基於身份的認證密鑰協商方案

楊伏夷　　蕭宇揚
朝陽科技大學資訊工程系　朝陽科技大學資訊工程系
副教授　　研究生
yangfy@cyut.edu.tw　s10027626@cyut.edu.tw

摘要

近年來，由於時代的進步與網際網路的快速發展，人跟人之間的溝通與資訊傳遞，越來越普及。基於安全性，學者們提出了身分驗證密鑰協商協議，並廣泛應用於網際網路的環境上。為了解決許多資訊安全的問題，在短短這幾年當中，眾多的學者提出了各種的方案，為的就是要帶給人們，便利又安全。但是，經過了這麼長的時間，許多技術協定還是沒辦法達到百分百的安全性，因為，在安全性與成本的考量上，沒辦法兩全其美。然而在 2012 年 Kyung-Ah Shim 所提出回顧 HöLBL-WELZER 的兩個方案並找出其中的弱點，但是卻沒有提出改進的方案。在本篇文章中，我們將分析他們的弱點與攻擊方法，並改進他們的方案。
關鍵詞：身分認證、交互認證、認證中心。

Abstract

Because of the rushing progress and development of internet, the communication between people becomes easier and faster ever. For the security purpose, Identity-Based Authenticated Key Agreement Protocols are discussed by scholars and used in many areas and phases, hoping that there will be ways to achieve a safe and friendly internet environment. However, none of the theory so far is perfect. The security key and its cost are interfered. Kyung-Ah Shim in 2012 reviewed the two theories of HöLBL-WELZER and found the weaknesses of them, however, failed to do any improvement. In this case, we are going to do the analysis of the weakness and looking for the solution.
Keywords: identity authentication, mutual authentication, authentication generator.

1. 前言

在現今這個社會裡，我們日常生活中最常使用到的網路、通訊，很多都是點與點的溝通，因為便利，所以大量的使用，但也都忽略其安全性，以為不會有問題，往往等到發現資訊被竊取被盜用才會驚覺。基於這點，許多的學者也都紛紛的提出了很棒的方案，但是，很多的方案還是無法抵擋許多更厲害的攻擊方案。

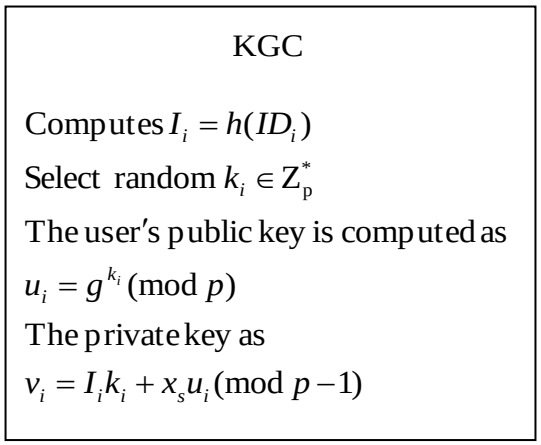
在 2009 年，Yang et al.[4]提出了一個三方認證密鑰交換協議的方案，A 與 B 的通訊透過一個伺服器去認證，但是卻沒有提供公私密金鑰。而在 2012 年，Hölbl et al.[3] 和 Islam and Biswas[5]提出會話密鑰的方案來進行通訊，會話密鑰是一個臨時訊息進行的加密方法。這兩個方案中的通訊兩方卻是經過複雜的運算而計算出來的，相對的計算量就大了。

在 2009 年，由 Hölbl and Welzer[2]提出了兩種基於身分認證密鑰協商協議，利用了密鑰認證中心的概念，提升兩方之間通訊的安全性，真的是很棒的一種概念。雖然已經有了安全性，但是在資訊安全學者眼裡還是不夠的，因此陸續被人提出了改進方案。在 2012 年，Shim[1]提出對 Hölbl and Welzer[2]方案的攻擊，指出此方案會遭受到中間人攻擊還有假冒攻擊，中間人攻擊就是攻擊者在兩方之間做假訊息的溝通，使得兩方之間無法察覺到資訊被竊取串改，而假冒攻擊就是攻擊者假冒了一方對另一方進行通訊，由於另一方無法去確認對方的合法性，所以就會被攻擊成功。然而 Shim[1]學者沒有提出改善的方案，所以在本篇文章中，我們將先回顧 Shim[1]的方案，並提出一個更有效率且能進行相互認證的方案以及抵擋攻擊安全性的分析。

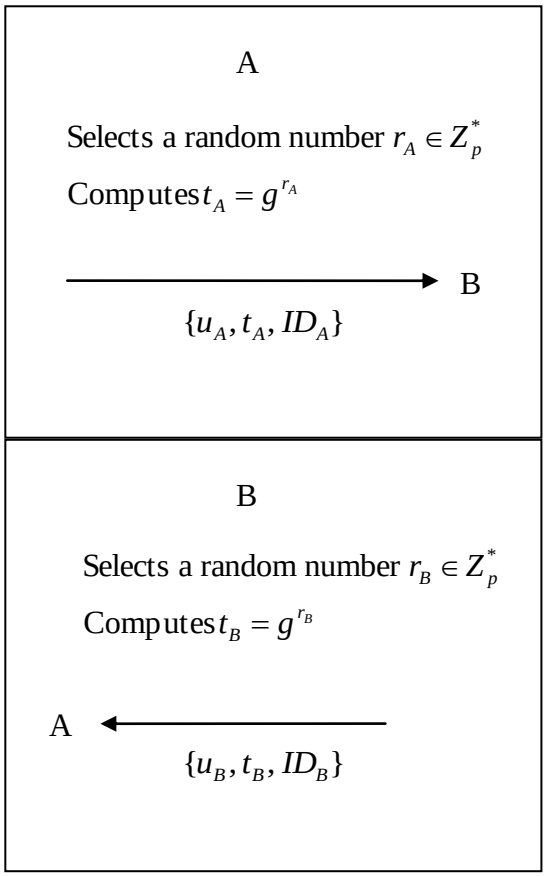
2. 回顧 Kyung-Ah Shim 的方案

Kyung-Ah Shim 的方案中分為三個階段: 回顧 HöLBL-WELZER 方案 1、回顧 HöLBL-WELZER 方案 2、安全性分析。

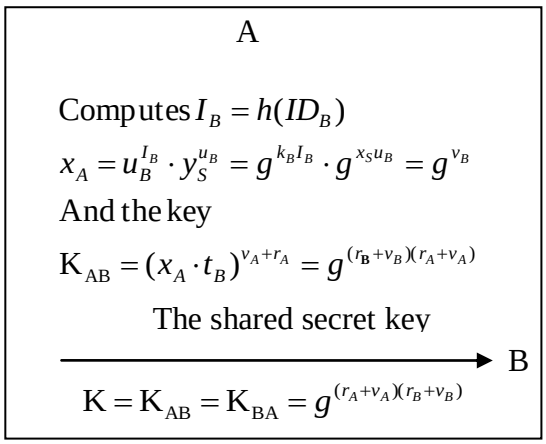
回顧 Hölbl-Welzer's 方案 1

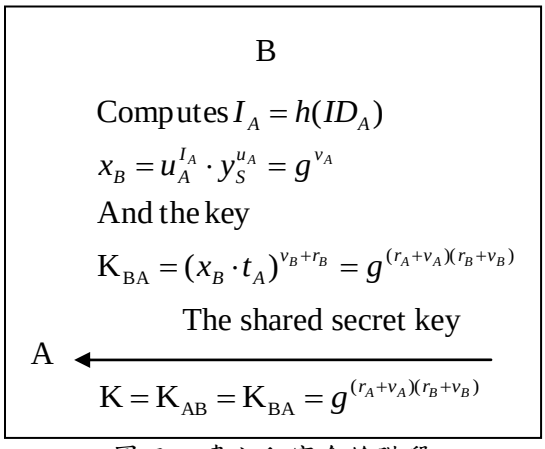


圖一、密鑰生成階段



圖二、密鑰協商協議階段





圖三、建立私密金鑰階段

該方案的參數:

ID_i	用戶i的身份
p	一個大質數
g	一個原根$g \in Z_p^*$
x_S	一個隨機數$x_S \in Z_p^*$
y_S	$y_S = g^{x_S} \pmod p$
$h(\cdot)$	安全的單向雜湊函數

2.1 密鑰生成階段:

由 KGC (金鑰生成中心)計算 $I_i = h(ID_i)$，並選擇一個隨機數 $k_i \in Z_p^*$，然後產生出使用者的公開金鑰 $u_i = g^{k_i} \pmod p$ 與私密金鑰 $v_i = I_i k_i + x_s u_i \pmod{p-1}$，流程如圖一所示。

2.2 密鑰協商協議階段:

用戶 A 選擇隨機數 $r_A \in Z_p^*$，計算 $t_A = g^{r_A}$，並透過安全通道傳送訊息 $\{u_A, t_A, ID_A\}$給用戶 B。

用戶 B 收到用戶 A 訊息 $\{u_A, t_A, ID_A\}$後，用戶 B 也選擇隨機數 $r_B \in Z_p^*$，計算 $t_B = g^{r_B}$，並透過安全通道傳送訊息 $\{u_B, t_B, ID_B\}$給用戶 A。流程如圖二所示。

2.3 建立私密金鑰階段:

用戶 A 在接收到 B 的訊息後，計算 $I_B = h(ID_B)$

$x_A = u_B^{I_B} \cdot y_S^{u_B} = g^{k_B I_B} \cdot g^{x_S u_B} = g^{v_B}$

產生金鑰 $\mathrm{K_{AB}} = (x_A \cdot t_B)^{v_A + r_A} = g^{(r_B + v_B)(r_A + v_A)}$

用戶 B 在接收到 A 的訊息後，計算

$I_A = h(ID_A)$

$x_B = u_A^{I_A} \cdot y_S^{u_A} = g^{v_A}$

產生金鑰 $\mathrm{K_{BA}} = (x_B \cdot t_A)^{v_B + r_B} = g^{(r_A + v_A)(r_B + v_B)}$

成功運行後，共同的私鑰就產生

$\mathrm{K} = \mathrm{K_{AB}} = \mathrm{K_{BA}} = g^{(r_A + v_A)(r_B + v_B)}$

流程如圖三所示。

回顧 Hölbl-Welzer's 方案 2

KGC

Computes $I_i = h(ID_i)$

Select random $k_i \in \mathrm{Z_p^*}$

The user's public key is computed as

$u_i = g^{k_i}$

The private key as

$v_i = k_i + x_s h(ID_i, u_i) \pmod{p-1}$

圖四、密鑰生成階段

A

Select a random number $r_A \in Z_p^*$

Computes $t_A = g^{r_A}$

$\longrightarrow$ B

$\{u_A, t_A, ID_A\}$

B

Select a random number $r_B \in Z_p^*$

Computes $t_B = g^{r_B}$

A $\longleftarrow$

$\{u_B, t_B, ID_B\}$

圖五、密鑰協商協議階段

A

Computes $I_B = h(ID_B)$

$w_A = r_A + v_A$

$x_A = u_B \cdot y_S^{h(ID_B, u_B)} = g^{k_B} \cdot g^{x_S h(ID_B, u_B)} = g^{v_B}$

And the key

$\mathrm{K_{AB}} = (x_A \cdot t_B)^{w_A} = (g^{v_B} \cdot g^{r_B})^{w_A} = g^{w_A w_B}$

The shared secret key

$\longrightarrow$ B

$\mathrm{K} = \mathrm{K_{AB}} = \mathrm{K_{BA}} = g^{w_A w_B} = g^{(r_A + v_A)(r_B + v_B)}$

B

Computes $I_A = h(ID_A)$

$w_B = r_B + v_B$

$x_B = u_A \cdot y_S^{h(ID_A, u_A)} = g^{k_A} \cdot g^{x_S h(ID_A, u_A)} = g^{v_A}$

And the key

$\mathrm{K_{BA}} = (x_B \cdot t_A)^{w_B} = (g^{v_A} \cdot g^{r_A})^{w_B} = g^{w_A w_B}$

The shared secret key

A $\longleftarrow$

$\mathrm{K} = \mathrm{K_{AB}} = \mathrm{K_{BA}} = g^{w_A w_B} = g^{(r_A + v_A)(r_B + v_B)}$

圖六、建立私密金鑰階段

該方案的參數:

ID_i	用戶i的身份
p	一個大質數
g	一個原根$g \in Z_p^*$
x_S	一個隨機數$x_S \in Z_p^*$
y_S	$y_S = g^{x_S}$
$h(\cdot)$	安全的單向雜湊函數

2.4 密鑰生成階段:

由 KGC (金鑰生成中心)計算 $I_i = h(ID_i)$，並選擇一個隨機數 $k_i \in \mathrm{Z_p^*}$，然後產生出使用者的公開金鑰 $u_i = g^{k_i}$ 與私密金鑰 $v_i = k_i + x_s h(ID_i, u_i) \pmod{p-1}$，流程如圖四所示。

2.5 密鑰協商協議階段:

用戶 A 選擇隨機數 $r_A \in Z_p^*$，計算

$t_A = g^{r_A}$，並透過安全通道傳送訊息$\{u_A, t_A, ID_A\}$給用戶 B。

用戶 B 收到用戶 A 訊息$\{u_A, t_A, ID_A\}$後，用戶 B 也選擇隨機數$r_B \in Z_p^*$，計算$t_B = g^{r_B}$，並透過安全通道傳送訊息$\{u_B, t_B, ID_B\}$給用戶 A。流程如圖五所示。

2.6 建立私密金鑰階段:

用戶 A 在接收到 B 的訊息後，計算

$I_B = h(ID_B)$

$w_A = r_A + v_A$

$x_A = u_B \cdot y_S^{h(ID_B, u_B)} = g^{k_B} \cdot g^{x_S h(ID_B, u_B)} = g^{v_B}$

產生金鑰

$\mathrm{K_{AB}} = (x_A \cdot t_B)^{w_A} = (g^{v_B} \cdot g^{r_B})^{w_A} = g^{w_A w_B}$

用戶 B 在接收到 A 的訊息後，計算

$I_A = h(ID_A)$

$w_B = r_B + v_B$

$x_B = u_A \cdot y_S^{h(ID_A, u_A)} = g^{k_A} \cdot g^{x_S h(ID_A, u_A)} = g^{v_A}$

產生金鑰

$\mathrm{K_{BA}} = (x_B \cdot t_A)^{w_B} = (g^{v_A} \cdot g^{r_A})^{w_B} = g^{w_A w_B}$

成功運行後，共同的私鑰就產生

$\mathrm{K} = \mathrm{K_{AB}} = \mathrm{K_{BA}} = g^{w_A w_B} = g^{(r_A + v_A)(r_B + v_B)}$

流程如圖六所示。

3. 安全性分析

3.1 方案一遭受到的中間人攻擊

首先攻擊者 E 竊取 A 和 B 之間的通信訊息，當 A 傳送$\{u_A, t_A, ID_A\}$給 B 的時候，攻擊者 E 攔截此訊息並傳送$\{u_A, t'_A, ID_A\}$給 B，當中的$t'_A = g^{\alpha - \upsilon A}$，而$\alpha$是攻擊者 E 隨機選擇的一個數。同樣的 B 在傳訊息給 A，攻擊者攔截訊息$\{u_B, t_B, ID_B\}$並傳送$\{u_B, t'_B, ID_B\}$給 A，當中的$t'_B = g^{\beta - \upsilon B}$，而$\beta$是攻擊者 E 隨機選擇的一個數。由於攻擊者傳送假冒的資訊給 A 和 B，所以 A 和 B 計算出來的私鑰數值分別為$\mathrm{K_{AB}} = (g^{\beta})^{v_A + r_A}$和$\mathrm{K_{BA}} = (g^{\alpha})^{v_B + r_B}$，因此攻擊者 E 也可以計算出這兩把私鑰$\mathrm{K_{AB}}$和$\mathrm{K_{BA}}$，造成 A 和 B 之間的資訊安全漏洞。

3.2 方案一遭受到的假冒攻擊

假設攻擊者 E 想要假冒 A，並與 B 進行通信。因此首先攻擊者 E 選擇一個隨機數$t \in Z_p^*$，$t = r_A + v_A$，接著攻擊者 E 假冒 A 傳送訊息$\{u_A, t_A = g^{r_A}, ID_A\}$給 B，接著 B 計算$\mathrm{K_{BA}} = (x_B \cdot t_A)^{v_B + r_B} = (g^{v_A} \cdot g^{r_A})^{v_B + r_B} = g^{(r_A + v_A)(r_B + v_B)}$接著攻擊者 E 能透過 B 傳送過來的訊息$\{u_B, t_B, ID_B\}$來計算出$\mathrm{K_{AB}} = (x_A \cdot t_B)^t = (g^{v_B} \cdot g^{r_B})^t = g^{(r_A + v_A)(r_B + v_B)}$，最後攻擊者 E 成功假冒 A 與 B 通訊。

3.3 方案二遭受到的假冒攻擊

假設攻擊者 E 想要假冒 A，並與 B 進行通信。因此首先攻擊者 E 選擇一個隨機數$T \in Z_p^*$，接著計算$t_A = g^{T - v_A}$並假冒 A 傳送訊息$\{u_A, t_A = g^{T - v_A}, ID_A\}$給 B，此時 B 計算$\mathrm{K_{BA}} = (x_B \cdot t_A)^{v_B + r_B} = (g^{v_A} \cdot g^{T - v_A})^{v_B + r_B} = g^{T(r_B + v_B)}$接著攻擊者 E 能透過 B 傳送過來的訊息$\{u_B, t_B, ID_B\}$來計算出$K_{AB} = (x_A \cdot t_B)^T = (g^{v_B} \cdot g^{r_B})^T = g^{T(r_B + v_B)} = K_{BA}$最後攻擊者 E 成功假冒 A 與 B 通訊。

經由 Kyung-Ah Shim 學者的解說，第一篇方案無法抵擋中間人攻擊，而兩篇方案都無法抵擋假冒攻擊。

兩篇方案都在“密鑰協商協議階段”遭受到另一方的假冒，得以攻擊，而第一篇方案也是在“密鑰協商協議階段”被攻擊者從中擷取並串改訊息，以至於被攻擊成功。

4. 改進方案

在本章節中，我們將對 Kyung-Ah Shim 所提出攻擊方案，進行增強的改進，已達到對其攻擊，成功的抵擋，並說明其安全性。我們的增強方案如下所述：

KGC

Computes $I_i = h(ID_i)$

Select random $k_i \in \mathrm{Z_p^*}$

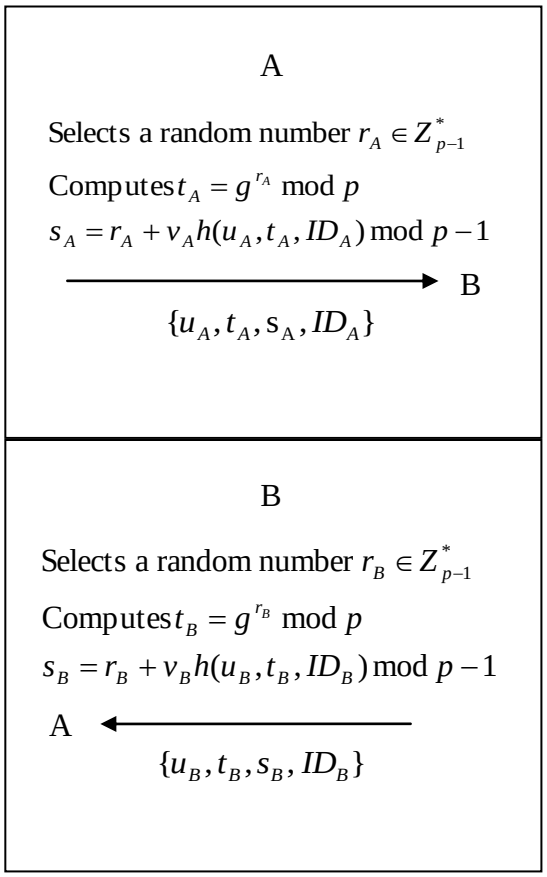
The user's public key is computed as

$u_i = g^{k_i}$

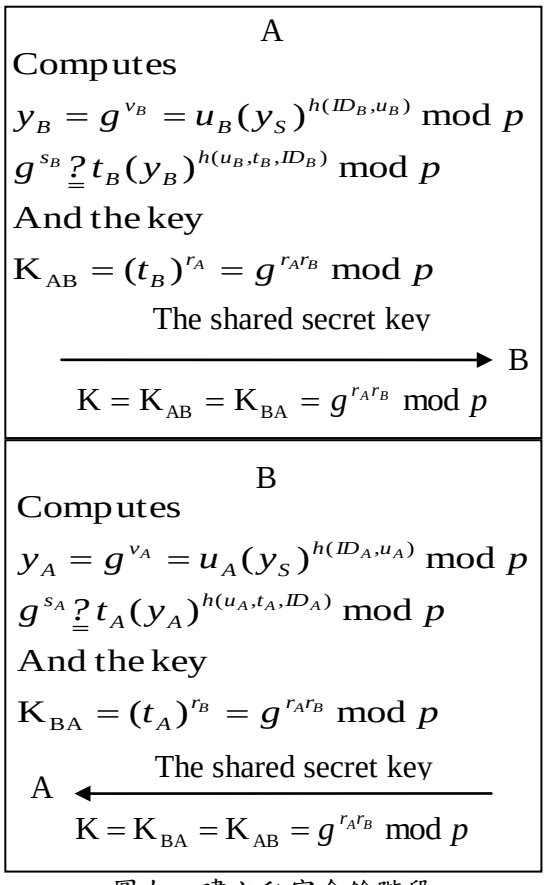
The private key as

$v_i = k_i + x_s h(ID_i, u_i) (\mathrm{mod}\ p-1)$

圖七、密鑰生成階段



圖八、密鑰協商協議階段



圖九、建立私密金鑰階段

該方案的參數:

ID_i	用戶i的身份
p	一個大質數
g	一個原根$g \in Z^*_p$
x_S	一個隨機數$x_S \in Z^*_p$
y_S	$y_S = g^{x_S}$
$h(\cdot)$	安全的單向雜湊函數

4.1 密鑰生成階段:

由 KGC (金鑰生成中心)計算 $I_i = h(ID_i)$，並選擇一個隨機數 $k_i \in Z^*_p$，然後產生出使用者的公開金鑰 $u_i = g^{k_i}$ 與私密金鑰 $v_i = k_i + x_s h(ID_i, u_i) (\bmod p-1)$，流程如圖七所示。

4.2 密鑰協商協議階段:

用戶 A 選擇隨機數 $r_A \in Z^*_{p-1}$，計算 $t_A = g^{r_A} \bmod p$
$s_A = r_A + v_A h(u_A, t_A, ID_A) \bmod p - 1$，並傳送訊息 $\{u_A, t_A, s_A, ID_A\}$ 給用戶 B。

用戶 B 收到用戶 A 訊息 $\{u_B, t_B, s_B, ID_B\}$ 後，用戶 B 也選擇隨機數 $r_B \in Z^*_{p-1}$，計算 $t_B = g^{r_B} \bmod p$
$s_B = r_B + v_B h(u_B, t_B, ID_B) \bmod p - 1$，並傳送訊息 $\{u_B, t_B, s_B, ID_B\}$ 給用戶 A。流程如圖八所示。

4.3 建立私密金鑰階段:

用戶 A 接收到 B 的訊息 $\{u_B, t_B, s_B, ID_B\}$ 後，計算 $y_B = g^{v_B} = u_B (y_S)^{h(ID_B, u_B)} \bmod p$ 並驗證 $g^{s_B} \stackrel{?}{=} t_B (y_B)^{h(u_B, t_B, ID_B)} \bmod p$，然後產生金鑰 $K_{AB} = (t_B)^{r_A} = g^{r_A r_B} \bmod p$。

用戶 B 接收到 A 的訊息 $\{u_A, t_A, s_A, ID_A\}$ 後，計算 $y_A = g^{v_A} = u_A (y_S)^{h(ID_A, u_A)} \bmod p$ 並驗證 $g^{s_A} \stackrel{?}{=} t_A (y_A)^{h(u_A, t_A, ID_A)} \bmod p$，然後產生金鑰 $K_{BA} = (t_A)^{r_B} = g^{r_A r_B} \bmod p$。
成功運行後，共同的私鑰就產生
$K = K_{AB} = K_{BA} = g^{r_A r_B} \bmod p$，流程如圖九所示。

5. 安全性分析

在本篇文中，我們的文章的改進，雖然比起 HöLBL-WELZER 學者方案一增加了 1 個指數運算的計算量，以及方案二增加了 2 個指數運算的計算量，但是卻可以增加其安全性。因為在方案一與方案二在傳送訊息$\{u_A, t_A, ID_A\}$並未經過 A 的簽署，傳送$\{u_B, t_B, ID_B\}$也未經過 B 的簽署，安全的弱點因而顯現。因此我們的方案加入了一個簽署的元素進去，大大的增加其安全性去驗證用戶 A 和用戶 B 的真實性。

6. 結論

在本篇文章中，我們回顧 Kyung-Ah Shim 所提出的方案，在方案中，提出了對 HöLBL-WELZER 學者的兩篇文章的弱點，並加以攻擊，但是卻沒有提出改進的方案，因此，我們增強了 Kyung-Ah Shim 的方案，並且也成功增強了方案中的安全性。

致謝

審稿委員們寶貴的評論與建議以及國科會專案研究計畫補助部分經費，謹此致謝，計畫編號：NSC 101-2221-E-324-047。

參考文獻

[1] Kyung-Ah Shim, “Cryptanalysis of Two Identity-Based Authenticated Key Agreement Protocols,” ***IEEE Communications Letters,*** Vol.16, Issue4, pp.554-556, 2012.

[2] HöSlbl and Welzer, “Two improved two-party identity-based authenticated key agreement protocols,” ***Computer Standards & Interfaces,*** Svol. 31, no. 6, pp. 1056–1060, 2009.

[3] Marko Hölbl, Tatjana Welzer, Boštjan Brumen, “An improved two-party identity-based authenticated key agreement protocol using pairings,” ***Journal of Computer and System Sciences,*** Vol. 78, Issue 1,pp. 142-150, 2012.

[4] Jen-Ho Yang and Chin-Chen Chang, “An efficient three-party authenticated key exchange protocol using elliptic curve cryptography for mobile-commerce environments,” ***Journal of Systems and Software,*** Vol. 82, Issue 9, pp. 1497-1502, 2009.

[5] SK Hafizul Islam and G.P. Biswas, “An improved pairing-free identity-based authenticated key agreement protocol based on ECC,” ***Procedia Engineering,*** Vol.30, pp.499-507, 2012.