()所傳回的 pair(S, k)，其中 S 確為欲作安全廣播之分割 P_i 的一個 renewable subset，且 k 確為該 renewable subset 的一個 common key。

證明：

(1) 由 Procedure ESBM 的第七行及第八行，我們可以得知 S 為 P_j, $j \neq i$ 的一個完整區塊。由定理 2.1.3，可知若扣除 S 中的點，則 P_i 將無任何完整的區塊，又因為 ESBM 的輸入是一個 balanced PHF，故 $|S| = P_i$ 的區塊數。亦即 S 為從 P_i 中每一個區塊各取出一點所形成的集合，即 S 為 P_i 的一個 renewable subset。

(2) 由 Procedure ESBM 的第九行，可知 k 為區塊 S 的一個 share。因為 S 為的 P_i 一個 renewable subset，故 k 為 S 的一個 common key。

Q.E.D.

定理 3.3.1 保證了 ESBM()的正確性，也就是說，ESBM()傳回的 pair(S, k)的確是一個 renewable subset 及其 common key，它可以當作 share renewal 程式的一個副函式。

3.4 安全性分析

於本節中，我們將會針對 ESBM 的安全性作分析。其中安全性是指除了 ESBM 找到的 renewable subset 外，沒有其他任何一點能夠解密該 renewable subset 之間傳送的加密訊息。

定理 3.4.1：

假設 ESBM 傳回 pair(S, k)，則除了 S 之外的任一點，都無法解密 S 中成員互相傳遞的加密訊息。

證明：

由 Procedure ESBM 的第七行及第八行，我們可以得知 S 為 P_j, $j \neq i$ 的一個完整區塊，故除了 S 中成員外，不存在任何一點擁有 S 的 share。即若以 k 來作為 S 中成員互相傳遞訊息的加密金鑰的話，則任何一點都無法對訊息作解密。並且，此無法對訊息作解密的保證，是來自於所使用對稱式加密演算法的安全性。

Q.E.D.

3.5 容錯能力分析

於本小節，我們會定義何謂一次 ESBM 執行的失敗，並且，我們將分析並尋求一個下限值 n，滿足當錯誤或不存在的點個數少於 n 時，ESBM 將有百分之百的成功機率；反之，ESBM 可能失敗。

3.5.1：ESBM 失敗的定義

由前面討論，我們知道 ESBM 一次成功的執行，就是能夠找到一個 renewable subset 及其 common key。相對地來說，若是無法對於給定的分割，找到一個 renewable subset 及其 common key，是否就是 ESBM 的失敗呢？

我們可針對上面的情況：“無法對於給定的分割，找到一個 renewable subset 及其 common key”，再細分為下列兩種情形。情形一：該分割仍有 renewable subset，但 ESBM 無法為該 renewable subset 找到 common key。情形二：該分割已不存在 renewable subset。就情形二的情況，任何演算法都無法針對該分割找到一個 renewable subset 及其 common key，因為該分割已不存在任何的 renewable subset。故我們定義 ESBM 的失敗僅包含情形一，也就是針對一個仍有 renewable subset 的分割，無法找到其中一個 renewable subset 及其 common key。

定義 3.5.1：(*ESBM 的失敗*)

若對於一個仍有 renewable subset 的分割，ESBM 無法找到其中一個 renewable subset 及其 common key，則我們稱為 ESBM 於該分割的失敗。

□

範例 3.5.2：ESBM 的失敗

對於 PHF(4,3)，若點 1,4,5,6,9,11 發生錯誤或不存在，則 ESBM 於 P_1 無法找到一個 renewable subset，因為 $P_2, \cdots, P_5$ 中已無任何完整區塊。然而，此時 P_1 仍有 renewable subset。因此 ESBM 在 P_1 為失敗。如下圖：

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
f_1	1	1	1	1	2	2	2	2	3	3	3	3	4	4	4	4
f_2	4	3	2	1	4	3	2	1	4	3	2	1	4	3	2	1
f_3	3	4	2	1	4	3	1	2	2	1	3	4	1	2	4	3
f_4	3	2	4	1	1	4	2	3	2	3	1	4	4	1	3	2
f_5	2	4	3	1	3	1	2	4	1	3	4	2	4	2	1	3

圖 13　ESBM 失敗的例子

說明：上頭打星號的點代表發生錯誤或不存在，而 $P_2, \cdots, P_5$ 皆有四個不同的區塊元素不存在(被圈起來的地方)，故 $P_2, \cdots, P_5$ 皆無完整區塊。

□

3.5.2：欲分析的問題

於接下來的分析，我們將探討一個問題：在至少多少個點不存在的情形下，ESBM 有可能會失敗呢？換句話說，我們也為下面的問題尋求一個解答：在不存在的點的個數少於多少點的情形下，ESBM 一定會成功？

3.5.3：定義變數

為了方便分析時的討論，我們定義下列變數。

(1) q：PHF 的第一個參數，也就是說，輸入至 ESBM 的 PHF 為 PHF(q, w)。

(2) N：一個點的集合，若集合內的點皆不存在，則 ESBM 將會失敗。

(3) n：集合 N 的大小。

(4) p：不失一般性，我們假定欲尋找 renewable subset 及其 common key 的分割為 P_1，則在將 N 與 P_1 的各個區塊一一作交集所形成的集合中，其最大的元素大小為 p。

故我們想要問的問題便是：集合 N 的大小 n 至少要多小？

3.5.4：界定 n 的範圍

現在考慮 n 的範圍，假設 $n<q$，則任意分割都必存在至少一個完整區塊，ESBM 可找到該區塊並成功的傳回，所以 $n<q$ 不成立。假設 $n = q$，則在 $P_2, \cdots, P_{q+1}$ 中，N 中的 n 個點必屬於不同的區塊，由定理 2.1 可知，此 n 點必在 P_1 屬於同一區塊。但是，這種情況不在 ESBM 失敗的定義內，故 $n = q$ 不成立。

引理 3.5.3：

假設輸入至 ESBM 的分割的索引為 k，令 $P_k = \{B_1, B_2, \ldots, B_q\}$。對於所有能夠使 ESBM 失敗的集合 N，存在 $B_i \in P_k \ni \forall B_j \in P_k, j \neq i, |B_j \cap N| \leq |B_i \cap N|$。令 $B_i \cap N = \{u_1, u_2, \ldots, u_p\} = U$，$B_i - B_i \cap N = \{v_1, v_2, \ldots, v_{q-p}\} = V$。$\forall P_m, m \neq k$，可定義 $Q = \{$點 s 的 share$|s \in V\}$，$R = \{$點 s 的 share$|s \in N-U\}$，則有 $Q \subseteq R$。

證明：

因為 N 在輸入至 ESBM 的分割的索引為 k 時，能使 ESBM 失敗，故由定義 3.5.1 可知，N 必滿足下列條件：

1. $\forall B \in P_k$，$B - N \neq \varnothing$，即 $B \not\subset N$。

2. 對於 P_k 以外的其他分割 P_j，$\forall B \in P_j$，$|B - N| < |B|$，即 B 中至少有一元素屬於 N。

亦即若 N 中的點皆不存在，則 P_k 必仍有至少一個 renewable subset。

並且，若 N 中的點皆不存在，則 ESBM 將傳回”FAIL”，因為此時 $P_m, m \neq k$ 中已無任何完整的區塊。

考慮 $u_1, u_2, \ldots, u_p, v_1, v_2, \ldots, v_{q-p}$ 這 q 個點，由於在 P_k 擁有相同的 share，故在 $P_m, m \neq k$ 擁有不同的 share（定理 2.1.2）。假設 $N=\{u_1, u_2, \ldots, u_p, w_1, w_2, \ldots, w_{n-p}\}$，則由性質 2 可以推知，若 V 中有一點在 $P_m, m \neq k$ 擁有 share s，則 $N - U = W = \{w_1, w_2, \ldots, w_{n-p}\}$ 中也必有一點在 P_m 擁有 share s。亦即對於 P_m，可定義兩個收集 share 為元素的集合 $Q=\{$點 s 的 share $| s \in V\}$ 以及 $R=\{$點 s 的 share $| s \in N-U=W\}$，滿足 $Q \subseteq R$。

Q.E.D.

定理 3.5.4：

$n \geq q + p$

證明：

承引理 3.5.3，V 中任一點 s 在 $P_m, m \neq k$ 中共有 q 個 share。由定理 2.1.1，$N-U$ 中任一點 t 擁有 s 的一個 share。

因為 $Q \subseteq R$，故 $|N-U| \geq q$。

即 $|N| \geq q + |U|$

$\Rightarrow |N| \geq q+p$

$\Rightarrow n \geq q+p$

Q.E.D.

範例 3.5.5：$n=q+p$

若 $q=4$ 且 $N=\{1,4,5,6,9,11\}$，則由 p 的定義可知 $p=2$。假設 $B_i=\{1,2,3,4\}$，則由引理 3.5.3 可知，N 中除了 1,4 以外的點，需要擁有點 2,3 在 $P_2, \cdots, P_5$ 所擁有的 share。並且，N 中除 1,4 外的任一點，皆擁有點 2,3 中任一點在 $P_2, \cdots, P_5$ 所擁有的一個 share。而 2,3 中任一點在 $P_2, \cdots, P_5$ 共有四個 share，故起碼需要再增加 1,4 以外的四點（如下圖的 5,6,9,11），N 才能夠擁有點 2,3 在 $P_2, \cdots, P_5$ 所有的 share。如下圖所示：

	1	**2**	**3**	**4**	5	6	7	8	9	10	11	12	13	14	15	16
f_1	1	1	1	1	2	2	2	2	3	3	3	3	4	4	4	4
f_2	4	3	2	1	4	3	2	1	4	3	2	1	4	3	2	1
f_3	3	4	2	1	4	3	1	2	2	1	3	4	1	2	4	3
f_4	3	2	4	1	1	4	2	3	2	3	1	4	4	1	3	2
f_5	2	4	3	1	3	1	2	4	1	3	4	2	4	2	1	3

圖 14　$n=q+p$ 的範例

□

定理 3.5.6：

假設 $n = q + p$，則 $\binom{q+p}{2} \le q\binom{p+1}{2} + \left\lfloor \frac{q+p}{p} \right\rfloor \binom{p}{2} + \binom{q+p-\left\lfloor \frac{q+p}{p} \right\rfloor \cdot p}{2}$

證明：

已知 $n = q + p$，則可依之前的討論，假設 $V = \{u_1, u_2, \ldots, u_p, w_1, w_2, \ldots, w_q\}$，即除了 U 內元素外，再增加 q 點便可使 ESBM 失敗。　　(3.1)

考慮這 $q + p$ 個點，其所擁有的 pair key 個數恰為 $\binom{q+p}{2}$。以下將計算此 $q + p$ 個點在 $P_1, P_2, \cdots, P_{q+1}$ 所能夠擁有最多的 pair key，並以”最多的 pair key 量應大於等於 $\binom{q+p}{2}$” 這樣的事實，來為這 $q + p$ 個點的存在與否下一個定論。

考慮此 $q + p$ 個點在 P_j，$j \in \{2, 3, \cdots, q+1\}$ 的情形。對於 $w_1, w_2, \ldots, w_q$ 這 q 個點，可取出 $q - p$ 個點使其擁有 V 中點的所有 share，故此 $q - p$ 個點與 $u_1, u_2, \ldots, u_p$ 皆擁有不同 share。並且，此 $q - p$ 個點不與其他 p 個點中任一個擁有相同 share，否則除了 U 內元素外，至少須再增加 $q+1$ 個點，才可使 ESBM 失敗，這違反了(3.1)，故對於 P_j，$w_1, w_2, \ldots, w_q$ 中能夠用作 pair key 的點有 $q - (q - p) = p$ 個。而 $u_1, u_2, \ldots, u_p$ 這 p 個點在 P_j 皆皆擁有不同的 share，且與 $w_1, w_2, \ldots, w_q$ 內擁有 V 中 share 的 $q - p$ 個點也皆皆擁有不同的 share，故這 p 個點能夠用作 pair key 的點只有一個。總的來說，$u_1, u_2, \ldots, u_p, w_1, w_2, \ldots, w_q$ 這 $q+p$ 個點能夠用作為 pair key 的點有 $p + 1$ 個，使其為最多 pair key 的情形為一個$(p + 1)$-pair key，其 pair key 量為 $\binom{p+1}{2}$。又這樣的 P_j 共有 q 個，故於 $P_2, \cdots, P_{q+1}$，此 $q + p$ 個點

所能擁有最多的 pair key 量為 $q\binom{p+1}{2}$。

考慮此 $q+p$ 個點在 P_1 的情形。已知 N 中各點在 P_1 最多僅能有 p-pair key（由 p 的定義可以推知），故此 $q+p$ 個點於 P_1 所能擁有最多 pair key 的情形為 $\left\lfloor \frac{q+p}{p} \right\rfloor$ 個 p-pair key，以及一個 $(q+p-\left\lfloor \frac{q+p}{p} \right\rfloor * p)$-pair key，其 pair key 量為 $\left\lfloor \frac{q+p}{p} \right\rfloor \binom{p}{2} + \binom{q+p-\left\lfloor \frac{q+p}{p} \right\rfloor * p}{2}$。

所以，此 $q+p$ 個點最多擁有的量為 $q\binom{p+1}{2} + \left\lfloor \frac{q+p}{p} \right\rfloor \binom{p}{2} + \binom{q+p-\left\lfloor \frac{q+p}{p} \right\rfloor * p}{2}$，

由”最多的 pair key 量應大於等於 $\binom{q+1}{2}$”這樣的事實，我們可以得知以下不等式成立：

$$\binom{q+p}{2} \le q\binom{p+1}{2} + \left\lfloor \frac{q+p}{p} \right\rfloor \binom{p}{2} + \binom{q+p-\left\lfloor \frac{q+p}{p} \right\rfloor \cdot p}{2} \qquad (3.2)$$

Q.E.D.

範例 3.5.7：不等式(3.2)

假設 $q = 5$，考慮 $p = 2$ 是否可滿足 $n = q + p$ 使 ESBM 失敗。

代入(3.2)的左半，可得應有的 pair key 量：$\binom{7}{2}$=21。

代入(3.2)的右半，可得最大的 pair key 量：$5\cdot\binom{3}{2} + \left\lfloor \frac{7}{2} \right\rfloor \binom{2}{2} + \binom{7-\left\lfloor \frac{7}{2} \right\rfloor \cdot 2}{2}$

=15+3+0=18

因為 18<21，故不滿足(3.2)，亦即 $p = 2$ 時 $n = q + p = 7$ 不能使 ESBM 失敗。

同樣假設 $q = 5$，考慮 $p = 3$ 是否可滿足 $n = q + p$ 使 ESBM 失敗。

代入(3.2)的左半，可得應有的 pair key 量：$\binom{8}{2}$=28。

代入(3.2)的右半，可得最大的 pair key 量: $5\cdot\binom{4}{2}+\left\lfloor\frac{7}{3}\right\rfloor\binom{3}{2}+\binom{7-\left\lfloor\frac{7}{3}\right\rfloor\cdot 3}{2}$

=30+6+0=36

因為 36>28，故滿足(3.2)，亦即 $p = 3$ 時 $n = q + p = 8$ 能使 ESBM 失敗。

另外，一個滿足此 $n = q + p = 8$ 的實例為取 N ={1, 7, 11, 13, 15, 21, 24, 25}。

□

3.5.5：一個保持 n 為最小的增加點策略

若給定一個 p 值，可使得不等式(3.2)成立，則我們可能找到一個大小為 $q + p$ 的點集 N，滿足”若 N 中元素皆不存在，則 ESBM 會失敗”。

若給定一個 p 值，將使得不等式(3.2)不成立，則這表示我們不可能找到一個大小為 $q + p$ 的點集 N，滿足”若 N 中元素皆不存在，則 ESBM 會失敗”。換句話說，N 的大小至少應超過 $q + p$，才有可能滿足使 ESBM 失敗的需求。

考慮最單純的情況，假設目前的 p 值無法使不等式(3.2)成立，而我們打算再多取一點，即取 N 的大小為 $q + p + 1$。則一個即將面臨的問題是：多取的這一點要取在哪裡，才有比較大的機會使 ESBM 失敗？

我們有以下兩種選擇：

(請回憶之前曾定義過 $B_i \in P_1 \ni \forall B_j \in P_1, j \neq i, |B_j \cap N| \leq |B_i \cap N|$)

一．取點 n_k 滿足 $n_k \in B_i - B_i \cap N = B_i - \{u_1, u_2, ..., u_p\}$。

二．取點 n_k 滿足 $n_k \in B_j - B_j \cap N$，其中 $B_j \in \{B \mid B \in P_1, |B \cap N| < p\}$。

（在此要注意的是，假如使得 p 值增加一的是取點 n_k 在 $B_k, k \neq i$，我們仍能不失一般性地令 $i=k$，也就是從討論 B_i 變成討論 B_k。）

這兩個取點方式最關鍵的差別在於，選擇一將使 p 的值增加一，而選擇二保持 p 的原值。以下將證明：使用選擇一的方式來取點，可找到使 ESBM 失敗的一個下界。

假設 $|N| = q + p + 1 = n$ 且 $N = \{n_k, u_1, u_2, ..., u_p, w_1, w_2, ..., w_q\}$，其中 $u_1, u_2, ..., u_p, w_1, w_2, ..., w_q$ 的取法為目前為止討論的方法，則考慮以下事件：

E: N 中的點不包含 P_1 中的任一個區塊且擁有 $V = \{v_1, v_2, ..., v_{q-p}\}$ 在 P_2, …, P_{q+1} 中的所有 $q(q - p)$個 share。

T: 如果事件 E 成立，則其最大的 pair key 量大於等於 $\binom{|N|}{2}$。

定理 3.5.8：

若事件 E 成立，則事件 T 成立。即 $E \Rightarrow T$。

證明：

很容易可以得知，因為 N 中的點是從(λ=1)-PHF 選出，故其所含的 pair key 恰為 $\binom{|N|}{2}$，則 T 成立，定理 3.5.8 得證。

Q.E.D.

定義事件如下：

C_1：n_k 以選擇一的方式來選取。

C_2：n_k 以選擇二的方式來選取。

定理 3.5.9：

若事件 $C_2 \cap T$ 成立，則事件 $C_1 \cap T$ 成立。即 $C_2 \cap T \Rightarrow C_1 \cap T$。

證明：

考慮選擇一與選擇二，在事件 E 成立時，可能擁有最多的 pair key 個數。於 P_j，$j \in \{2, 3, \cdots, q+1\}$，兩者皆有$(q + p + 1) - q + 1 = p + 2$ 個點可以用作 pair key，使其為最多 pair key 的情形為$(p + 2)$-pair key。

於 P_1，選擇一最多可有一個$(p + 1)$-pair key，$\left\lfloor \frac{q}{p} \right\rfloor$ 個 p-pair key，以及一個 $\left(q - \left\lfloor \frac{q}{p} \right\rfloor * p\right)$-pair key。

同樣於 P_1，選擇二最多可有 $\left\lfloor \frac{q+p+1}{p} \right\rfloor$ 個 p-pair key，以及一個 $\left(q+p+1 - \left\lfloor \frac{q+p+1}{p} \right\rfloor * p\right)$-pair key。

由一些簡單的觀察，可以推知於 P_1，選擇一最多可有的 pair key 個數大於選擇二的。故於 $P_1, P_2, \cdots, P_{q+1}$，選擇一最多可有的 pair key 個數大於選擇二的，即若選擇二可滿足 T，則選擇一也可滿足。換句話說，若 $C_2 \cap T$ 成立，則 $C_1 \cap T$ 成立，定理 3.5.9 得證。

Q.E.D.

由定理 3.5.9，我們可以推知若打算從 $|N| = q + p$ 再增加一點，則若想要滿足 $|N| = q + p + 1$ 可能使 T 成立，理想的選擇是採用選擇一的取點方式。我們可以推廣至增加 k 個點的情況，也就是選擇一的取點方式為每次都取點 n_k 滿足 $n_k \in B_i - B_i \cap N$，其中 $B_i \in P_1 \ni \forall B_j \in P_1, j \neq i, |B_j \cap N| \leq |B_i \cap N|$。

由定理 3.5.9，我們可以很容易地推廣至以下結論。

推廣 3.5.10：

相較於其他所有方式，選擇一的取點方式可在 n 最小的情形下滿足 T。

□

考慮事件 S：若 N 中的點不存在，ESBM 將會失敗。

定理 3.5.11：

若 n 存在下限使其滿足 T，則 n 存在下限使其滿足 S。

證明：

n 存在下限使其滿足 T，即存在 t 滿足 $n \geq t$ 才能滿足 T。

假設 $n < t$ 時可能滿足 S，則由引理 3.5.3 及定理 3.5.8，可知 $n < t$ 時可能滿足 $E \Rightarrow n < t$ 時可能滿足 T，此與已知的敘述”$n \geq t$ 才能滿足 T”為矛盾。

故原假設不成立，即 $n \geq t$ 才能滿足 S，也就是 n 存在下限使其滿足 S。

Q.E.D.

由推廣 3.5.10 以及定理 3.5.11，我們可以很容易地推廣至以下結論。

推廣 3.5.12：

相較於其他所有方式，選擇一的取點方式可在 n 最小的情形下滿足 S。

□

由推廣 3.5.12 可知，以選擇一的方式來增加點到 N，可在 $|N|$ 最小的情形下使 ESBM 失敗。因為選擇一的增加點方式，其實是增加 p 值，故其是否擁有足夠 pair key 的判斷可交由式(3.2)來決定。如果式(3.2)成立，代表增加的 p 值(點的個數)已足夠多；如果式(3.2)不成立，則代表增加的 p 值(點的個數)仍不夠多。

3.5.6：總結

經由上面略嫌冗長的討論，我們終於能夠確定限制 $|N|=n$ 下限的一組方程式，為

$$n \geq q + p, p \in \mathbb{N}, \tag{3.3}$$

以及

$$\binom{q+p}{2} \leq q\binom{p+1}{2} + \left\lfloor \frac{q+p}{p} \right\rfloor \binom{p}{2} + \binom{q+p-\left\lfloor \frac{q+p}{p} \right\rfloor \cdot p}{2} \tag{3.4}$$

也就是說，當不存在的點的個數大於等於 n 時，ESBM 便有可能失敗，否則，ESBM 會有百分之百的成功機率。

[13]提到了一個與ESBM相類似的演算法，它與ESBM不同的地方在於，選取區塊的方

式為隨機選取。並且，[13]針對此演算法的容錯能力作了程式的模擬，其中失敗的定義與ESBM不同，改為”***找不到一個renewable subset，便是失敗，不管該分割目前有沒有renewable subset***”。

下表列出了在q=4,5，n=3,4,5,6,7,8 時，若套用 [13]的定義，ESBM的可能失敗情形個數：

表 2　　q與n的關係

	q = 3	q = 4	q = 5
n = 3	3	0	0
n = 4	18	4	0
n = 5	72	48	5
n = 6	75	312	100
n = 7	36	2224	950
n = 8	9	5838	7200

資料來源：[13]

由(3.3)及(3.4)，我們可以得知 q=3 時，使 ESBM 失敗的最小 n 值為 5； q=4 時，使 ESBM 失敗的最小 n 值為 6；q=5 時，使 ESBM 失敗的最小 n 值為 8。

考慮 q=3 的情形。表 2 中(q,n)=(3,3)時的失敗情形有 3 種，恰等於此時欲更新分割沒有 renewable subset 的選取點方法個數，為$3\cdot\binom{3^2-3}{3-3}$=3 種；表 2 中(q,n)=(3,4)時的失敗情形有 18 種，恰等於此時欲更新分割不含 renewable subset 的選取點方法個數，為$3\cdot\binom{3^2-3}{4-3}$=18 種。故我們可以得知 q=3, n<5 時確實不能使 ESBM 失敗，這與(3.3)、(3.4)吻合。並且，我們實際地找到一個 n=5 時，使 ESBM 失敗的選取點方式，為選取點 1,2,4,5,9。

考慮 q=4 的情形。表 2 中(q,n)=(4,4)時的失敗情形有 4 種，恰等於此時欲更新分割沒有 renewable subset 的選取點方法個數，為$4\cdot\binom{4^2-4}{4-4}$=4 種；表 2 中(q,n)=(4,5)時的失敗情形有 48 種，恰等於此時欲更新分割不含 renewable subset 的選取點方法個數，為$4\cdot\binom{4^2-4}{5-4}$=48 種。故我們可以得知 q=4, n<6 時確實不能使 ESBM 失敗，這與(3.3)、(3.4)吻合。並且，我們實際地找到一個 n=6 時，使 ESBM 失敗的選取點方式，為選取點 1,4,5,6,9,11。

考慮 q=5 的情形。表 2 中(q,n)=(5,5)時的失敗情形有 5 種，恰等於此時欲更新分割沒有 renewable subset 的選取點方法個數，為$5\cdot\binom{5^2-5}{5-5}$=5 種；表 2 中(q,n)=(5,6)時的失敗情形有 100 種，恰等於此時欲更新分割不含 renewable subset 的選取點方法個數，為$5\cdot\binom{5^2-5}{6-5}$=100 種；表 2 中(q,n)=(5,7)時的失敗情形有 950 種，恰等於此時欲更新分割不含 renewable subset 的選取點方法個數，為$5\cdot\binom{5^2-5}{7-5}$=950 種。故我們可以得知 q=5, n<8 時確實不能使 ESBM 失敗，這與(3.3)、(3.4)吻合。並且，我們實際地找到一個 n=8 時，使 ESBM 失敗的選取點方式，為選取點 1,7,11,13,15,21,24,25。

考慮最簡單的情況：q=2，我們可以很容易推知此時 ESBM 不可能失敗。另外，由以上討論，我們可以得知由(3.3)與(3.4)所推出的理論值，在 q=3、q=4 以及 q=5 時，與實際值吻合。

四 、 結果與比較

4.1 結果

於本節，我們將為第三章所介紹的 ESBM 做一個總結。

ESBM是適用在PHF-based的臨界密碼系統，考量Proactive秘密分享的概念，便有對各個share作更新的需求。由於PHF-based的臨界密碼系統可依share的分佈情況分成多個group(擁有同一個share的為處於同一group)，這些group在更新時，是需要從各個group中選出header node，並由這些header node，一起來決定如何更新share。因此，我們需要一個機制，以讓這些header node能夠安全並有效率地作溝通。然而，一個一般化的安全廣播機制[1]需要一個TA來產生及分配key(稱之為pre-key)，各個節點也需要儲存這些額外的pre-key，並且，針對單一個訊息，需要傳送額外的訊息來達到安全的目的。

而 ESBM 不需要節點儲存任何的 pre-key，因為它使用了 PHF-based 秘密分享的 share 來作為安全廣播的金鑰。另外，ESBM 不需傳送額外的訊息，而有效降低了更新 share 時的網路流量。

在建構一個利用到 ESBM 的 PHF-based 臨界密碼系統時，我們需要網路上節點的個數為一個 prime power，並且，當錯誤或不存在的點超過一個下限 n 時，ESBM 便有失敗的可能，限制 n 的不等式如下：

$n \geq q + p, p \in \mathbb{N}$，

以及

$$\binom{q+p}{2} \leq q\binom{p+1}{2} + \left\lfloor \frac{q+p}{p} \right\rfloor \binom{p}{2} + \binom{q+p-\left\lfloor \frac{q+p}{p} \right\rfloor \cdot p}{2}$$

由上述公式，我們可以得知一個使 ESBM 失敗的下限 n，也就是說，如果發生錯誤或不存在的點超過 n，ESBM 有可能失敗。由下表可以看出，n 與網路內節點數 t 的關係為 t 越大，$\frac{n-1}{t}$ 越小，也就是能夠系統中允許發生錯誤的節點比率越小。在 t 為 9 點時，系統中允許發生錯誤的節點比率為百分之四十四點四，而當 t 成長到 100 點時，系統中允許發生錯誤的節點比率為百分之十三。

表 3　ESBM 容許發生錯誤的節點數與全部節點數的關係

q	$t=q^2$	p	n	$(n-1)/t$
3	9	2	5	44.4%
4	16	2	6	31.3%
5	25	3	8	28.0%
6	36	3	9	22.2%
7	49	3	10	18.4%
8	64	3	11	15.6%
9	81	3	12	13.6%
10	100	4	14	13.0%

說明：固定 q，則可知共有 $t=q^2$ 個節點，表內為滿足式(3.2)的最小 p,n，以及系統中允許發生錯誤的節點比率 $(n-1)/t$。

4.2 比較

我們於 2.2 節曾經定義過 *k-resilient*，為對任何 n 個參與者的子集合 T 作廣播，並且除 T 外的不超過 k 個參與者集合起來，便無法得知該廣播的訊息。而由前面的討論可知 ESBM 滿足的不只是 *k-resilient*，而是就算所有除 T 外的參與者都集合起來，尚無法得知廣播的訊息。我們定義滿足上述特性的機制為具有 *perfect-resiliency*。

以下是 ESBM 與 Fiat,Naor 所提出的 One Level 以及 Multi-Level 機制所作的相關比較，我們假設此時各個節點已獲得了 PHF-based 秘密分享的 share：

表 4　ESBM 與 One Level,Multi-Level 的比較

	ESBM	One Level	Multi-Level
適用的節點數	prime power	無限制	無限制
需要 TA 與否	否	是	是
廣播的對象	renewable subset 之間、單一區塊的各個點之間	包含自己的所有節點的子集合	包含自己的所有節點的子集合
安全性	*perfect-resiliency*	*k-resiliency*	*k-resiliency*
需儲存的 pre-key 量	不需要	$O(k\log n\cdot w)$	$O(k\log k\log n\cdot w)$
廣播所需的訊息量	O(1)	$O(k^3\log n)$	$O(k^2\log^2 k\log n)$

資料來源：[1]

說明：當不預作任何密碼學假設時，$w=n+1$；當假設 one-way 函式存在時，$w=\log n$；當假設 Factoring 很難時，$w=1$。

4.3 貢獻

我們提出了一個適用在 PHF-based 之臨界密碼系統的安全廣播機制，稱之為 ESBM，它能夠提供各個 renewable subset 之間，以及單一區塊的各個點之間的安全廣播，並且相較於一個一般化的安全廣播機制，ESBM 不需要由一個 TA 來作 prearranged key 的分派，也就是說，除了原有的 share 外，各個點不需要額外儲存這些 prearranged key。同時，於廣播時所需要實際傳送的訊息量，相較於一般化的機制，ESBM 也少的多。

另外，為了分析 ESBM 的容錯能力，我們也證明了一個數學定理，此定理可以表達如下：

一個 order 為 q 的 affine plane 由一個大小為 q^2 的點(point)集 P 與一個大小為 q (q + 1)的集合 B 組成。同時，B 中任一元素 b 皆為 P 的子集合且 $|b|=q$。

B 可被分成 q + 1 個 P 的分割，且每個分割皆含有 q 個 B 中元素。假設此 q + 1 個分割為 P_1， P_2， …， P_{q+1}。

另假設一個 P 的子集合 Q，$|Q|=n$ 且滿足下列性質：

1. 對於某一分割 P_i，$\forall\, b \in P_i$，$b - Q \neq \varnothing$，即 b 不能包含於 Q。
2. 對於 P_i 以外的其他分割 P_j，$\forall b \in P_j$，$|b - Q| < |b|$，即 b 中起碼有一元素屬於 Q。

則 n 滿足下列不等式：

$n \geq q + p, p \in \mathbb{N},$

p 滿足下列不等式：

$$\binom{q+p}{2} \leq q\binom{p+1}{2} + \left\lfloor \frac{q+p}{p} \right\rfloor \binom{p}{2} + \binom{q+p-\left\lfloor \frac{q+p}{p} \right\rfloor \cdot p}{2}$$

五、 結論與展望

由 4.1 節的 表 3，我們可得知ESBM在系統內包含愈多節點數的情況下，其容錯能力愈低，因此，一個可適用於更大節點數之PHF-based臨界密碼系統的安全廣播模組，是未來有待研究及改進的課題。

另外，一個值得研究的方向是：相較於一般化安全廣播機制所擁有的 *w-resilient* 性質(針對 PHF(N;n,m,w))，ESBM 擁有 *perfect-resilient* 的性質，然而在節點數超過一定程度的情形時，ESBM 便無法避免地擁有較低的容錯能力。由於這樣的特性，我們有下面的猜想：是否能夠改進 ESBM，滿足系統內節點數較少時，擁有 *perfect-resilient* 的性質，而在系統內節點數較多時，犧牲一些 resiliency，來換取較大的容錯能力的可能呢？

參考文獻

[1] Amos Fiat and Moni Naor,"Broadcast Encryption", Lecture Notes in Computer Science **",** 773**,** pp.480 - 491**,** 1994.

[2] C.Siva Ram Murthy and B.S.Manoj,"Ad Hoc Wireless Networks: Architectures and Protocols", Prentice Hall Communications Engineering and Emerging Technologies Series, 2004.

[3] William Stallings,"Cryptography and Network Security:Principles and Practive",2nd edition,Prentice Hall, 1998.

[4] Douglas R.Stinson,"Cryptography: Theory and Practice", 3rd edition, Chapman & Hall/CRC, 2005.

[5] Elisabeth Oswald,"Introduction to Elliptic Curve Cryptography", Institute for Applied Information Processing and Communication, http://www.iaik.tugraz.at/aboutus/people/oswald/papers/Introduction_to_ECC.pdf, July 29, 2005.

[6] Vipul Gupta,Douglas Stebila,Stephen Fung,Sheueling Chang Shantz,Nils Gura,Hans Eberle,"Speeding up Secure Web Transactions Using Elliptic Curve Cryptography", In Proceedings of the Network and Distrubuted System Security (NDSS) Symposium, pp.231 - 239, 2004.

[7] W. Diffie and M.Hellman"Multiuser Cryptographic Techniques.", In Proceedings of the AFIPS National Computer Conference, pp.109 - 112, June 1976.

[8] C.C. Lindner,C.A. Rodger,"Design Theory", CRC Press LLC, 1997

[9] Kyung-Mi Kim,"Perfect Hash Families: Constructions and Applications", a thesis of Waterloo, Ontario, Canada, 2003.

[10] A.Herzberg, S.Jarecki, H.Krawczyk.M.Yung,"Proactive Secret Sharing Or: How to Cope With Perpetual Leakage", In Advances in Cryptology, Proc., Crypto'95, ser. LNCS, vol.936, pp.339 – 352.

[11] A.Shamir,"How to share a secret", Communications of the ACM, vol. 22, pp.612-613, 1979.

[12] S.R.Blackburn,"Combinatorics and Threshold Cryptography.In Combinatorial Designs and Their Applications", CRC Press, pp.49 - 70, 1999.

[13] Hung-Hsiang Hsu,"Efficient share renewal protocol design for mobile ad hoc network using perfect hash families",thesis for the degree of master in NCTU CSIE, 2006.