一個有效率的交談金鑰協定

Fuw-Yi Yang　　Ming-Huei Hsu　　Tzung-Da Wu
Department of Computer Science and Information Engineering,
Chaoyang University of Technology

yangfy@cyut.edu.tw　　s9627621@cyut.edu.tw　　s9727621@cyut.edu.tw

摘要

在 2003 年，Ryu 等學者提出一個簡單交談金鑰協定，此協定可使得使用者能夠輕易的與遠端伺服器完成所需之通訊服務，其最大特色在於僅需一組密碼即可完成雙方的交互認證，在此協定中雖可達到許多安全之特性，但對於抵擋阻斷服務攻擊(Denial of Service, DoS)而言是無法預防的。因此在本篇論文中，我們將針對 Ryu 等學者的協定提出分析及有效的改善方法，讓我們的協定保有原本協定的優點，並同時解決無法抵擋阻斷服務攻擊之問題，加上在效率方面，我們的協定僅需兩次通訊次數，就能夠提供使用者在現今不安全的網路中一個安全的溝通管道。

關鍵詞：交談金鑰、阻斷服務攻擊、交互認證。

Abstract

In 2003, Ryu et al. proposed a simple key agreement protocol, which could enable the users can easily attain the communication services with remote servers. Its main characteristics rested on just requiring one set of secret password to finish off the mutual authentications for both parties online. Although within this protocol, it had the characteristic of being able to reach the desired levels of security it was still unable to prevent nor immune from attacks like Denial of Service, DoS. Thus, within this thesis, the analyses and effective methods proposed in regards to the protocols from Ryu et al., which leads to retain the original protocol's advantages as well. In addition, it simultaneously resolves the problems of unable to prevent and protect from DoS attacks. Furthermore, in the aspect of efficiency, our protocol only requires only two communication rounds which would provide the users with a safe communication channel within today's unsafe internet accessing.

Keywords: Session key, Denial of Service, Mutual authentication.

1. 前言

近年來，隨著資訊科技的發展與網際網路的發展，帶動了整個網路的快速成長與普及化，使得人們可輕易的透過網路向遠端伺服器取得服務，以進行較私密的通訊活動。但在傳輸過程中如何能夠確保通訊資料在不安全的網路中，免於遭受外部威脅，將通訊資料安全的傳送到對方，對於現今而言是非常重要的議題。

在 1976 年，Diffie 和 Hellman[1]提出了金鑰交換系統，此系統目的在於當在網路上的雙方需要通訊時，彼此不需要見面，就可透過計算模數與指數的運算，使得雙方可獲得相同的秘密金鑰，對所想要傳送之訊息加密，但此協定容易遭受到中間人攻擊，倘若傳送者與接受者之間存在一個攻擊者，若是攻擊者想要假扮傳送者傳送其公開金鑰給接收者，則接收者會因缺乏身分確認，而無法辨別出此訊息是否由傳送者所發送，導致容易遭受中間人攻擊。因此近幾年來，許多學者對此問題紛紛提出解決

方法，其中以密碼做為雙方的身分確認方法最為廣泛採用；在 2003 年，Ryu[2]等學者提出一個簡單金鑰交談協定，在此協定中使用者僅需與遠端伺服器註冊一組密碼，做為雙方通訊時身分確認之用途，即可完成雙方通訊所需之秘密交談金鑰，並達到前推私密性與防止驗證表遺失以及防止交談金鑰洩漏之攻擊。

然而在 Ryu 等學者所提出的協定中，雖然可抵擋許多攻擊與安全特性，但我們卻發現到此協定對於阻斷服務攻擊(Denial of Service, DoS)方面，無法做出有效的抵擋與預防，設有攻擊者持續的對遠端伺服器發送錯誤封包，迫使遠端伺服器無法正常運作，這對於雙方通訊而言可能會造成重大的損失。

因此在本論文中，我們針對此協定的缺失提出一個有效的改善方法，並在通訊次數方面能夠減少至兩次，不僅降低了錯誤發生的機會，更提升了整體的通訊效率。

在本論文中，將在第二章節回顧 Ryu 等學者所提出的協定，第三章節針對 Ryu 等學者的協定提出攻擊方法，第四章節說明我們所提出改善的方法，並在第五章節做安全性分析與效率分析的講解，最後一章節則是我們的結論。

1.1 符號定義

以下是本篇論文中會用到的參數及符號的定義。

- n: n 為一個大質數。
- g: g 是由 Z_n^* 中所選取的原根。
- A:使用者 A。
- S:伺服器 S。
- π :使用者的密碼。
- s:伺服器的秘密金鑰。
- r_A, r_B :由 Z_{n-1}^* 中所選取的短暫秘密金鑰。
- $h(\cdot)$:無碰撞單向雜湊函數。
- ||:字串連結運算符號。
- K:使用者與伺服器通訊之秘密交談金鑰。

2. 回顧 Ryu et al.的協定

Ryu 等學者在 2003 年提出一個簡單的交談金鑰協定，此協定最大優點在於僅需使用密碼做為身分確認，即可與伺服器完成交互認證並協商出交談金鑰，使得使用者與伺服器能夠在不安全的網路中進行私密性的通訊活動；而在 Ryu 等學者的協定以兩個階段來表示，分別為註冊階段與通訊階段，底下將會詳細的敘述整個交談金鑰協商過程，如圖一為 Ryu et al. 的交談金鑰協商之流程。

根據此協定可將區分為兩個主要的角色: 使用者 A 與伺服器 S。

2.1 註冊階段:

首先使用者 A 自行選取一組密碼傳送至伺服器 S 進行註冊動作，伺服器 S 收到密碼後，先將密碼經由無碰撞單向雜湊函數運算處理，再利用其秘密金鑰 s 加密計算 $\upsilon = h(\pi)^s \bmod n$，並將 υ 儲存在驗證表中，最後伺服器 S 則將所收到密碼由系統中移除，然而此註冊階段傳送過程皆在安全通道之下通訊。

2.2 通訊階段:

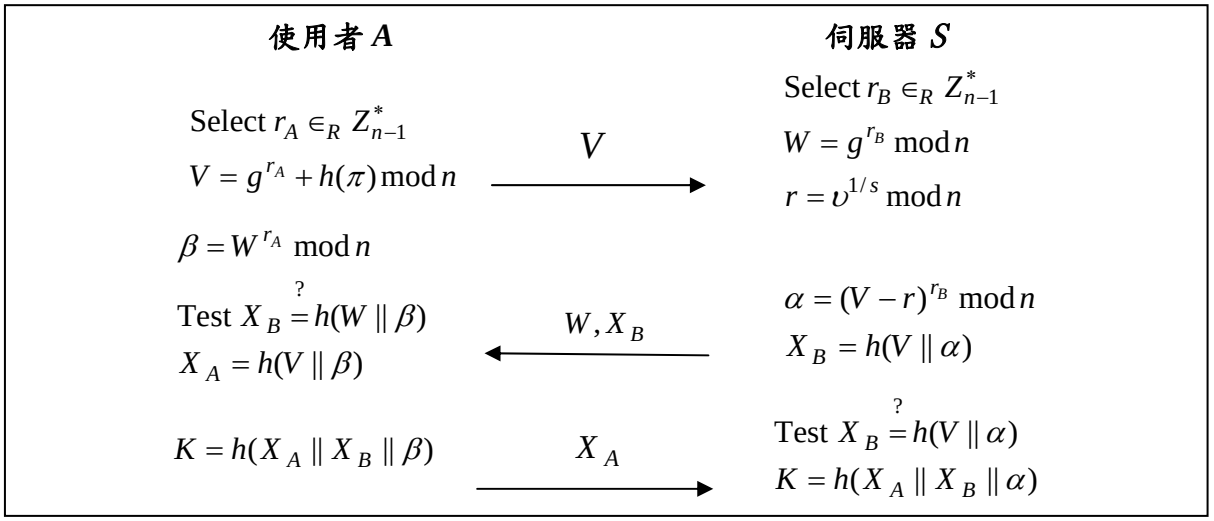
當使用者 A 向伺服器 S 註冊完成之後，若使用者 A 欲取得伺服器 S 通訊服務，則必須與伺服器 S 達成交互認證，並協商出交談金鑰 $K = h(X_A \| X_B \| g^{r_A r_B} \bmod n)$，再利用此交談金鑰對訊息加密，其通訊階段之流程，以下詳細敘述之。

步驟 1:

使用者 A 由 Z_{n-1}^* 中隨機選取一個亂數 r_A，計算 $V = g^{r_A} + h(\pi) \bmod n$，接著將所計算訊息 V 傳送給伺服器 S。

步驟 2:

當伺服器 S 收到訊息 V 後，由 Z_{n-1}^* 中隨機選取一個亂數 r_B，計算 $W = g^{r_B} \bmod n$、$r = \upsilon^{1/s} \bmod n$ 以及 $\alpha = (V - r)^{r_B} \bmod n$ 和 $X_B = h(W \| \alpha)$，接著傳送訊息 (W, X_B) 給伺服器 S。



圖一. Ryu et al. 的交談金鑰協商之流程

步驟 3:

使用者 A 接收到訊息 (W, X_B) 後，利用所選取亂數 r_A，計算 $\beta = W^{r_A} \bmod n$、$X_A = h(V \| \beta)$，並驗證 $X_B \stackrel{?}{=} h(W \| \beta)$ 是否相等，若相等則視為合法訊息，並將訊息 X_A 傳送給伺服器 S。

步驟 4:

伺服器 S 接收到訊息 X_A 後，驗證 $X_A \stackrel{?}{=} h(V \| \alpha)$ 是否相等，若相等則視為使用者 A 為合法使用者，並達到交互認證之效果。

步驟 5:

最後，當使用者 A 與伺服器 S 完成以上步驟，雙方即可計算出共同擁有交談金鑰 $K = h(X_A \| X_B \| \alpha) = h(X_A \| X_B \| \beta) = h(X_A \| X_B \| g^{r_A r_B} \bmod n)$。

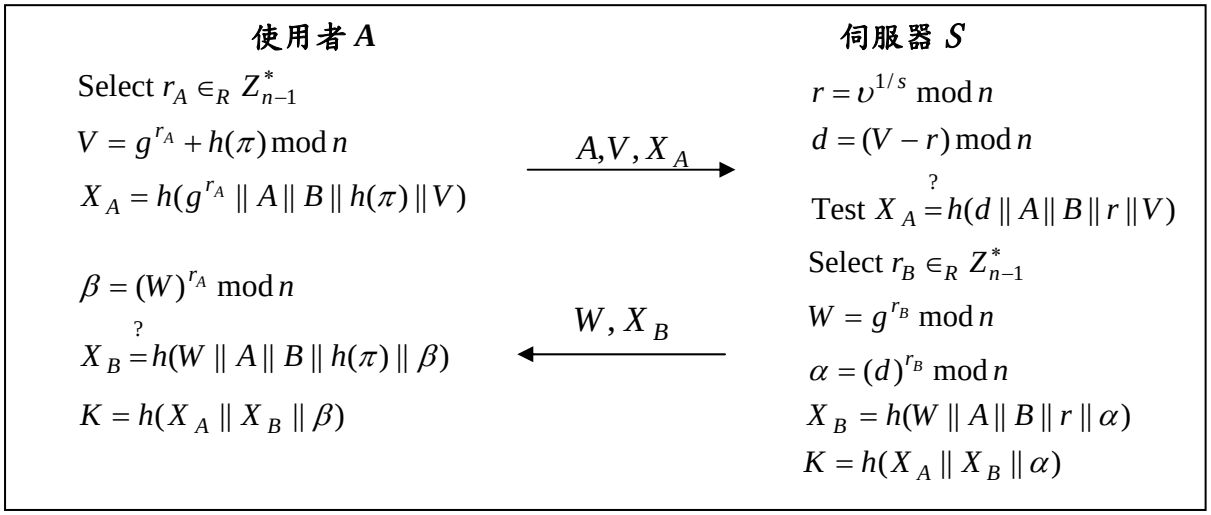
在 Ryu 等學者的協定中，使用者 A 僅需一組密碼就可達到身分確認之效果，並且將協定中的安全性建立在於解 Diffie-Hellman 難題上，以防止第三人擁有交談金鑰 $K = h(X_A \| X_B \| g^{r_A r_B} \bmod n)$，對於伺服器 S 而言，如果驗證表遺失，亦不具影響整體協定中的安全性。

3. 討論

Ryu 等學者所提出的協定，雖然可以抵擋許多攻擊並達到前推私密性與防止驗證表洩漏之特性，但我們可以在協定中發現一個重大的缺失，當使用者 A 註冊完之後，欲取得伺服器 S 通訊服務時，伺服器 S 無法在第一次通訊後馬上驗證使用者 A 是否為合法使用者，直到最後一次通訊時才驗證使用者 A 的密碼是否正確 $X_A \stackrel{?}{=} h(V \| \alpha)$，因此倘若有攻擊者不斷以錯誤的封包在第一次通訊時傳送給伺服器 S，此時伺服器 S 會因遭受到阻絕服務攻擊 (Denial of Service, DoS)，導致伺服器 S 無法正常運作，所以在 Ryu 等學者的協定中，對於阻絕服務攻擊(Denial of Service, DoS)，是無法有效預防的。

4. 我們的協定

經由以上討論可以發現 Ryu 等學者所提出的協定，在第一次通訊時無法立刻判斷出使用者 A 的密碼是否正確，導致容易遭受到阻絕服務攻擊，因此我們提出一個有效率的簡單金鑰交談協定，在此協定中我們將通訊次數減少至兩次，並能夠在第一次通訊時就可驗證使用者 A 的密碼是否正確，有效解決 Ryu 等學者協定中的問題，並將整體安全性一樣建立在於解 Diffie-Hellman 難題上，來防止第三人擁有交談金鑰與前推私密性以及防止驗證表洩漏之特性。



圖二. 我們的交談金鑰協商之流程

我們的協定分為兩個階段，分別為註冊階段與通訊階段；以下將會詳細的敘述整個交談金鑰協商過程，如圖二為交談金鑰協商之流程。

根據此協定可將區分為兩個主要的角色：使用者 A 與伺服器 S。

4.1 註冊階段:

首先使用者 A 自行選取一組密碼傳送給伺服器 S 進行註冊動作，伺服器 S 收到密碼後，先將密碼經由無碰撞單向雜湊函數運算處理，再利用其秘密金鑰 s 加密計算 $\upsilon = h(\pi)^s \bmod n$，並將 υ 儲存在驗證表中，最後伺服器 S 則將所收到密碼由系統中刪除，此註冊階段傳送過程皆在安全通道之下通訊。

4.2 通訊階段:

當使用者 A 向伺服器 S 註冊完成之後，若使用者 A 欲取得伺服器 S 通訊服務，則必須與伺服器 S 達成交互認證，並協商出交談金鑰 $K = h(X_A \| X_B \| g^{r_A r_B} \bmod n)$，其通訊階段之流程，以下詳細敘述之。

步驟 1:

使用者 A 由 Z_{n-1}^* 中隨機選取一個亂數 r_A，計算 $V = g^{r_A} + h(\pi) \bmod n$ 以及 $X_A = h(g^{r_A} \bmod n \| A \| B \| h(\pi) \| V)$，接著將訊息 (A, V, X_A) 傳送給伺服器。

步驟 2:

當伺服器 S 收到訊息 (A, V, X_A) 後，利用其秘密金鑰 s 計算 $r = \upsilon^{1/s} \bmod n$ 與 $d = (V - r) \bmod n$，並驗證 $X_A \stackrel{?}{=} h(d \| A \| B \| r \| V)$ 是否相等，若相等則代表使用者 A 為合法使用者；接著伺服器 S 由 Z_{n-1}^* 中隨機選取一個亂數 r_B，計算 $W = g^{r_B} \bmod n$ 與 $\alpha = (d)^{r_B} \bmod n$ 以及 $X_B = h(W \| A \| B \| r \| \alpha)$，最後將訊息 (W, X_B) 傳送給使用者 A。

步驟 3:

使用者 A 接受到訊息 (W, X_B) 後，計算 $\beta = (W)^{r_A} \bmod n$ 並驗證訊息 $X_B \stackrel{?}{=} h(W \| A \| B \| h(\pi) \| \beta)$ 是否相等，若相等即代表與伺服器 S 雙方驗證成功。

步驟 4:

當使用者 A 與伺服器 S 完成以上步驟雙方即可計算出共同擁有之交談金鑰 $K = h(X_A \| X_B \| \alpha) = h(X_{A|} \| X_B \| \beta) = h(X_{A|} \| X_B \| g^{r_A r_B} \bmod n)$，最後雙方即可利用其交談金鑰對訊息加密，來完成通訊活動。

在我們的協定中，保有 Ryu 等學者協定中的優點，並且能夠明顯的改善協定中無法抵抗 *DOS* 攻擊的缺點，在通訊次數方面，我們的協定只需兩次通訊次數，即可達到雙方的交

互驗證與協商出交談金鑰，因此我們的協定可適用於在目前不安全的網路當中。

5. 協定分析

我們將在這個章節針對協定的安全性以及效率進行分析。

5.1 安全性分析:

在我們的協定中，我們將安全性建構於解 Diffie-Hellman 難題上，來抵擋外部攻擊，底下為我們的協定所具有的安全特性。

前推私密性:

倘若使用者 A 的密碼洩漏，則攻擊者只能假冒 A 並計算出這次通訊所需之交談金鑰 $K = h(X_A \| X_B \| g^{r_A r_B} \bmod n)$，但無法由這次所取得之交談金鑰解開之前通訊之訊息內容，因在協定中交談金鑰的取得是由雙方從 Z_{n-1}^* 中選取之兩個亂數 r_A, r_B 所計算而成，然而在每次通訊時所需之交談金鑰都是不同的，因此我們的協定可達到前推私密性。

交談金鑰洩漏攻擊:

設若有攻擊者想要從通訊過程攔截訊息，經由 X_A 或 X_B 中計算出交談金鑰 K 是不可行的，因若想計算出交談金鑰 $K = h(X_A \| X_B \| g^{r_A r_B} \bmod n)$，將會遇到解 Diffie-Hellman 難題，所以只有使用者 A 與伺服器 S 擁有交談金鑰，第三人是無法由通訊過程得知交談金鑰之內容，因此我們的協定可抵抗交談金鑰洩漏攻擊。

驗證表洩漏之攻擊:

假設若伺服器的驗證表遺失，則攻擊者無法由驗證表中得知有任何關於使用者的密碼，因儲存於驗證表的密碼，都經由無碰撞單向雜湊函數與伺服器 S 的秘密金鑰加密計算而成 $\upsilon = h(\pi)^s \bmod n$，因此攻擊者無法由洩漏的驗證表中得知使用者 A 的密碼，所以在我們的協定中可抵擋驗證表洩漏之攻擊。

阻絕服務攻擊(Denial of Service, DoS):

設想有攻擊者想要針伺服器 S 發動阻絕服務攻擊，則伺服器 S 可以在與使用者 A 第一次通訊時，就可由 $X_A \stackrel{?}{=} h(d \| A \| B \| r \| V)$ 判斷出使用者 A 是否為合法使用者，使得若有攻擊者想要進行阻絕服務攻擊時，對伺服器 S 而言是無法奏效的，因此我們的協定具有抵抗阻絕服務攻擊之特性。

5.2 效率分析:

在效率分析部分，我們針對通訊次數以及通訊花費與計算量來做比較。設 n 為 1024 位元的大質數，雜湊函數 $h(\cdot)$ 的輸出為 160 位元，個人身分資訊為 32 為位元，如圖三為效能分析表。

圖三. 效能分析表

	Ryu et al. 的協定	我們的協定
通訊花費（位元數）	2368	2400
計算量（指數運算）	5	5
通訊次數	3	2

由上表可得知，在我們的協定中只需兩次通訊次數就可完成交互認證與協商出所需之交談金鑰，並且能夠在第一回合的資訊辨別使用者身份，防止來自攻擊者的阻斷服務攻擊，有效的改善 Ryu 等學者協定中的缺點，因此我們的協定能夠提供給使用者一個既有效率又安全的環境。

6. 結論

在本篇論文中，我們可看出 Ryu 等學者的協定，因無法在第一次通訊時有效的判斷使用者的密碼是否正確，因此容易遭受到阻斷服務攻擊，而在我們所提出的協定能夠有效的解決問題，並保有原本協定中所具有的優點，並將

協定的安全性建立在解 Diffie-Hellman 難題上，在通訊次數方面，我們的協定只需兩次即可達到協定所需之目標。

7. 參考文獻

[1] W.Diffie and M.E.Hellman, “New directions in cryptography, ” ***IEEE Transactions on Information theory,*** Nov 1976, pp.644-654.

[2] Eun-Kyung Ryu, Kee-Won Kim, and Kee-Young Yoo, “A simple key agreement protocol**,** ”***International Carnahan Conference on Security Technology***, ”Oct 2003, pp.128-131.

[3] Dong-Hwi Seo and Sweeney.P, “Simple authenticated key agreement algorithm**,** ” ***IEE Electronics Letters***, June 1999, pp.1073-1074.

[4] Wet-Chi Ku and Sheng-De Wang, “Cryptanalysis of modified authenticated agreement protocol**,** ” ***Electronics Letters***, Oct 2000, pp.1770-1771.

[5] Yuh-Min Tseng, “Weakness in simple authenticated key agreement protocol, ” ***Electronics Letters***, Jan 2000, pp.48-49.