植基於關鍵字搜尋之匿名驗證

周新偉
國立中興大學
e-mail：
g103056116@mail.nchu.edu.tw

陳國璋
國立中興大學
e-mail：
s9756013@csmail.nchu.edu.tw

洪國寶
國立中興大學
e-mail：
gbhorng@nchu.edu.tw

摘要

在網路世界中隱私保護逐漸成為一個重要的議題，截至目前為止為達到隱私保護進而發展出很多不同的方式，本文透過關鍵字搜尋(Keyword search) 以及運用 Diffie-Hellman Key Exchange(DHKE)以達到匿名驗證，讓雲端伺服器在無法揭露使用者身分的情況下完成使用者身分的驗證。

關鍵詞：匿名驗證，關鍵字搜尋，迪菲-赫爾曼密鑰交換，隱私保護。

Abstract

Protecting private data becomes a major issue in modern society. There are many ways to achieve privacy preserving. In this paper we utilize keywords search and Diffie-Hellman key exchange to achieve anonymous authentication such that cloud server can authenticate users without knowing their identities.

Keywords: Anonymous Authentication, Keyword search, Diffie-Hellman Key Exchange, Privacy preserving.

1. 前言

一般而言，使用者向伺服器端申請服務時，伺服器必須驗證使用者的身分，判斷是否有權限啟用相對應的服務。然而在某些特定的狀況下，使用者的身分不能夠被揭露，例如電子投票、線上論壇等等，因為這些情況具有匿名的需求，所以伺服器端必須在不揭露使用者身分的條件下審核使用者的權限，此稱為匿名驗證。匿名驗證包含了三個實體：可信任的第三方(TTP)、伺服器端(AP)、使用者(User)，使用者一開始向 TTP 進行註冊，之後使用者對 AP 端進行匿名性的驗證，在通過驗證之後使用者就可以要求伺服器提供服務。

在 2004 年 Teranishi 等學者提出透過更改群簽(Group signature)，讓使用者可以跟伺服器進行有限次數的匿名驗證[1]。之後也相繼有很多學者提出達成匿名驗證的方法 [5,10,11,13]，到了 2010 年 Lindell 等學者提出對於匿名驗證的安全性要求以及公開金鑰加密和環簽(Ring signature)等兩種可以達到匿名驗證的作法[3]。

關鍵字搜尋最早是由 Song 等學者在 2000 時提出[9]，透過加密訊息可以讓使用者和不可信任的伺服器進行互動，Song 等學者假設伺服器端會正常的運作，並且只是對於訊息的內容感到好奇，想要進行窺探。

本文參考 Chen 等學者對於關鍵字搜尋的研究 [2] 加上 Diffie-Hellman Key Exchange(DHKE)，讓雲端伺服器在無法揭露使用者身分的情況下完成使用者身分的驗證已達到匿名驗證的要求。

在我們的所提出的構想中一共存在4個實體，可信任的第三方、發起人、使用者和伺服器。使用的情境為發起人手上有一份名單，名單內是他所認可的使用者所代表的身份資訊，可以為電子信箱帳號、電話號碼或是其他可以代表該使用者身份的資訊，再將這些資訊做處理之後上傳給伺服器。當名單內的使用者想要取得服務時，將自己的身份資訊傳給伺服器做驗證，在伺服器通過驗證之後就可以取得服務。

本文主要的貢獻在於首次將匿名驗證的觀念加入關鍵字搜尋，產出一種全新進行匿名驗證的方式，由於以往的研究都沒有做這方面的結合，我們相信這是一種新的突破，未來我們以往提升此方法的效率作為研究的主要方向。

2. 相關研究

在使用者向伺服器端要求服務或是資源時，伺服器必須要驗證使用者的資格是否合法。但是在某些條件下，必須要伺服器在不知道使用者真實身分的情況下驗證使用者的身份，此稱為匿名驗證。

匿名驗證大致上分成兩種方式：

Password-based 跟 Credential-based。

Password-based 多運用在計算能力較弱的設備上[4,7,12]，其要求大多是能夠快速的反應使用者的要求。做法常會使用到雜湊函數以及 XOR 以加速計算的速度。

Credential-based 則是用在網路環境為主的架構，以安全性為主要的訴求，常使用較複雜的密碼學技巧，如零知識證明或是群簽等等的做法[6,8,14]。

在 Lindell 等學者的論文中提到實作匿名驗證的方法，第一種是透過 RSA 的運用，在他假設的情境下一共有 n 個使用者，每一個使用者都擁有一個密鑰以及相對應的公鑰，在進行驗證時，伺服器端用每個使用者的公鑰加密一段訊息 m 成為 $E_{pk}(m)$，將加密後的訊息傳給每一個使用者，使用者用自己的私鑰將 m'解回來後回傳給伺服器，伺服器再檢驗 m'= m 是否成立，在此情況下，使用者可以在不透露自己身分的情況下跟伺服器端完成驗證。第二種方法使用者身上會有智慧卡(smart card)，透過智慧卡的輔助運算，透過類似於法一的方法，伺服器端在要傳的內容加上亂數，使用者解密回傳之後，伺服器只取不含亂數的訊息來比對，通過驗證之後使用者才可以取得伺服器的服務。

在 Chen 等學者的論文中，發起人將自己所產生的密文傳到伺服器端，產生密文的方式是透過發起人將使用者所會運用到的關鍵字加入到修改過後的 Lagrange 方程式以產生跟關鍵字相對應的密文，接著把密文及要給使用者的文件加密後傳給伺服器。使用者要跟伺服器要求服務時，將自己所掌握的關鍵字製作成後門(trapdoor)傳給伺服器，伺服器再比對使用者所傳的後門跟發起者所傳的密文是否吻合，一旦吻合及通過驗證，可以取得伺服器的服務。

3. 預備知識

在此章節我們將會對於運用到的相關技巧進行解釋，包括 Bilinear pairing、DHKE、Lagrange 方程式。

3.1 雙線性映射

雙線性映射又稱為 Bilinear pairing，是在橢圓曲線上的一種特性，存在著一個配對同構的值。以下我們介紹雙線性映射的定義以及特性：

令G_1, G_2為加法循環群，G_T為乘法群，有相同的 order p，p 為一個大質數，g_1, g_2分別為G_1，G_2的生成元，雙線線性映射的函式可以表示為：e:$G_1 \times G_2 \to G_T$，並具有以下三個特性：

(1) 雙線性：對任一個整數 $a, b \in Z_p$，$u, u_1, u_2 \in G_1$為G_1的生成元，$v \in G_2$為G_2的生成元，使得

$$e(au, bu) = e(u, u)^{ab}$$

$$e(u_1 + u_2, v) = \mathrm{e}(u_1, v) \cdot \mathrm{e}(u_2, v)$$

(2) 非退化性(Non-degenerate)：假設 u 和 v 為G_1，G_2的生成元，則 $e(u, v)$為G_T的生成元。

(3) 可計算性：給定 $u \in G_1$，$v \in G_2$，存在一個多項式時間的演算法可以找到G_T上的對應值 $e(u, v) \in G_T$

3.2 Diffie-Hellman Key Exchange(DHKE)

一種安全協定。它可以讓雙方在完全沒有對方任何預先資訊的條件下通過不安全信道建立起一個金鑰。這個金鑰可以在後續的通訊中作為對稱金鑰來加密通訊內容。

Alice 擁有公鑰K_A、私鑰α，Bob 擁有公鑰K_B、私鑰β。雙方透過互相交換公鑰再用自己所擁有的私鑰進行不同方式的加密可得到兩個完全相同的金鑰$(K_A)^{\beta}$、$(K_B)^{\alpha}$。

3.3 Lagrange 方程式

許多實際問題中都用函數來表示某種內在聯繫或規律，而不少函數都只能通過實驗和觀測來了解。如對實踐中的某個物理量進行觀測，在若干個不同的地方得到相應的觀測值，Lagrange 插值法可以找到一個多項式，其恰好在各個觀測的點取到觀測到的值。這樣的多項式稱為 Lagrange（插值）多項式。

在已給定的 $k+1$ 個取值點，可以得到 Lagrange 基本多項式：

$$l_j(x) = \prod_{i=0, i \neq j}^{k} \frac{(x - x_i)}{(x_j - x_i)}$$

4. 植基於關鍵字搜尋之匿名驗證

在此章節中，我們提出一種新的實現匿名驗證的方法。在介紹演算法前，我們先對設計的背景架構進行簡單的介紹，接著講解我們所提出的四個演算法(1)初始化(2)註冊(3)驗證(4)註銷。

4.1 植基於關鍵字搜尋之匿名驗證

在此章節中，我們將會對本文將要使用到的四個演算法進行介紹。本文中所使用的參數分別為雜湊函式 $H: W \to Z_q^*$ (W為關鍵字的

的集合)、雜湊函數 H': $\{0,1\}^* \rightarrow G_2$、雙線性映射函數$\hat{e}$：$G_1 \times G_2 \rightarrow G_3$，其中加法群$G_1$、$G_2$、乘法群$G_3$的 order 皆為 q 且 $G_1 \neq G_2$ 。P_1為G_1的生成元，P_2為G_2的生成元。系統參數為$\{P_1, P_2, G_1, G_2, G_2, H, H', \hat{e}, q\}$

(1) Initial：系統一開始由可信任的第三方進行初始化的動作，他將發起人以及使用者的公鑰及私鑰發給雙方。發給發起人的公鑰$U_S = \alpha_S P_1$，私鑰$\alpha_S(\alpha_S \in_R Z_P^*)$。發給使用者的公鑰$U_i = \alpha_i P_1$(for *i*=1,…,*l*), X_1=αP_1, X_2=βP_1, X_3，私鑰:α_i, α, β (α_i, α, β都是Z_P^*上的亂數)。

(2) Registration：在此階段是由發起人替使用者進行註冊，透過取得使用者的公鑰及本身擁有的使用者的身份資訊 D=$\{ID_1, \dots, ID_l\}$再加上隨機變數 r ($r \in_R Z_q^*$)，以計算出上傳到伺服器的名單。

1.計算$k_i = H(\alpha_S U_i \| ID_i)$for *i*=1,…,*l*，再取一個$k_{l+1} = H(\widetilde{W})$其中 $\widetilde{W} \notin W$。

2.根據$k_1, \dots, k_{l+1}$可以求得一個方程式 $f(x)$。

$f(x)$=$\sum_{i=1}^{l+1}(\prod_{1 \le j \ne i \le l+1} \frac{(x-k_j)}{(k_i-k_j)}) \, mod \, q$

$=a_0 + a_1 x + \cdots + a_l x^l \, mod \, q$。

3.最後取得$B_1 = rX_1$,

$B_2 = r(\sum_{i=0}^{i} a_i)X_1$,

$C_i = ra_i P_1$ for *i*=1,…,*l*。

名單為 $C_D = \{B_1, B_2, C_1, \dots, C_l\}$

(3) Authentication：在此階段，參與的使用者(U_l)想從伺服器端通過驗證以獲得服務就用自己的密鑰α_i, α, β以及掌握的關鍵字 ID，計算後傳給伺服器做驗證。

User：

s_0= $H(\alpha_1 U_S \| ID_1)^0 mod \, q$

s_1=$H(\alpha_1 U_S \| ID_1)^1 mod \, q$

$\vdots$

s_l=$H(\alpha_1 U_S \| ID_1)^l mod \, q$

接著組成邀請証明T_Q，取 $R \in_R G_2$

V= $\alpha^{-1} R$,

$T_i = s_i R + \beta X_3$

$T_Q = \{R, V; T_0, \dots, T_l\}$

把T_Q傳給伺服器進行驗證

Server：

執行伺服器驗證

$$\prod_{i=0}^{l} \hat{e}(C_i, T_i) = ? \, \hat{e}(B_1, V)\hat{e}(B_2, X_3)$$

等號成立伺服器輸出 1，否則輸出 0。

(4) Revoke：當伺服器端發現通過驗證的使用者在系統內進行惡意的動作，由於使用者是透過匿名的方式通過驗證，所以伺服器端無法透過使用者傳來的資訊揪出惡意的使用者，此時伺服器端又希望能夠註銷這名使用者的資格。在此階段，由可信任的第三方跟伺服器合作，透過可信任的三方的幫助找出使用者。

Server:

將$T_Q = \{R, V; T_0, \dots, T_l\}$傳給可信任的第三方。

TTP:

$$T_i = s_i R + \beta X_3$$

可信任的第三方在擁有β、X_3、R的條件下，透過將所有使用者的 ID 以及相對應的 DHKE 密鑰投入 H 中就可以得到s_i for *i*=1,…,*l*，可信任的第三方再把所有得參數組合起來得到$s_i R + \beta X_3$，透過比對伺服器傳來的資訊就可以抓出誰是惡意的使用者，註銷他的使用權利。

5. 分析

在此章節我們檢驗驗證式的正確性，以及分析所提出的方法時否能夠符合匿名驗證的安全性要求：匿名性(Anonymous)與不可連結性(Unlinkabiliy)。

接著透過比較其他的匿名驗證方式，以證明我們所提出的做法確實比現有的方法來的優秀。

5.1 正確性

首先假設 $f(x)$中所有 x，x=$k_i \in \{k_1, \dots, k_l\}$，則 $f(x)$=1。令$T_i = T_{i,1} + T_{i,2} = s_i R + \beta X_3$。我們可以推得$\sum_{i=0}^{l} a_i s_i = a_0 s_0 + \cdots + a_l s_l$，

則$\sum_{i=0}^{l} a_i s_i = a_0 s_0 + \cdots + a_l s_l$

$= a_0(H(W_1')^0)$+$a_1(H(W_1')^1)$+$\cdots$+$a_l\big(H(W_1')^l\big)$

=$(a_0 k_1'^0$+$a_1 k_1'^1$+$\cdots$+$a_l k_1'^l)$

=1

由以上結果，可知

$\prod_{i=0}^{l} \hat{e}(C_i, T_i)$=$\prod_{i=0}^{l} \hat{e}(C_i, T_{i,1} + T_{i,2})$

=$\prod_{i=0}^{l} \hat{e}(C_i, T_{i,1}) \prod_{i=0}^{l} \hat{e}(C_i, T_{i,2})$

=$\prod_{i=0}^{l} \hat{e}(ra_i P_1, s_i R) \prod_{i=0}^{l} \hat{e}(ra_i P_1, \beta X_3)$

$=\hat{e}(P_1, R)^{r\sum_{i=0}^{l} a_i s_i} \hat{e}(\sum_{i=0}^{l} r a_i P_1, \beta X_3)$
$=\hat{e}(P_1, R)^{r} \hat{e}(r(a_0 + \cdots + a_l)\beta P_1, X_3)$
$=\hat{e}(rP_1, R)\hat{e}(B_2, X_3)$
$=\hat{e}(r\alpha P_1, \alpha^{-1}R)\hat{e}(B_2, X_3)$
$=\hat{e}(B_1, V)\hat{e}(B_2, X_3)$

5.2 匿名性與不可連結性

以下討論匿名驗證的安全性要求：匿名性與不可連結性。

(1)匿名性：在發起人製作使用者的名單時，除了將使用者的 *ID* 放入雜湊函數 H 之外，發起人也運用 DHKE 的技巧，將使用者的公鑰用自己所掌握的私鑰加密，跟 *ID* 串接後在放入 H 中產生 k。使用者也透過類似的方式產生自己要送給伺服器的T_Q(使用者將發起人的公鑰用自己的私鑰進行加密)。由於伺服器端無法得知雙方 DHKE 之後的結果，所以不論是在C_D或是T_Q都無法或的使用者的真實身分，此做法可以保證使用者的匿名性。

(2) 不可連結性：在使用者製作T_Q時，加入隨機數 R 使得每次生成的T_Q都不相同，讓伺服器端無法透過多次的 session message 後得知使用者的真身分。為了擁有註銷使用者的能力，所以 R 會公開給伺服器端，但是在基於 Discete Logarithm 的假設下，就算知道 $R, s_i R$還是無法求出s_i。在此情況下可以保障不可連結性成立。

(3)不可偽造性：在伺服器進行驗證時，需要計算

$\prod_{i=0}^{l} \hat{e}(C_i, T_i)=\hat{e}(B_1, V)\hat{e}(B_2, X_3)$

在此我們討論不合法的使用者將無法通過驗證式的驗證。

在驗證式中只有C_i, B_1可以讓使用者自行計算，在此條件下不合法的使用者想要偽造數據令驗證式通過，相當於解 Discete Logarithm 問題，所以是不可行的。

5.3 效能分析

我們跟 Sunder 等學者的論文[15]進行比較，可以得出兩點優勢。首先在我們所提出的方案中，除了基本的 Initial、Registration 以及 Authentication 之外，還另外提出了如果有存在惡意的使用者在系統中，可以透過 Server 跟可信任第三方一起合作，進而註銷使用者權限的功能。Sunder 等學者的論文中，最後進行驗證的階段時，使用者方所要付出的計算量為包含 pairing，而在我們的方案中，使用者的計算量只有包含到指數的運算，所以可以確定我們所提出的方案確實比 Sunder 等學者的論文來的有效率。

6. 結論

在本文中，我們提出一個新的達到匿名驗證的方法。首先對匿名驗證、關鍵字搜尋以及 DHKE 做概念性的介紹，接下來透過修改 Lindell 等學者及 Chen 等學者分別對於匿名驗證以及關鍵字搜尋所提出的新方法，得到我們的植基於關鍵字搜尋之匿名驗證。最後我們分析驗證式的正確性以及提出的方法有沒有滿足匿名驗證的要求。

在未來的研究中，我們希望能夠對此方法進行優化的處理，讓他在計算量或是傳輸量上能夠有所提升。

致謝

本研究接受科技部編號：MOST 104-2221-E-005-047 研究計畫經費補助。

參考文獻

[1] I. Teranishi, J. Furukawa, K. Sako. ”k-Times Anonymous Authentication.”. In ASIACRYPT, pp. 308-322, 2004.

[2] Kuo-Chang Chen, Yu-Chi Chen, Gwoboa Horng.”Efficient public key encryption with user-friendly keyword search for searchable cloud storage”. International journal of communication systems, pp.2-12, 2014.

[3] Yehuda Lindell.”Anonymous Authentication.”. In Journal of Privacy and Confidentiality, pp. 35-63. 2010.

[4] Jingwei Liu, Zonghua Zhang. “Certificateless Remote Anonymous Authentication Schemes for wireless Body Area Networks”In IEEE Transections on parallel and distributed systems vol.25 no.2, pp. 332-342, 2014.

[5] Man Ho Au, Willy Susilo, Yi Mu.”Constant-Size Dynamic *k*-TAA”In SCN, pp. 111-125. 2006.

[6] D. Boneh, X. Boyen.”Short group signature”. In EUROCRYPT, pp. 41-55, 2004.

[7] J. Zhu, J. Ma.”A New Authentication Scheme with Anoymity Wireless Environments”. In IEEE Trans. Consumer Electronics, vol. 50, no. 1, pp. 231-235, 2004.

[8] Long-Hai Li, Cheng-Qiang Huang, Shao-Feng Fu.”Pairing-based Anonymous Boardroom Voting Scheme”. In International Conference on Cyber-

Enabled Distributed Computing and Knowledge Discovery, pp. 264-268, 2014.

[9]D. Song, D. Wagner, A. Perrige. ”Practical techniques on encrypted data”. In Proceedings of the IEEE Security and Privacy Stmposium, pp. 44-55, 2000.

[10] Xuefei Cao, Xingwen Zeng, Weidong Kuo, Liangbing Hu. ”Identity-Based Anonymous Remote Authetication for Value-Added Services in Mobile Networks”. In IEEE TRANSACTIONS on Vehicular Technology, vol. 58, no. 7, pp. 3508-3517, 2009.

[11] Y. Zhang, W. Lou, Y. Fang. ”Anonymous on-demand routing in mobile ad hoc networks”. In IEEE Trans. Wireless Communication, vol. 5, no. 9, 2006.

[12] S. J. Wang. ”Anonymous wireless authentication on a portable cellular mobile system”. In IEEE Trans. Comput. Vol. 53, no. 10, pp. 1317-1329, 2004.

[13] L. Zhu, F. Zhang. ”Efficient ID-Based ring signature and ring signcryption schemes”. In International Conference on Computational Intelligence and Security, vol. 2, pp. 303-307, 2008.

[14] Y. Yu, Y. Bo, C. Xu, Y. Sun. ”An efficient identity based anonymous signcryption scheme”. In Journal of Natural Science, vol. 13, pp. 670-694, 2008.

[15] Sunder Lal, Prashant Kushwah. “Anonymous ID Based Signcryption Scheme for Multiple Receivers”. In Cryptology ePrint Archieve: Report 2009/345.