改進一個匿名的用戶識別和密鑰分發技術協定

楊伏夷
朝陽科技大學資訊工程系
副教授
yangfy@cyut.edu.tw

劉鎮瑋
朝陽科技大學資訊工程系
研究生
s9727628@cyut.edu.tw

摘要

近年來，由於網際網路和資訊科技的快速發展，使用者只要透過網路就可獲得遠端服務供應者提供的相關服務。其中在 2009 年，Hsu 和 Chuang 提出一個新穎的用戶識別和密鑰分發保持匿名的分散式計算機網路，不僅達到交互驗證和匿名的安全特性，在效率方面也有所提升；然而，此方案在用戶識別階段，卻容易遭受共同模數攻擊。另一方面，Hsu 和 Chuang 協定中使用時間戳章來預防重送攻擊，因此表示需要設置同步時鐘，對於分散式系統也是額外的負擔。在本論文中，我們將提出改進方法來抵擋共同模數攻擊，並避免使用同步時鐘來降低系統的負擔，使得協定能擁有更完善的安全性，也更適合使用在分散式系統中。

關鍵詞：用戶識別、交互驗證、匿名性、Diffie-Hellmen。

1. 緒論

隨著網路技術的蓬勃發展與普及化，在網路上使用電子商務相關服務已經是日漸普遍。而在分散式網路環境中，透過不安全的通道來保密通訊是非常重要的議題。因此，用戶識別和秘密金鑰的發行在分散式網路環境中成為相當重要的一環。

在 1976 年 Diffie 和 Hellman[1]首先提出公開金鑰密碼系統的概念。此金鑰交換系統主要目的在於當網路上的雙方要進行通訊時，透過模指數運算，使得雙方獲得相同一把交談金鑰，以確保此次通訊的安全性，其安全性建立於解 Diffie-Hellman Problem 的數學難題上；然而，此協定容易遭受中間人攻擊，原因在於傳送端與接收端在通訊之前，沒有進行用戶識別，因此攻擊者可扮演其中一方來欺騙合法的傳送端或接收端。在 2004 年，Yang et al.[2]提出一個新的用戶識別和密鑰分配方案，提供使用者在公開的分散式網路環境中保有匿名之特性。隨後，Mangipudi 和 Katti[3]顯示 Yang et al. 提出的方案容易遭受到阻斷服務攻擊，攻擊者可竄改使用者的傳送資訊讓伺服器拒絕合法使用者的請求；Mangipudi 和 Katti 因此提出一個改進方案，利用數位簽章不易被竄改的特性加以保護欲傳送的訊息，來抵擋阻斷服務攻擊。在 2009 年，Hsu 和 Chuang[4]指出 Yang et al. 與 Mangipudi 和 Katti 的方案容易遭受到用戶公開攻擊，攻擊者可藉由公開的資訊來找出合法使用者為誰；Hsu 和 Chuang 因此提出一個適合於分散式計算機網路的用戶匿名識別和密鑰分發技術協定，不僅改善了 Mangipudi 和 Katti 協定上的缺陷，並且提議的方案更具有效率。

在本篇論文中，我們將指出 Hsu 和 Chuang 方案容易遭受共同模數攻擊，為了解決這些問題，我們提出一個改進方案。此提議方案比前述方案減少一回合的通訊，也達到雙方交互驗證，並且解決了 Hsu 和 Chuang 協定易遭受共同模數攻擊的問題。

第二章節回顧 Hsu 和 Chuang 協定，第三章節分析 Hsu 和 Chuang 方案的漏洞並提出攻擊方法，第四章節將說明我們所提出的方案，第五章節分析該方案之安全特性，最後第六章節將結論本篇文章。

2. 回顧 Hsu 和 Chuang 方案

Hsu 和 Chuang 提出一個適用在分散式計算機網路的用戶匿名識別和密鑰分發技術協定。此系統運作可分為三個階段：1.系統初始階段。2.註冊階段。3.用戶識別階段。協定中的參與者包括：使用者 U_i，服務供應者 P_j 以及可信任的第三方 *SCPC* (Smart card producing center)。

2.1 系統初始階段

- p,q：可信任的第三方所選取兩個隨機大質數 p 和 q。
- N：為二質數相乘之乘積，換言之，$N = p \cdot q$ 而 N 為往後計算的共同模數。

- g：由 Z_N^* 中所選取的元素，g 是 Z_p^* 與 Z_q^* 之原根。
- e：可信任的第三方之公開金鑰，且 $e \in Z_N^*$ 。
- d ：可信任的第三方之私密金鑰，且 $e \cdot d = 1 \bmod \phi(N)$ 。
- K_{ij} ：為使用者與服務供應者共享之交談金鑰。
- $E(\cdot), D(\cdot)$ ：對稱式加密與解密函數。
- $h(\cdot)$ ：單向無碰撞雜湊函數。
- $\|$ ：位元串接運算符號。

2.2 註冊階段

首先，使用者(或服務供應者)必須傳送身份資訊 ID_i 給可信任的第三方進行註冊動作，然後可信任的第三方使用秘密金鑰 d 計算 $S_i = ID_i^d \bmod N$ ，並將 S_i 發給使用者(或服務供應者)為日後身份驗證之用。此註冊階段通訊過程皆在安全通道中傳送。並以圖一表示之：

2.3 用戶識別階段

在此階段，若使用者想獲得服務供應者所提供之服務時，則必須與服務供應者達成協商交談金鑰以及交互驗證。其通訊過程如下所示，並以圖二表示之。

步驟 1

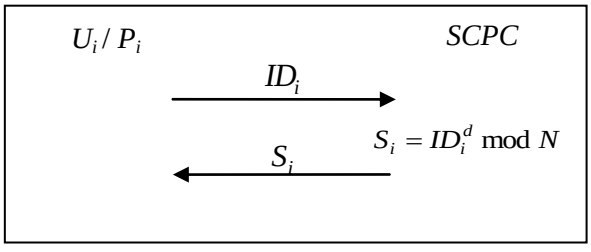
首先，使用者必須傳送服務請求(*Service Request*)給服務供應者。

步驟 2

服務供應者收到使用者的服務請求後，從 Z_N^* 選擇一個隨機亂數 k ，並使用自己的私密參數 S_j 計算 $Z = g^k \cdot S_j \bmod N$ ，隨後傳送 (Z) 給使用者。

步驟 3

當使用者收到訊息 (Z) 後，利用服務供應者公開之身份資訊計算 $a = Z^e \cdot ID_j^{-1} \bmod N$ ，接著從 Z_N^* 選擇一個隨機亂數 t，產生使用者與服務供應者共享之交談金鑰 $K_{ij} = a^t \bmod N$，並計算 $w = g^{e \cdot t} \bmod N$ 以及 $x = S_i^{h(K_{ij} \| Z \| w \| T)} \bmod N$ ，最後使用交談金鑰 K_{ij} 對身份資訊 ID_i 加密產生 $y = E_{K_{ij}}(ID_i)$ ，且傳送訊息 (w, x, y, T) 給服務供應者。其中 T 表示當下所選取的時間戳章。



圖一 Hsu 和 Chuang 方案之註冊階段

步驟 4

當服務供應者收到 (w, x, y, T) 後，驗證時間戳章 T 是否在合法之延遲範圍內，若不合法則終止此次通訊。接著利用所選取的亂數 k 計算出交談金鑰 $K_{ij} = w^k \bmod N$ ，將收到的密文解密得到使用者之身份 $ID_i = D_{K_{ij}}(y)$ ，並且以驗證式 $ID_i^{h(K_{ij} \| Z \| w \| T)} \stackrel{?}{=} x^e \bmod N$ 來驗證所計算出之資訊 ID_i ，設若通過上述驗證，則表示此次通訊的使用者擁有合法身份，反之則結束此次通訊；接著服務供應者會選取一個當下的時間戳章 T' 並計算 $D_i = h(K_{ij} \| T' \| Z \| ID_i \| ID_j)$ ，然後傳送訊息 (D_i, T') 給使用者。

步驟 5

當使用者收到訊息 (D_i, T') 時，驗證時間戳章 T' 是否在合法之延遲範圍內，若不合法則終止此次通訊。接著使用者計算 $D_i' = h(K_{ij} \| T' \| Z \| ID_i \| ID_j)$ 後，驗證所產生之訊息 $D_i' \stackrel{?}{=} D_i$ 是否相等，若相等則代表此次通訊的服務供應商為合法，反之則中斷此次通訊。

3. 討論

本章節將指出 Hsu 和 Chuang 提出的方案存在安全漏洞，並且針對協定的漏洞提出了攻擊方法。在以下的內容中，將顯示攻擊者多次的攔截公開資訊 (w, x, y, T) 後，即可計算出使用者之秘密參數 S_i，其過程如下：

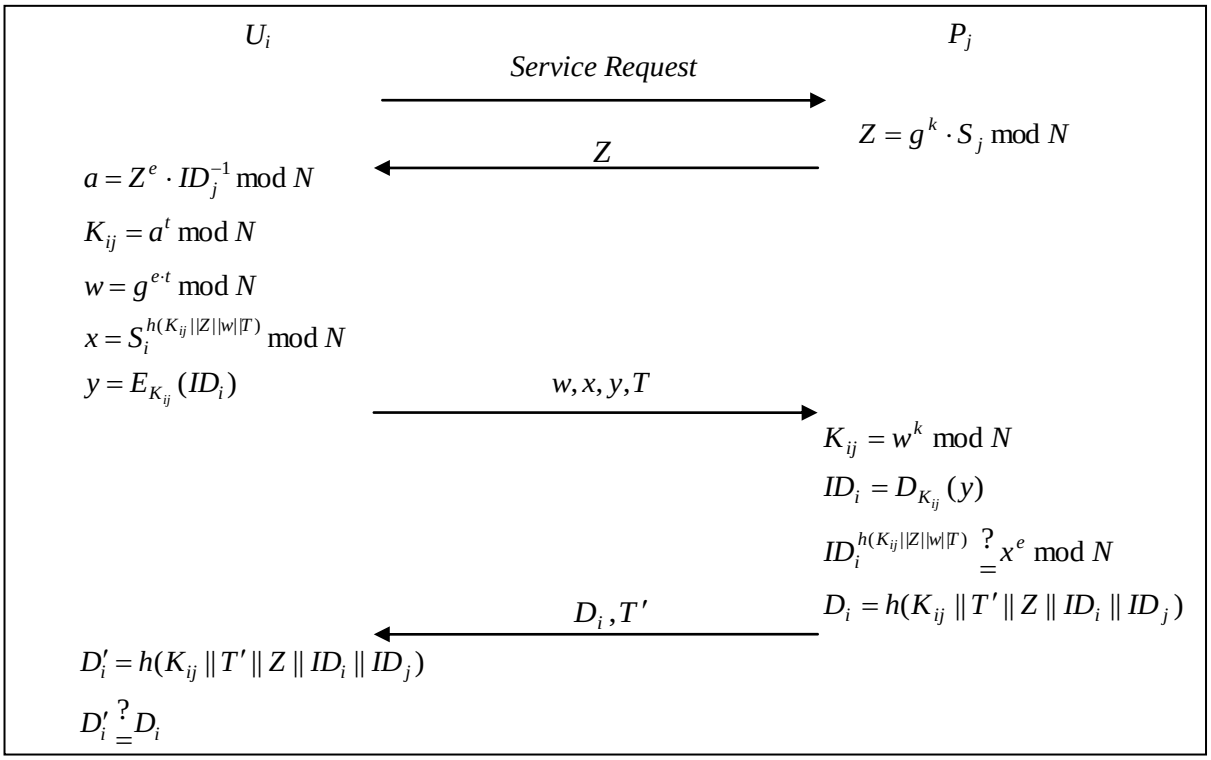
共同模數攻擊(Common modulus attack)

若使用者與服務供應者在公開通道傳送訊息，而攻擊者在每一次的通訊過程攔截訊息 (w, x, y, T) ，並從中選擇兩組訊息 x_1 及 x_2 ：

$$x_1 = S_i^{h(K_{ij_1} \| Z_1 \| w_1 \| T_1)} \bmod N,$$

$$x_2 = S_i^{h(K_{ij_2} \| Z_2 \| w_2 \| T_2)} \bmod N.$$

令 $h_1 = h(K_{ij_1} \| Z_1 \| w_1 \| T_1)$ ，$h_2 = h(K_{ij_2} \| Z_2 \| w_2 \| T_2)$。設 $h(\cdot): \{0,1\}^* \to \{0,1\}^l$，即映射任意長度字串至 l 位元字串，所以 $h(\cdot)$ 映射出來之數值最大不超過 2^l ，因為 $1 \sim 2^l$ 間之



圖二 Hsu 和 Chuang 方案之用戶識別階段

質數至少有 $\frac{2^l}{(\ln 2^l)}$ 個，故 h_1 是質數的機率至少為 $\frac{\left(2^l / \ln 2^l\right)}{2^l} = \frac{1}{\ln 2^l}$ ，所以 h_1 與 h_2 互質之機率至少為 $\left(\frac{1}{\ln 2^l}\right)^2$ 。以 SHA-1 為例 $l = 160$，故 (h_1, h_2) 互質之機率 $> \frac{1}{160^2}$ 。當 (h_1, h_2) 互質時，則滿足條件式 $\gcd(h_1, h_2) = 1$，利用擴充歐幾里德演算法(Extended Euclidean Algorithm)可計算得到整數 a 和 b 使得 $a \cdot h_1 + b \cdot h_2 = 1$，從 x_1 和 x_2 的式子，可得 $x_1^a \cdot x_2^b = S_i^{a \cdot h_1 + b \cdot h_2} \bmod N = S_i \bmod N$。如此一來，攻擊者在擁有足夠訊息的情況下即可輕易算出合法使用者之秘密參數 S_i，因此攻擊者就可扮演合法的使用者來欺騙服務供應商以獲得相關之服務。

4. 我們的協定

在本篇文章，我們將運用 Diffie-Hellmen 公開金鑰技術來確保協定之安全性，並且透過使用者與服務供應者所共享之交談金鑰來交互驗證彼此身份，設若攻擊者想要藉由公開資訊來計算出合法的交談金鑰是很困難的，因為攻擊者必須面臨解 Diffie-Hellmen 的數學問題。

提出方案的系統運作分為三個階段：1.系統初始階段，2.註冊階段，3.用戶識別階段，協定中的參與者包括：使用者 U_i，服務供應者 P_j 以及可信任的第三方 *SCPC*。並增加系統參數；$H(\cdot)$ 為單向無碰撞雜湊函數。系統設置參數 $(p, q, N, g, e, d, K_{ij})$ 與註冊階段則如同 Hsu 和 Chuang 的協定。底下我們將闡釋用戶識別階段。

4.1 用戶識別階段

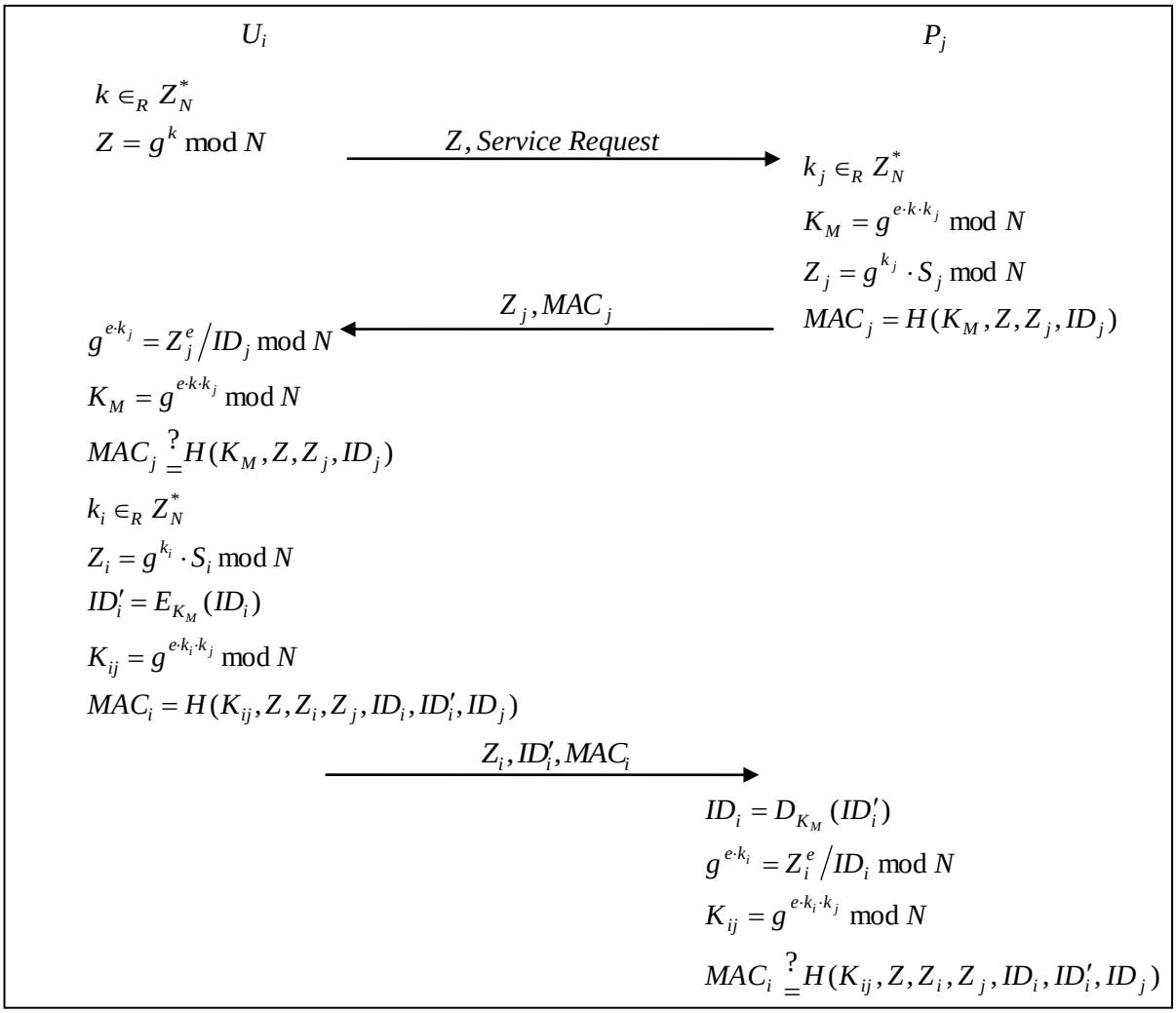
在此階段，當使用者想獲得服務供應者所提供之服務時，則必須與服務供應者達成交互驗證，並且共同產生交談金鑰 $K_{ij} = g^{e \cdot k_i \cdot k_j} \bmod N$。其通訊階段之流程將會詳細敘述如下。並以圖三表示之：

步驟 1

使用者從 Z_N^* 選擇一個隨機亂數 k，並且計算 $Z = g^k \bmod N$，隨後傳送服務請求資訊 $(Z, Service\ Request)$ 給服務供應者。

步驟 2

服務供應者從 Z_N^* 選擇一個隨機亂數 k_j，產生會議金鑰 $K_M = Z^{e \cdot k_j} = g^{e \cdot k \cdot k_j} \bmod N$，並使用自己的私密參數 S_j 計算 $Z_j = g^{k_j} \cdot S_j \bmod N$，



圖三用戶識別階段

最後計算驗證訊息 $MAC_j = H(K_M, Z, Z_j, ID_j)$，並且傳送訊息 (Z_j, MAC_j) 給使用者。

步驟 3

當使用者收到訊息 (Z_j, MAC_j) 後，利用服務供應者之身份資訊計算出 $g^{e \cdot k_j} = Z_j^e / ID_j \bmod N$，接著運用 $g^{e \cdot k_j}$ 計算出會議金鑰 $K_M = g^{e \cdot k_j \cdot k} \bmod N$，並驗證所產生之訊息 $MAC_j \stackrel{?}{=} H(K_M, Z, Z_j, ID_j)$ 是否相等，若相等則代表此次通訊的服務供應者為合法，反之則結束此次通訊；使用者從 Z_N^* 選擇一個隨機亂數 k_i，並使用自己的私密參數 S_i 計算出 $Z_i = g^{k_i} \cdot S_i \bmod N$，接著將會議金鑰 K_M 對身份資訊 ID_i 加密得到匿名的身份資訊 $ID_i' = E_{K_M}(ID_i)$，最後將服務供應者資訊 $g^{e \cdot k_j}$ 與隨機亂數 k_i 來計算使用者與服務供應者共享之交談金鑰 $K_{ij} = g^{e \cdot k_i \cdot k_j} \bmod N$ 以及計算驗證訊息 $MAC_i = H(K_{ij}, Z, Z_i, Z_j, ID_i, ID_i', ID_j)$，並且傳送訊息 (Z_i, ID_i', MAC_i) 給服務供應者。

步驟 4

當服務供應者收到訊息 (Z_i, ID_i', MAC_i) 時，使用事先產生之會議金鑰 K_M 對匿名之身份資訊 ID_i' 解密得到使用者的身份資訊 $ID_i = D_{K_M}(ID_i')$，並計算出使用者之相關訊息 $g^{e \cdot k_i} = Z_i^e / ID_i \bmod N$，接著運用 $g^{e \cdot k_i}$ 與隨機亂數 k_j 計算出使用者與服務供應者共享之交談金鑰 $K_{ij} = g^{e \cdot k_i \cdot k_j} \bmod N$，最後驗證所產生之訊息 $MAC_i \stackrel{?}{=} H(K_{ij}, Z, Z_i, Z_j, ID_i, ID_i', ID_j)$ 是否相等，若相等則代表此次通訊的使用者為合法，反之則結束此次通訊。

5. 安全分析

在本章節中，將分析上述的攻擊方法是否

也對我們所提出的方案造成威脅，以及一些常見的攻擊方法與安全需求，如下所示:

5.1 共同模數攻擊

若攻擊者想要從每次的通訊過程中攔截其訊息 (Z_i, ID_i', MAC_i) 進行共同模數攻擊，來計算出使用者的秘密參數 S_i 是不可行的。在我們的協定中，使用者會從 Z_N^* 選取隨機亂數 k_i，並計算 $Z_i = g^{k_i} \cdot S_i \bmod N$。若攻擊者想要計算出秘密參數 S_i 是非常困難的，因為每次通訊皆使用不同的 k_i 來達到混淆 S_i 之目的。

5.2 重送攻擊

設若攻擊者在使用者與服務供應者通訊過程中攔截合法訊息 (Z_i, ID_i', MAC_i)，並於下次通訊時執行重送攻擊，這是非常困難的。由於使用者與服務供應者在每次通訊時，雙方都會重新選擇隨機亂數 k_i 與 k_j，因此每次通訊產生的交談金鑰都會不同，所以攻擊者無法由先前攔截的訊息，假冒使用者或服務供應者來進行通訊；在此條件之下，我們的協定是可抵擋重送攻擊的。

5.3 偽造攻擊

一方面若攻擊者想要偽造服務供應者的合法資訊 (Z_j, MAC_j)，來使得使用者驗證成功這是不可能的，因為 $Z_j = g^{k_j} \cdot S_j \bmod N$ 包含服務供應者的秘密參數 S_j，而秘密參數 S_j 則是經由安全通道所取得的，因此攻擊者在不知道秘密參數 S_j 的情況下，就無法計算出相對應的服務供應者資訊來通過驗證式 $MAC_j \stackrel{?}{=} H(K_M, Z, Z_j, ID_j)$。另一方面，若攻擊者想要偽造使用者的合法資訊 (Z_i, ID_i', MAC_i) 來欺騙服務供應者也是不可行的，因為攻擊者也同樣無法獲得使用者的秘密參數 S_i，所以攻擊者依然無法計算出相對應之使用者資訊來通過驗證式 $MAC_i \stackrel{?}{=} H(K_{ij}, Z, Z_i, Z_j, ID_i, ID_i', ID_j)$。

5.4 已知的金鑰安全

在此協定中，交談金鑰的建立能夠保護使用者與服務供應者此次的訊息交換，而交談金鑰 $K_{ij} = g^{e \cdot k_i \cdot k_j} \bmod N$ 是由隨機亂數 (k_i, k_j) 產生，並且每次的通訊都會重新產生隨機亂數 (k_i, k_j)；如此一來，攻擊者即使攔截到此次的交談金鑰，依然無法由此次的交談金鑰解開之前通訊的交談內容。

5.5 使用者匿名性

任何人都無法由公開的資訊來找出合法使用者為誰，因為使用者將透過會議金鑰 K_M 對其身份資訊加密，得到匿名身份資訊 $ID_i' = E_{K_M}(ID_i)$，只有合法的服務供應商才知道相對應的會議金鑰 K_M 對匿名身份資訊解密，獲得使用者的真實身分 $ID_i = D_{K_M}(ID_i')$。因此任何人在不知道會議金鑰 K_M 的情況下就無法計算出使用者的真實身份。

6. 結論

在本篇文章，我們發現 Hsu 和 Chuang 所提議的方案，容易遭受共同模數攻擊，攻擊者可以扮演合法的使用者來使用服務供應者所提供的服務，為了解決 Hsu 和 Chuang 方案中存在的問題，我們提出一個改進方案，來抵擋這樣的攻擊;而通訊次數僅需要三回合就能達到交互認證，與 Hsu 和 Chuang 方案相較之下減少一回合通訊次數，以降低使用者與服務供應者等待驗證的時間。此外，在驗證協定中並未使用時間戳章，免除分散式系統使用同步時鐘之困擾，因此我們提出的方案也更適合在分散式電腦網路環境內運用。

參考文獻

[1] Diffie, W. and Hellman, M., "New directions in cryptography," ***IEEE Transactions on Information Theory***, Vol. 22, Issue 6, pp.644-654, 1976.

[2] Yang, Y., Wang, S., Bao F., Wang, J. and Deng, R.H., "New efficient user identification and key distribution scheme providing enhanced security," ***Computers & Security***, Vol. 23, Issue 8, pp.697-704, 2004.

[3] Mangipudi, K. and Katti, R., "A Secure Identification and Key agreement protocol with user Anonymity (SIKA)," ***Computers & Security***, Vol. 25, Issue 6, pp.420-425, 2006.

[4] Hsu, C.L. and Chuang, Y.H., "A novel user identification scheme with key distribution

preserving user anonymity for distributed computer networks," ***Information Sciences***, Vol. 179, Issue 4, pp.422-429, 2009.