模糊傳輸協定

李榮三[1] 張真誠[1, 2]
[1]國立中正大學資訊工程學系暨研究所
電子郵件：ljs@cs.ccu.edu.tw
[2]逢甲大學資訊工程學系
電子郵件：ccc@cs.ccu.edu.tw

摘要

十年來，模糊傳輸已被視為密碼學上一項重要的訊息交換技術，主要的理由在於模糊傳輸的機制可以被應用在許多方面，好比說電子商務、秘密訊息交換或是傳送認證過的電子郵件等等。在一九八一年， Rabin 率先提出模糊傳輸的主要概念。我們可以將 Rabin 所提出的模糊傳輸協定視為一個遊戲，遊戲中有兩個參賽者，分別是 Alice 和 Bob，其中 Alice 代表訊息傳送端，Bob 代表訊息選擇端，遊戲一開始，Alice 傳送一個位元給 Bob，而 Bob 只有二分之一的機會能夠收到這個位元，另外二分之一的機會什麼也收不到。Rabin 提出的這個想法雖然簡單，但自從 Rabin 提出這個概念之後，很多學者專家爭相探討這個問題，試圖應用這個概念來解決其他問題，很快地，模糊傳輸受到了廣泛的注意，因而，它成為一項網路訊息交換的熱門研究題目。

模糊傳輸的發展過程主要分成三個階段：二選一的模糊傳輸協定，n 選一的模糊傳輸協定以及 n 選 t 的模糊傳輸協定。在本文中，我們將回顧近年來所發表的模糊傳輸協定，並進一步地探討模糊傳輸未來的發展方向。

第一節　緒論

隨著網路及通訊科技的日益發達，電子商務已逐漸成為商業行為的主流，利用網路或是無線通訊器材來從事商業交易，舉目可見。數位化的產品，更是充斥

著整個網路通訊世界；然而，隨之而起的便是網路通訊安全的威脅大增，病毒、害蟲與駭客無所不在，它們四處地攻擊伺服器、竊取資訊和毀壞個人電腦中所儲存的重要資訊，可謂無所不用其極地破壞網路世界。關係個人財務的電子商務行為以及個人隱私，往往是大部分惡意攻擊者的頭號目標。由於網路世界中人與人之間的互動，有別於我們日常生活中人跟人之間面對面的互動，於是許多通訊協定就被提出來保護網路通訊者在見不到彼此的情況下，可以安全地完成通訊或是交易行為。

好比在電子股票交易的應用上，為了要防止股票炒作的情況發生，下單的買家需要隱瞞他所購入的股票項目，於是，在整個電子交易過程中，除了買家與伺服器端的互相身份確認外，通訊協定必須做出適當的保護，使得伺服器端或是其他人無法得知買家的交易項目。模糊傳輸協定在這個地方就可以發揮它最貼切的功能，它除了確保買家可以正確地交易所選擇的股票項目之外，也可以防堵交易項目的外洩。以上所述的應用只是模糊傳輸眾多的應用之一，它的應用其實還相當廣闊，例如在訊息的查詢系統方面或是數位訊息的交易方面，都可以發揮很大的功用，也因此，模糊傳輸協定已儼然成為現代密碼學上一個相當重要的資訊交換安全機制[1, 3, 4, 5, 6]。

模糊傳輸的主要概念，最早由 Rabin 在一九八一年所提出[11]，我們可以將他當初所提出的概念想像成一個遊戲，遊戲中存在兩個參與者，Alice 和 Bob，由 Alice 發動這個遊戲，Alice 先傳送一個位元給 Bob，不過 Bob 只有一半的機會能夠得到 Alice 所傳送的位元，而有另一半的機率什麼也得不到。

Rabin 所提出的想法可以延伸為二選一的模糊傳輸協定，其中 Alice 傳送兩個位元 b_1 和 b_2 給 Bob，Bob 能夠選擇他想要得到的位元是 b_1 或是 b_2。不過，他只有一半的機率能夠得到他想要得到的那個位元，此外，Alice 也無法得知 Bob 在這本次的傳輸中所得到的位元為何。

接著，由 Brassard 等人提出了一個更有意義的模糊傳輸概念， n 選一的模糊傳輸協定，其中 Alice 擁有 n 個訊息，而 Bob 想要在本次的訊息傳輸中得到其

中的某一個訊息，與二選一的模糊傳輸協定相同地，Alice 無法得知 Bob 所獲得的訊息為何，而且，Bob 僅能得知他所想要得知的那筆訊息。

至今，許多的模糊傳輸協定被提出來增強模糊傳輸協定的功能與應用或是增加傳輸時的效率，最新的模糊傳輸協定的研究應屬 n 選 t 的模糊傳輸協定，其中傳送端 Alice 持有 n 個訊息，而選擇端 Bob 想要在一次的訊息傳輸中同時得到其中的 t 個訊息，然而，Alice 無法知道 Bob 所選擇的 t 個訊息為何，Bob 也無法得知除了此 t 個訊息以外的其他資訊。很不幸地，為了達到由 n 選 t 的模糊傳輸協定功能，大部分的改善方式不是需要平行處理的計算方式，就是得耗費很繁重的計算資源。

日本學者 Wakaha 教授和其學生 Ryota 在二零零四年共同提出一個安全的 n 選 t 的模糊傳輸協定[13]，他們所提出的模糊傳輸協定是架構在一個由 Naor 與 Pinkas 所提出的 n 選一的模糊傳輸協定上。雖然 Wakaha 和 Ryota 所提出的方法能夠安全地達到在一次的訊息傳輸中送方安全地同時傳送 t 個訊息給選擇端，他們所提出的協定在效率上的考量依然不足，而使得他們的方法難以被實際地應用推廣[1, 2, 7, 10, 12]。

第二節　n 選一的模糊傳輸協定之演進

繼 Rabin 提出模糊傳輸概念後，二選一的模糊傳輸協定是最早被提出來的[11]。它的基本定義如下：

Alice 表示訊息持有端也就是傳送端，Bob 表示選擇端，Alice 手中握有兩個位元 b_1 和 b_2，Bob 可以挑選他想要由 Alice 處獲得的位元，然而，他只有二分之一的機會能夠收到他想得到的位元，另外二分之一的機會得到的不是他想要的位元。除此之外，Alice 無法得知 Bob 所選擇的位元為何，且 Bob 也僅能收到一個位元而已。

二選一的模糊傳輸協定被提出以後，有關模糊傳輸的研究成果陸續地被發表

出來，一個較具代表性的里程碑就是 n 選一的模糊傳輸協定，這個時候的模糊傳輸協定已趨於成熟，定義也較完整[8, 9, 12]。

n 選一的模糊傳輸協定定義：

令 Alice 代表訊息傳送端，Bob 表示選擇端，Alice 手中握有訊息 $M_1, M_2, \ldots, M_n$，Bob 想要由 Alice 所持有的 n 個訊息中獲得某一個訊息，在傳輸過程結束後，整個傳輸協定必須達到下列三項要求：

需求一：傳輸項目的正確性

在傳輸程序結束後，模糊傳輸協定必須能夠確保選擇端能夠正確地獲得他所想要的資訊項目，而不可以是非其所要求的資訊。

需求二：選擇端的隱私安全

在傳輸程序結束後，模糊傳輸協定必須要能夠確保傳送端無法得知選擇端所挑選的資訊項目為何，如此才能保護選擇端的個人隱私。

需求三：傳送端的隱私安全

在傳輸程序結束後，模糊傳輸協定必須要能夠確保選擇端只能夠獲得他所挑選的資訊項目，而無法獲得其他非其選擇的資訊，如此才能確保傳送端的資訊安全。

底下，我們介紹在 2001 年由 Naor 和 Pinkas 所提出的 n 選一模糊傳輸協定，我們首先定義一些在他們所提出的協定中所使用的符號。 假設 g 是一個乘法群的產生器，g 的循環是質數 q。 Alice 表示傳送端，而 Bob 表示選擇端，$M_1, M_2, \ldots, M_n \in \langle g \rangle$ 是 Alice 所持有的 n 個訊息。 G 是一個大質數。Mc 是 Bob 所選的訊息，其中 c 是所選訊息的序號而且 $1 \le c \le n$。 Naor 和 Pinkas 所提出的 n 選一模糊傳輸協定之步驟如下：

步驟一： Bob 建立一個多項式

$$f(x) = x - c,$$

接著，他隨機地從 Z_q 中選出 a 和 b。

接下來，Bob 再造出另一個多項式如下：

$$f'(x) = f(x) + ab = x + (ab - c),$$

然後計算

$$e = ab - c。$$

最後，Bob 計算出下列結果

$$A = g^a \bmod G，$$

$$B = g^b \bmod G，$$

$$E = g^e \bmod G，$$

然後將{A, B, E} 這三個計算結果傳送給 Alice。

步驟二： 在接收到 Bob 所傳來的訊息後，Alice 計算出

$$Y_i = Eg^i \bmod G，i = 1，2 到 n。$$

接著，對於 i = 1，2 到 n，Alice 由 Z_q 中隨機地選出 s_i 和 r_i，然後執行下列計算：

$$H_i = A^{s_i} g^{r_i} \bmod G，$$

$$K_i = Y_i^{s_i} B^{r_i} \bmod G，$$

$$F_i = K_i * M_i \bmod G。$$

最後 Alice 將每一對(H_i, F_i) 傳送給 Bob，其中 i = 1，2 到 n。

步驟三： 當 Bob 接收到 Alice 所傳來的訊息後，他計算出

$$K_c = H_c^b \bmod G，$$

然後，利用這個計算結果來選取他真正想要的訊息如下，

$$M_c' = F_c / K_c \bmod G。$$

第三節　n 選 t 的模糊傳輸協定

有關模糊傳輸協定的最新研究就屬 n 選 t 的模糊傳輸協定了，由於它的應用範圍較廣泛，而且也較具有彈性，它已儼然成為密碼學上的研究重點了。完整的定義如下：

n 選 t 的模糊傳輸協定定義：

令 Alice 表示訊息傳送端，Bob 代表選擇端，Alice 手中握有訊息 $M_1, M_2, \ldots, M_n$，Bob 想要由 Alice 所持有的 n 個訊息中獲得其中 t 個訊息，在傳輸過程結束後整個傳輸協定必須達到下列三項要求：

需求一：傳輸項目的正確性

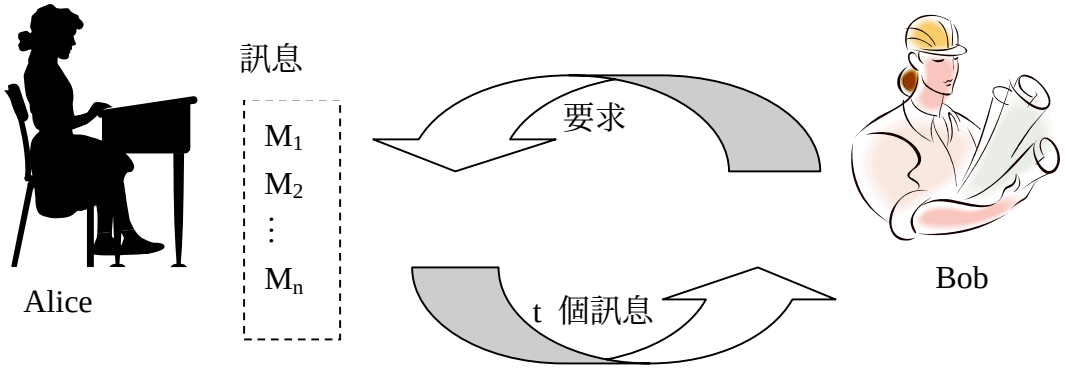
在傳輸程序結束後，模糊傳輸協定必須能夠確保選擇端能夠正確地獲得他所想要獲得的那 t 項資訊，而不可以是其他非其所求的資訊。

需求二：選擇端的隱私安全

在傳輸程序結束後，模糊傳輸協定必須要能夠確保傳送端無法得知選擇端所挑選的資訊項目到底為那 t 個，如此方能確保選擇端的個人隱私。

需求三：傳送端的隱私安全

在傳輸程序結束後，模糊傳輸協定必須能夠確保選擇端只能夠獲得他所選擇的那些資訊項目，而無法獲得其他非其選擇的資訊，如此才能確保傳送端的資訊安全。



圖一　n 選 t 的模糊傳輸協定

接著，我們介紹在 2004 年由日本學者 Wakaha 教授和其學生 Ryota 所提出的的由 n 選 t 的模糊傳輸協定[13]。我們首先定義一些在他們的協定中所使用的符號。假設 g 是一個乘法群的產生器，g 的循環是質數 q。Alice 表示傳送端，而 Bob 表示選擇端，$M_1, M_2, \ldots, M_n \in \langle g \rangle$ 是 Alice 所持有的 n 個訊息。 G 是一個大質數。$Mc_1, Mc_2, \ldots, Mc_t$ 是 Bob 所選擇的 t 個訊息，其中 $Mc_1, Mc_2, \ldots, Mc_t \in$

{$M_1, M_2, \ldots, M_n$}而且 $1 \leqq c_1, c_2, \ldots, c_t \leqq n$。 Wakaha 和 Ryota 所提出的 n 選 t 模糊傳輸協定之流程如圖一所示，其詳細步驟如下：

步驟一：Bob 建立一個多項式

$$f(x) = (x - c_1)(x - c_2) \ldots (x - c_t)。$$

接著，Bob 由 Z_q 中隨機地選出 $a, b_0, b_1, \ldots, b_{t-1}$。

然後造出另一個多項式 $f'(x)$如下：

$$f'(x) = f(x) + a(b_0 + b_1x + \ldots + b_{t-1}x^{t-1})。$$

假設 $e_0, e_1, \ldots, e_t$ 為多項式 $f'(x)$的係數，也就是說

$$e_0 = (-c_1)(-c_2) \ldots (-c_t) + ab_0，$$

$$\vdots$$

$$e_{t-1} = (-c_1 - c_2 - \ldots - c_t) + ab_{t-1}，$$

$$f'(x) = e_0 + e_1x + \ldots + e_{t-1}x^{t-1} + x^t。$$

接著 Bob 計算出下列結果

$$A = g^a \bmod G，$$

$$B_j = g^{b_j} \bmod G，\text{其中 } 0 \leq j < t，$$

$$E_j = g^{e_j} \bmod G，\text{其中 } 0 \leq j < t。$$

並且將這些計算後的結果{$A, B_0, B_1, \ldots, B_{t-1}, E_0, E_1, \ldots, E_{t-1}$}傳送給 Alice。

步驟二：當 Alice 接收到 Bob 所傳來的訊息後, 她便計算出

$$Y_i = E_0 E_1^i E_2^{i^2} \ldots E_{t-1}^{i^{t-1}} g^{i^t} \bmod G，\text{其中 } i = 1, 2 \text{ 到 } n。$$

對於 i = 1，2 到 n，Alice 由 Z_q 中隨機地選出 r_i 與 s_i，然後求出

$$H_i = A^{s_i} g^{r_i} \bmod G，$$

$$K_i = Y_i^{s_i} (B_0 B_1^i B_2^{i^2} \ldots B_{t-1}^{i^{t-1}})^{r_i} \bmod G，$$

$$F_i = K_i * M_i \bmod G。$$

最後，Alice 將每一對 (H_i, F_i) 傳送給 Bob，其中 i = 1，2 到 n。

步驟三：當 Bob 接收到 Alice 所傳來的訊息後，對於每一個 $i \in \{c_1, c_2, \ldots, c_t\}$，

Bob 以下列式子計算出 K_i'

$$K_i' = H_i^{b_0 + b_1 i + \ldots + b_{t-1} i^{t-1}} \mod G。$$

最後，Bob 利用所求出的 K_i'來取出他所要求的 t 個訊息如下，

$M_i' = F_i / K_i' \mod G$，其中 $i \in \{c_1, c_2, \ldots, c_t\}$。

第四節　結論與分析

前兩節所提到有關模糊傳輸協定，可以說是目前有關模糊傳輸機制較新的研究成果。很明顯地，重複執行 n 選一的模糊傳輸協定 t 次，也可以達到執行一次 n 選 t 的模糊傳輸協定的效果，不過，相較於 n 選一的模糊傳輸協定，n 選 t 的模糊傳輸協定在應用上還是具有較佳的彈性與實際效用。表一是針對上述提到的方法所做的比較，其中有關 Naor 與 Pinkas 所提的方法所需耗費的時間是以執行 t 次整個傳輸協定來計算的。表中的“ Exp ”表示一次的指數運算 ； n 表示 Alice 資料庫中的訊息總數 ; t 表示 Bob 想要選取的資料個數。

表一 第二節與第三節所提出的模糊傳輸協定在時間耗費上的比較

角色 / 傳輸協定	選擇端	傳送端
Naor 與 Pinkas	4t Exp	4(t*n) Exp
Wakaha 與 Ryota	(3t + 1) Exp	4n Exp

由表一，我們可以很清楚地瞭解到，相對於 Naor 與 Pinkas 所提出的協定，Wakaha 與 Ryota 所提出的模糊傳輸協定有明顯較好的效能。然而這樣的效能，在實作上依然稍嫌不足，它還是有一定的困難度存在，如果要以這種效能的模糊傳輸協定應用在無線網路的環境中更是困難重重。因此，要使得 n 選 t 的模糊傳

輸協定的應用能更廣闊、更切合實際的話，必須先降低傳送端與選擇端的指數運算量。這也是未來模糊傳輸協定的研究工作者必須積極努力的方向。

參考文獻

1. B. Aiello, Y. Ishai, and O. Reingold, “Priced oblivious transfer: how to sell digital goods,” *Proceedings of Advances in EUROCRYPT‘01*, Aarhus, Denmark, pp. 119-135, May 21-23, 2001.
2. M. Bellare and S. Micali, “Non-interactive oblivious transfer and applications,” *Proceedings of Advances in Crypto’89*, vol. 435, pp. 547-557, 1990.
3. C. Cachin, “On the foundations of oblivious transfer,” *Proceedings of Advances in Cryptography (EUROCRYPT ‘98)*, Espoo, Finland, pp. 361-374, May/June 1998.
4. G. D. Crescenzo, T. Malkin, and R. Ostrovsky, “Single database private information retrieval implies oblivious transfer,” *Proceedings of Advances in EUROCRYPT‘00*, Bruges, Belgium, pp. 122-138, May 2000.
5. J. A. Garay and P. D. MacKenzie, “Concurrent oblivious transfer,” *Proceedings of 41st Symposium on Foundations of Computer Science*, Redondo Beach, California, USA, pp. 314-324, 2000.
6. J. Kilian, “Founding cryptography on oblivious transfer,” *Proceedings of 20th ACM Symposium on Theory of Computing*, Chicago, USA, pp. 20-31, 1988.
7. N.Y. Lee and T. Hwang, “On the security of blind signature protocol using oblivious transfer,” *Computer Communications*, pp. 287-290, 1999.
8. M. Naor and B. Pinkas, “Oblivious transfer with adaptive queries,” *Proceedings of Advances in Crypto’99*, Santa Barbara, California, USA, pp. 573-590, August 1999.
9. M. Naor and B. Pinkas, “Distributed oblivious transfer,” *Proceedings of Advances in Asiacrypt‘00*, Kyoto, Japan, pp. 205-219, December 2000.

10. M. Naor and B. Pinkas, “Efficient oblivious transfer protocols,” *Proceedings of 12th Annual Symposium on Discrete Algorithms*, Washington, USA, pp. 448-457, 2001.
11. M. Rabin, “How to exchange secrets by oblivious transfer,” *Technical Report*, Aiken Computation Laboratory, Harvard University, 1981.
12. W.G. Tzeng, “Efficient 1-out-of-n oblivious transfer protocols with universally usable parameter,” *IEEE Transactions on Computers*, vol. 53, no. 2, pp. 232-240, February 2004.
13. O. Wakaha and S. Ryota, “k out of n oblivious transfer without random oracle,” *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E87-A, no. 1, pp. 147-151, January 2004.