東海大學資訊管理研究所
碩士學位論文

在智慧卡上使用可取消式指紋模板的多重指紋序列認證系統

A novel multi-fingerprint authentication system based on cancelable fingerprint templates with smart card

指導教授：余心淳 博士
研究生：黃　能 撰

中華民國 106 年 7 月

東海大學資訊管理學系碩士學位
考試委員審定書

資訊管理學系研究所 黃 能 君所提之論文

在智慧卡上使用可取消式指紋模板的多重指紋序列認證系統

經本考試委員會審查，符合碩士資格標準。

學位考試委員會 召集人：段翰文 (簽章)

委 員：張學庸

段翰文

余以淳

中 華 民 國 106 年 7 月 5 日

誌 謝

隨著論文逐步完成之際，逐漸的從我心底湧出一股別離的惆悵，即將離開東海的校園與師長讓我突然意識到我有多麼的不捨，從大學到碩士東海帶我走過一段難忘難捨的求學經歷。

此篇論文的完成，首先要感謝我的指導教授余心淳老師，在寫作過程中用心的指導與鼓勵。這段從大學專題的指導教授到碩士論文指導教授而結下的特殊師生情緣，期間若沒有教授的耐心和不離不棄的扶持，學生是無法走到今天的，對教授的感謝學生將永記於心。

其次我要感謝我的口試委員教授段翰文教授與張榮庭教授。感謝兩位老師百忙之中抽空參與學生的口試，對學生的論文提出諸多寶貴建議，並且兩位老師對於學生論文不辭辛勞提供各項細微明確的意見修改與註記讓學生獲益良多，也因為兩位老師的指教，使全篇論文更加充實完善。

也非常感謝東海大學的優美環境伴我度過非常多有笑有淚的歲月，在求學其間每每看到許多到此遊玩的旅客，隨即想到再過不久我便不再是東海大學的學生，將來也會以一個旅客的身分重訪我的母校隨即心中又再次悵然若失，真的很感謝東海帶給我的一切，在這邊度過的每一刻都將是一輩子的回憶。

最後，還要感謝親愛的家人與朋友們，在我就讀研究所及論文寫作期間給予我的支持與陪伴，這篇論文也是因為有他們的陪伴與鼓勵才得以順利完成，要感謝的人事物還有很多很多，沒有寫在這裡的，在此也都一併感謝在心裡。

黃　能 謹誌於

東海大學資訊管理研究所

中華民國 106 年 7 月 20 日

論文名稱：在智慧卡上使用可取消式指紋模板的多重指紋序列認證系統

校所名稱：東海大學資訊管理學系研究所

畢業時間：2017 年 07 月

研究生：黃　能　　指導教授：余心淳博士

論文摘要：

近年來對於準確、高效的使用者認證方法受到越來越多的關注。由於個人指紋是獨特且易於使用的，所以指紋識別技術已被廣泛應用，此外指紋掃描器隨著時間的演進逐漸支持多重指紋辨識掃描，所以本研究提出基於使用多重指紋序列模板取代單一指紋模板與使用者密碼的雲端智慧卡認證方法。增加以往生物辨識模板的使用與比重，透過多重且可重複的指紋模板序列，以此提高認證安全性並藉由多重指紋模板的排列複雜度，取代傳統基於使用密碼的認證方法。研究提出的認證方法是使用高安全性的生物雜湊演算和單向雜湊函數來確保使用者認證資料的隱密性、使用者生物特徵的私密性與可取消性。有別於一般的雜湊函數，生物雜湊演算(Biohashing)是一種可取消式的指紋模板保護技術，也是一種專門用於生物特徵模板的鹽析湊雜演算，透過該演算可以將指紋特徵轉換成具有和生物特徵模板高度相依性的位元串資料稱作生物碼(Biocode)，同時生物特徵模板具有可取消的特性，亦可確保使用者原始的生物特徵資訊無法洩漏或竄改的可能性。此外本研究所提出的認證方法將可防止通訊屏蔽、通訊重送、假冒攻擊以及強化相互認證。

關鍵字：認證、生物辨識、可取消式指紋模板、多重指紋序列、生物雜湊驗算、智慧卡

Title of Thesis：A novel multi-fingerprint authentication system based on cancelable fingerprint templates with smart card

Name of Institute: Tunghai University, Institute of Information Management

Graduation Time：（07／2017）

Student Name：Neng Huang　　Advisor Name：Hsin-Chun Yu

Abstract：

In recent years, more and more attention has been paid to accurate and efficient user authentication methods. Due to the fingerprints of human beings are unique and easy to use, fingerprint identification techniques have been widely used. In addition, fingerprint scanners gradually support multiple fingerprint identification scans over time, wherefore this paper proposes a high-security cloud-based business smart card authentication mechanism based on the use of multiple fingerprint sequences to replace single fingerprint templates with user passwords. Increase the use of biometric templates and the proportion of the use of multiple and repeatable fingerprint template sequence, to improve the security and rely on multiple fingerprint template layout complexity, replacing the traditional use of password authentication mechanism. The research mechanism proposed in this study is to use highly secure Biohashing and one-way hash functions to ensure the confidentiality of user authentication data, privacy and exclusivity of user biometrics. Different from the general hash function, Biohashing is a salting consideration that is devoted to the biometric template. Through this algorithm, the fingerprint feature can be converted into bits string data named Biocode. Simultaneously, the biometric template can be cancel, to ensure that there is zero possibility the user's original biometric information can be compromised or tampering. Furthermore, in the process of user authentication, the certification mechanism proposed in this study will prevent communication shielding, communication re-transmission, counterfeiting attacks and enhanced mutual authentication.

Keywords：Authentication, Biometrics, Cancellable fingerprint templates, multi-fingerprint, Biohashing, Smart cards.

目 錄

表目錄

圖目錄

第一章　緒 論

第一節　研究背景與動機

在行動電子商務與網路雲端服務快速整合發展之下，使用者透過網路使用遠端交易多樣化的應用服務與商務模式與日俱增，為了滿足使用者可隨時隨地存取遠端資源服務的需求，伺服器必須能有效地認證遠端使用者的身份，因此建構一個注重安全性、隱私權、可靠性與便利性的網路傳輸環境與資訊系統平台乃為當務之急。近年來使用智慧卡對使用者遠端身分識別的認證需求大幅提升，許多使用智慧卡認證的雲端服務如：網路銀行、電子支付、第三方支付或跨境支付，都須依賴安全可靠的使用者認證方法，以此作為行動電子商務服務發展中的重要基石。使用智慧卡的遠端身份認證機制與資料安全傳輸協定至今已被廣泛的討論，應用智慧卡可以將使用者的 ID、密碼與認證參數儲存在晶片內，使得遠端伺服器不再需要儲存密碼表，可以順利解決伺服器成本以及安全性的問題。然而基於密碼的身份驗證方法還是不夠安全並且相應的使用者安全認證技術的演進卻未跟上其相關雲端平台服務發展的速度，因此提供快速可靠的使用者認證方法是極需被重視的議題。隨著認證方法的不斷改進，從最基本基於使用帳戶和密碼的認證方法到單一生物辨識模板的使用，彌補了單純只基於使用者帳戶和密碼認證結構策略上的不足如：密碼輕易的被猜測、密碼在使用時被窺視、輕易的被分享複製被轉發等問題。然而使用單一生物辨識資訊改善的使用者認證方法卻仍然沒有解決使用密碼認證的根本問題，既密碼需被額外記憶與管理。一般情況下普通使用者可能擁有許多需要以帳戶與密碼進行存取的雲端服務，持續使用密碼作為你所知道的認證因子，無疑會增加使用者記憶與管理帳戶密碼的困難。此外使用者為了使用上的方便往往設定了最小密碼長度，這樣的設定很可能會導致認證結構出現致命性弱點。

而為了克服這些問題，在此類使用者認證方法中常使用長密碼和加密金鑰。但該方法的問題是密碼過長不易使用且難以記憶，再加上這些認證資訊必須儲存在某些地方，所以隨著註冊使用者的增加，秘密金鑰的儲存成本與管理勢必變也將變得昂貴且困難。所以本研究提出基於使用多重有序指紋模板取代單一指紋模板與使用者密碼的認證技術來改善上述之問題，因為多重指紋模板具有排列的特性，須

依正確的指紋輸入順序才可通過認證且相同的指紋資訊可重複輸入。與使用密碼相比，密碼需要依靠長度才得以保證其安全強度，但是過長的密碼卻又難以記憶，然而使用有序的指紋只需記憶輸入的指紋序列之順序，其記憶難度將極大降低並產生高度複雜且安全的認證因子。例如當設定的指紋模板數是 6 時，其可能性便有 10^6 種的排列組合，但這邊我們需要強調，這 10^6 種不同的序列全是使用者的指紋模板所構成，而跟密碼不同的是，生物特徵資訊難以窺視、幾乎無法複製、不能隨意共享轉發以及難以透過數位攻擊破壞。

第二節　研究目的

由於基於密碼與單一生物辨識資訊的使用者驗證方法有許多安全上的隱患，所以本研究提出新穎的身份驗證方法來改進這些問題，並希望透過本研究達成以下成果：

(1) 透過多重序列指紋模板的使用取代使用者密碼，以達成更安全、更高效、更易用且更完善的認證有效性。

(2) 多重序列指紋模板的使用大幅度增加了攻擊者透過盜取使用者指紋進行非法存取的難度。因攻擊者不知道使用者當時註冊時輸入了那些指紋資訊，同時也無法知道指紋資訊輸入時的順序。

(3) 使用生物雜湊演算生成的指紋模板具有可取消性，讓使用者可以使用相同指紋資訊註冊多種不同雲端服務，此外假使當產生之指紋辨識模板不幸遭到竊取或破壞，也可以透過修改生物雜湊演算的參數重新使用相同指紋資特徵資訊產生新的指紋辨識模板。

本篇研究將使用生物雜湊演算生成的指紋模板具有可取消性，讓使用者可以使用相同指紋資訊註冊多種不同雲端服務，此外假使當產生之指紋辨識模板不幸遭到竊取或破壞，也可以透過修改生物雜湊演算的參數重新使用相同指紋資特徵資訊產生新的指紋辨識模板。

第三節　研究架構

本篇論文將以 Khan 與 Kumari 的方法[1]為基礎，通過提出改進的使用者認證方法來消除他們方法的弱點。本論文之架構共分為四章。第一章為緒論，主要是說明論文的研究背景與動機和研究目的。第二章為相關研究，將會介紹生物辨識技術，並討論過去學者所提出的遠端認證方法的相關文獻以及認證方法需要具備的基本要求，並分析遠端使用者身份認證時所容易遭受的各種攻擊，以及本文所提及之生物雜湊演算(Biohashing)之相關知識。第三章則會詳細說明本文所提出之遠端認證方法，並且進行安全性分析、功能分析以及計算成本分析，並且與過去學者所提出的基於指紋識別遠端認證方法進行比較。第四章為結論將整理本論文的研究成果與貢獻，以及本論文研究未來的發展方向。

第二章　相關研究

第一節　生物特徵辨識技術

生物特徵辨識基本上是一種模式識別系統，從個體獲取的生物特徵資訊中，提取特徵集並將該特徵集與資料庫中的生物特徵模板進行比較[2][3]。近年來生物特徵識別技術有了快速的進步，並且也被廣泛的應用，而生物特徵具有以下特點[4]:

(1) 普遍性(Universality): 每個人天生均擁有這些生物特徵。

(2) 獨特性(Distinctiveness): 任意兩人的生物特徵都會呈現相當程度差異性。

(3) 持久性(Permanence): 每個人的生物特徵即使很長的時間也不會發生變化。

(4) 可收集性(Collectability): 生物特徵可以用定量方式來測量。

而生物特徵識別的種類有人臉(Face)、指紋(Fingerprint)、虹膜(Iris)、視網膜(Retina)、掌型(Hand Geometry)、掌紋(Palm Print)、聲紋(Voice Pattern)、血管(Vein)、DNA 以及體味(Body Odor)等等。而其中又以指紋辨識技術發展最久也最純熟，而且成本相對低，因此應用的最為廣泛。而基於使用者生物特徵資訊而生成的生物特徵密鑰具有以下特性[5]:

(1) 生物特徵不會丟失或遺忘。
(2) 生物特徵是非常難以複製或共享。
(3) 生物特徵是非常難以偽造或分發。
(4) 生物特徵幾乎無法被猜到。
(5) 生物特徵不容易被其他人破壞。

在[6]的章節 7 — 生物辨識資訊是否能取代密碼?(Can Biometrics Replace Passwords?)中指出在合理並完善的使用者身份認證結構中使用生物辨識資訊能有效的抵擋在不安全的網路上進行存取時可能遭受的攻擊如網路釣魚(phishing)等，此外[7]提到使用密碼存在許多被廣泛認可的問題，而它們的缺點還未被解決，且一般人對於不停的更改與記憶密碼來維持身份認證的安全性感到厭煩，而生物辨

識資訊並沒有這類問題，因為一般人沒有辦法忘記他們的生物特徵資訊，且生物特徵資訊也幾乎不可能偽造。而在[8]提到生物辨識資訊的使用解決了一般人使用過於簡的使用者帳戶與密碼的問題，因為生物辨識有別於普通的字元符號，一般人無法直接依靠肉眼讀取生物辨識資訊，而且也無法簡單的被創造出來，因為有別於字元符號，生物辨識資訊是複雜並且難以竊取與分享的。

然而，生物辨識技術會面臨許多安全風險，特別是生物辨識模板的隱私和儲存問題[9]。因為這些因素，所以勢必要提出一種高效的保護生物辨識模板安全和隱私的方法。生物特徵模板保護方法可以大致分為兩類[10]：生物辨識加密系統(Biometric cryptosystem)以及可取消式的生物辨識技術(Cancelable biometrics)。生物辨識密碼系統的宗旨是使用生物特徵來確保秘密金鑰的安全性或直接從生物特徵產生加密金鑰。生物辨識加密系統可以進一步劃分為密鑰綁定和密鑰生成，具體取決於特徵資訊的獲取方式。

另一方面，可取消式的生物辨識技術是另一種保護生物特徵模板的方法。它是依靠所產生的生物特徵模板的不可逆變換特性來代替原始生物特徵資訊，其後僅存儲變換後的模板，以確保生物特徵模板的安全和隱私[11]。因此如果一個可取消式的生物特徵模板被破壞，則可以從相同的使用者生物特徵重新生成新的生物特徵模板。可取消式的生物辨識技術在文獻中有兩種主要方法，即非可逆變換(Non-invertible transform)[12]和生物特徵鹽析技術(Biometric salting)[13]。本篇所使用的生物雜湊演算(Biohashing)[14]是生物特徵鹽析技術(Biometric salting)的代表性實例之一，我們將在第貳章中詳細敘述。

儘管已經提出了各種解決方法來保護生物特徵模板，但是設計一種滿足以下條件的模板保護方法並不容易。Teoh 等人指出[15]指出生物特徵模板保護方法應該具備下列特性：

(1) 多樣性(Diversity)：

受保護的生物特徵模板不能允許在不同應用程序之間進行匹配，從而確保使用者的隱私。

(2) 可再用性(Reusability)：

如果舊的生物特徵模板被盜取或受損，可以重新產生新的受保護的生物特

徵模板。

(3) 不可逆性(Noninvertibility)：

幾乎不可能從受保護的生物特徵模板和相關資料逆向獲取原始的使用者生物特徵資訊。

(4) 性能(Performance)：

錯誤接受率(False acceptance rate，FAR)或 錯誤拒絕率(False rejection rate，FRR)的識別性能不應低於使用原始生物特徵模板的性能(我們會在此章中的第三節再次討論 FAR 與 FRR)。

第二節　遠端使用者認證方法的基本要求

透過文獻探討我們發現單純的加入並使用單一生物辨識資訊(如單一指紋模板資訊)並不能解決使用密碼本身所存在的缺陷。然而在這個問題上根據以往的研究 Li 與 Hwang[5]以及 Das 與 Goswami[16]列舉了一些基於生物識別的遠端使用者認證方法的基本要求。以下所列的安全要求與功能性要求至關重要，這些先決條件解決了使用智慧卡並結合生物辨識資訊方法中的潛在安全議題。對於使用者認證的保護方法每項要求與條件都是最基本並獨立的。因此本篇的研究目的是提出一種新的遠端使用者認證方法，以滿足以下基本要求，從而為使用多重指紋序列的使用者認證方法建立標準。

一、安全要求

必須能防止以下攻擊[5][16]：

(1) 使用者或伺服器假冒攻擊(Masquerade attacks)：

在這種惡意攻擊中，攻擊者可能會嘗試假冒成合法使用者與伺服器進行認證通訊，或者攻擊者假冒成合法伺服器，以便欺騙合法使用者進行認證通訊，進而竊取使用者登入資訊或其他與使用者相關的私密資料。

(2) 重送攻擊(Replay attacks)：

攻擊者透過在不安全的網路上進行通訊竊聽和資訊竊取，試圖阻止合法使用者與合法伺服器兩方之間相互通訊，然後冒充其中一方如合法使用或合法伺

服器等其他方式來重送先前攔截複製的資訊以進一步欺騙。

(3) 中間人攻擊(Man-in-the-middle attacks)：

在不安全的網路上進行通訊時，攻擊者可能會在傳輸過程中攔截訊息，然後可以更改或刪除或修改發送給接收者的訊息內容。

(4) 拒絕服務攻擊(Denial-of-service attacks)：

如果攻擊者阻止合法使用者傳送訊息至合法伺服器，便會使服務暫時中斷或停止，導致合法使用者無法存取遠端伺服器上的服務。

(5) 會話攻擊(Session attacks)：

其原理是攻擊者利用認證通訊時出現的漏洞，在使用者嘗試存取伺服器之前攻擊者先與伺服器建立會話，然後誘導使用者使用已建立的會話存取伺服器上的資源與服務。當使用者成功登入伺服器後，攻擊者就可以利用這個先前使用者與伺服器所建立的會話欺騙伺服器存取使用者的私密資訊，並利用這些私密資訊來啟動新的會話協議。

(6) 智慧卡資訊竊取攻擊(Loses the smart card)：

如果使用者丟失智慧卡或被盜，攻擊者可能可以使用能量分析攻擊或旁道攻擊竊取存儲在智慧卡中的所有敏感資訊，然後利用這些竊取來的資訊，攻擊者可以推導出使用者私密資訊或其他登入訊息。

二、功能要求

基於生物特徵的遠端使用者認證方法應滿足以下功能要求[5][16]：

(1) 相互認證(Mutual authentication)：

在兩個通訊方之間提供相互認證，並在認證成功後，應建立秘密會話密鑰，此會話密鑰為先前進行相互身分認證時所傳遞的關鍵秘密資訊，透過一些資訊保護手段如互次或演算(XOR)等，以確保只有合法的受信端才能還原出原始訊息中的關鍵資訊，並藉著相互分享只有自己知道的關鍵資訊，作為之後傳遞資訊的互斥或(XOR)運算密鑰，以便雙方之間進行安全通訊。

(2) 運算成本(Computational cost)：

在使用者進行註冊與登入請求時的身份認證通訊時，其認證計算的成本如單向雜湊演算的次數等因該盡量控制在一定的運算量之內以維持身分認證的效率。

(3) 變更登入資訊(Choose and change the passwords)：

允許使用者在本地端免費選擇和更改密碼，而無需進一步與伺服器進行聯繫。因此，它可以減少額外通訊和運算成本，藉此避免使用者與伺服器通訊雙方之間在不安全網絡上的一些可能遭受的惡意攻擊。

(4) 無須儲存與維護使用者登入資訊(Work without storing the password and verificationtables)：

在一般的認證系統中，伺服器會儲存使用者的登入相關資訊如使用者密碼的雜湊值在系統的驗證資訊表中，當使用者請求登入系統時便會依據使用者所輸入的登入關鍵資訊的雜湊值與伺服器所儲存的雜湊值相互比較是否一致，如果一致，則使用者通過身分驗證。然而若是系統支持不儲存密碼和驗證表，則是利用從使用者所送出的登入請求訊息進行特別的演算，以運算時間換取儲存空間的方式驗證使用者的身分，將可以防止伺服器可能被攻破導致密碼表被竊取或修改此外也節省了維護驗證資訊的時間與成本。

(5) 支持無時間同步(Support without synchronized clocks)：

當使用者與伺服器雙方無法進行時鐘同步時，支持沒有同步時鐘的認證通訊。

(6) 生物辨識資訊(Provide non-repudiation)：

由於採用個人生物識別技術，有別於密碼容易被非法竊取複製等，因此提供使用者認證時身份的不可否認性。

第三節 相等錯誤率(Equal error rate，EER)

相等錯誤率(Equal error rate，EER)[17]是一種特別的度量指標，通常被用作表示生物特徵辨識系統的精度與安全性強度。它是依照兩個重要的生物辨識比率—錯誤接受率(False acceptance Rate，FAR)與錯誤拒絕率(False rejection Rate，FRR)所決定，其中錯誤接受率(FAR)表示為當不應該通過認證的使用者卻通過生物辨識的比率；錯誤拒絕率(FRR)表示為應該通過認證的使用者卻被拒絕通過生物辨識的比

率，而當錯誤接受率(FAR)和錯誤拒絕率(FRR)是相同值時，其值被稱為相等錯誤率(EER)。如圖 2-1 所示，當生物辨識系統的敏感度(Sensitivity)越低時錯誤拒絕率(FRR)將越低，但與此同時錯誤接受率(FAR)將會越高，因為當生物辨識系統的敏感度越低的時候，表示系統能接受的生物辨識資料的容忍度將越寬，所以使用者將越容易通過身份驗證，但相反的也將越容易讓假冒者成功欺騙系統並通過身份驗證。

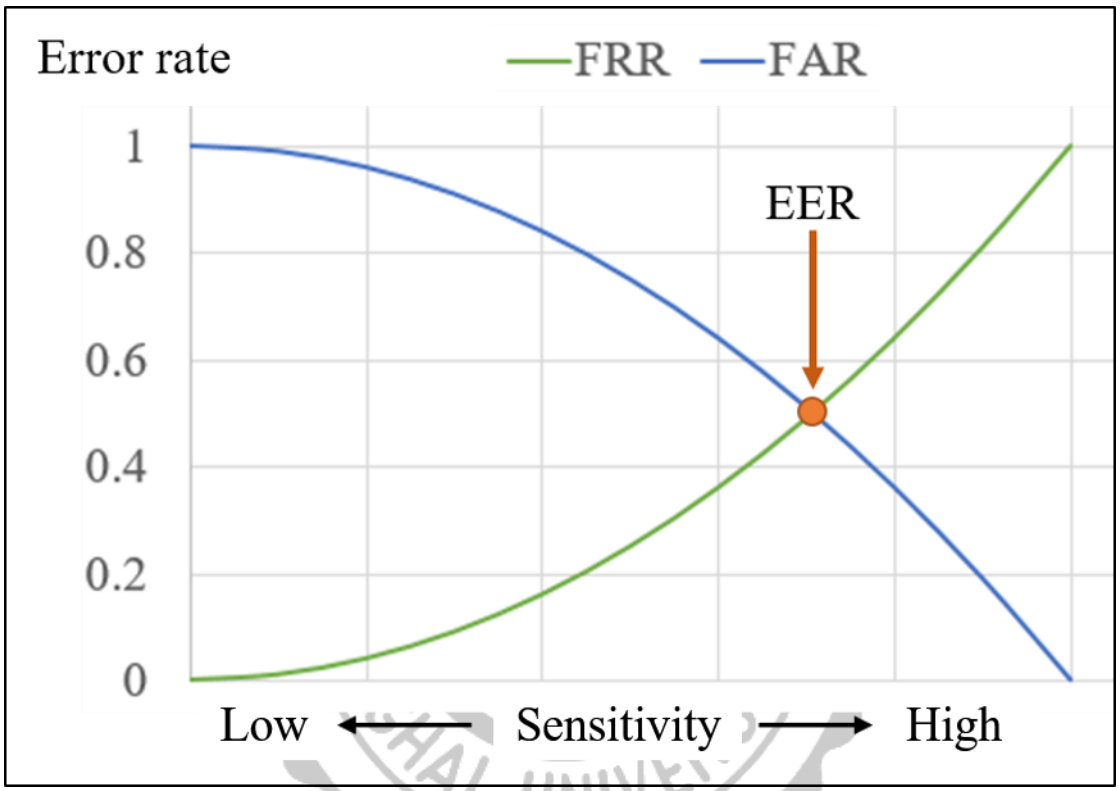

圖 2-1. FAR、FRR 以及 EER 關係圖

而若是生物辨識系統的敏感度越高時，情況則相反，此時錯誤接受率(FAR)將會越低，而錯誤拒絕率(FRR)將越高，因為當生物辨識系統的敏感度越高的時候，表示系統能接受的生物辨識資料的容忍度將越窄，所以使用者將越難通過身份驗證，但相反的也將越容易排除假冒者成功欺騙系統並通過身份驗證的可能性，而當錯誤接受率(FAR)與錯誤拒絕率(FRR)相等時，其值被稱為相等錯誤率(EER)。我們可以很容易的發現當一個辨識系統的錯誤接受率(FAR)與錯誤拒絕率(FRR)均越低的時候，表示系統的辨識精度將越高。此外，因為生物辨識資料容易受到環境、溫度以及濕度等影響，所以生物辨識系統需要設置合理的敏感度，因為當生物辨識系統敏感度設置太高時將會加大使用者被錯誤拒絕的機率(因為外在或其他因素導致生物辨識資料擷取不完整)，但當生物辨識系統敏感度設置太低時，又無法可靠的

阻擋試圖假冒成合法使用者的攻擊者通過生物辨識認證。為了解決這樣的困難，因此相等錯誤率(EER)是一個重要的參考指標，它能幫助系統設置合理的辨識敏感度以解決上述的問題，同時當相等錯誤率(EER)越低時，生物辨識系統的精度與高全性都將越高。

第四節 生物雜湊演算(Biohashing)介紹

生物雜湊演算是一種可取消式的生物辨識模板保護技術[18]，它是利用生物雜湊演算的非可逆轉換的特性來實現可取消式的生物特徵模板保護技術，也被稱為生物特徵鹽析技術[13]。此演算方法是利用標記化的偽隨機亂數(Tokenized random number，TRN)[19]以及使用者特定的生物辨識特徵[20]產生具有高度相依性的位元串資料稱作生物碼(Biocode)[21]。此演算是一種新穎的雙因子認證方法，因為成功的結合了使用者特定的生物辨識特徵資訊和標記化的偽隨機數。生物雜湊演算與單獨的生物特徵相比具有顯著的性能優勢，例如在不提高錯誤接受率(FAR)的前提下能保有極低的誤差率和高度辨識率[19]。簡單來說生物雜湊演算是一種把經過轉換的生物特徵資訊透過迭代內積運算映射到二進制資料表示法的轉換技術。Belguechi 與 Rosenberger[22]的研究顯示生物雜湊演算用於人臉(Face)、掌紋(Palmprint)、指紋(Fingerprint)以及虹膜(Iris)辨識等，均有極低的相等錯誤率(EER)。

基礎的生物雜湊演算程序首先被用於指紋辨識系統上[14]，其過程可以劃分為以下五個步驟：

- Step1 ：擷取指紋特徵訊號，並對擷取的訊號作預處理，最後生成生物特徵向量 $\{f_i \in \mathcal{R}^n | i = 1, \ldots\ldots, \mathrm{n}\}$。預處理過程使用集成小波轉換(Integrated wavelet)和傅立葉 - 梅林轉換(Fourier-Mellin transform)保留指紋圖像的局部邊緣影像並減少低頻域中的雜訊(高能壓縮/ Highenergy compacted)，因此降低指紋圖像形狀失真時對於辨識效能的影響。除此之外，圖像尺寸的減小還有助於提高計算效率，其轉換過程如圖 2-2。

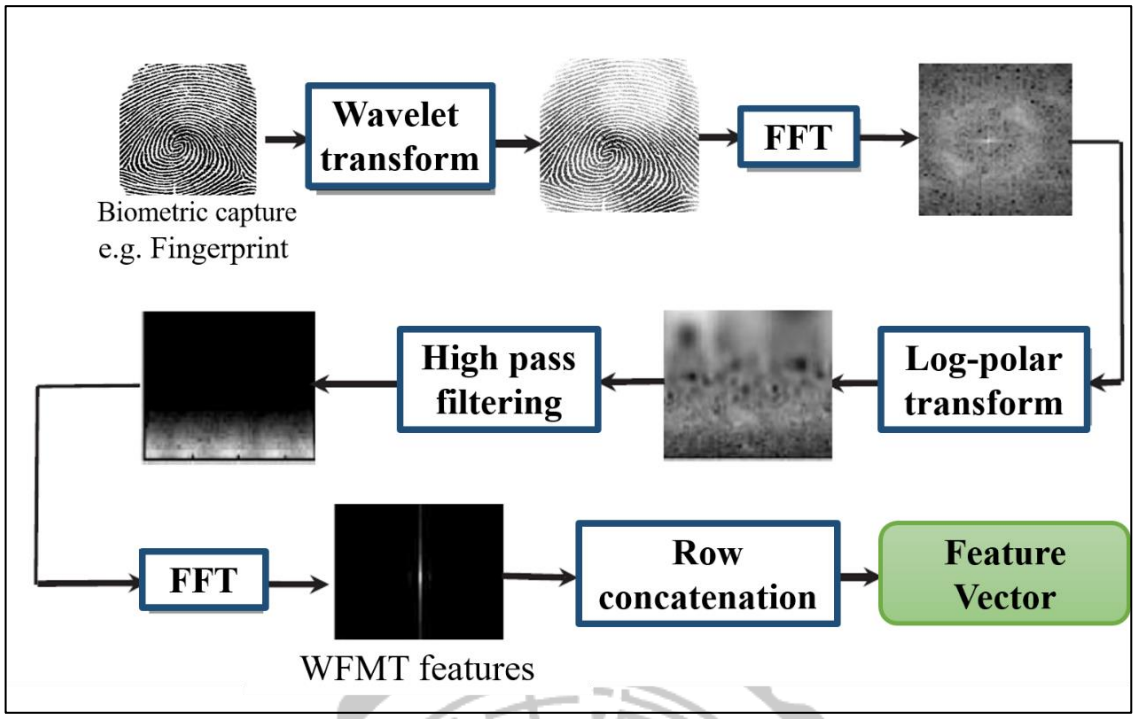

圖 2-2. 指紋特徵訊號預處理流程[14]

● Step2 ：利用使用者所持有的權杖(Token)(如實體物件：智慧卡、隨身碟..等等)中的偽隨機亂數種子(Seed)來產生偽隨機向量集$\{v_i \in \mathcal{R}^n | i = 1,2,\dots,\mathrm{m}\}$。

● Step3 ：利用正交轉換程序(e.g. Gram-Schmidt orthogonalization)，轉換偽隨機向量矩陣集$\{v_i \in \mathcal{R}^n | i = 1,2,\dots,\mathrm{m}\}$產生正交向量矩陣集$\{v_{\perp i} \in \mathcal{R}^n | i = 1,2,\dots,\mathrm{m}\}$。

● Step4 ：把從 Step 1 得到的生物特徵向量集$\{f_i \in \mathcal{R}^n | i = 1,2,\dots,\mathrm{m}\}$與步驟 3 得到的正交向量矩陣集$\{v_{\perp i} \in \mathcal{R}^n | i = 1,2,\dots,\mathrm{m}\}$作內積運算$\{\langle f_i \mid v_{\perp i}\rangle \in \mathcal{R}^n | i = 1,2,\dots,\mathrm{m}\}$，其中⟨A|B⟩表示內積(Inner product)運算程序。

● Step5 ：使用預設閥值(Threshold)τ 將步驟 4 的內積結果轉成生物碼(Biocode)，$\{b_i \in 2^m | i = 1,2,\dots,\mathrm{m}\}$，方式如 $b_i = \begin{cases} 0 & if \ \langle f_i | v_{\perp i}\rangle \le \tau \\ 1 & if \ \langle f_i | v_{\perp i}\rangle > \tau \end{cases}$ $m \le n$。圖 2-3 顯示了基礎生物雜湊演算的過程。

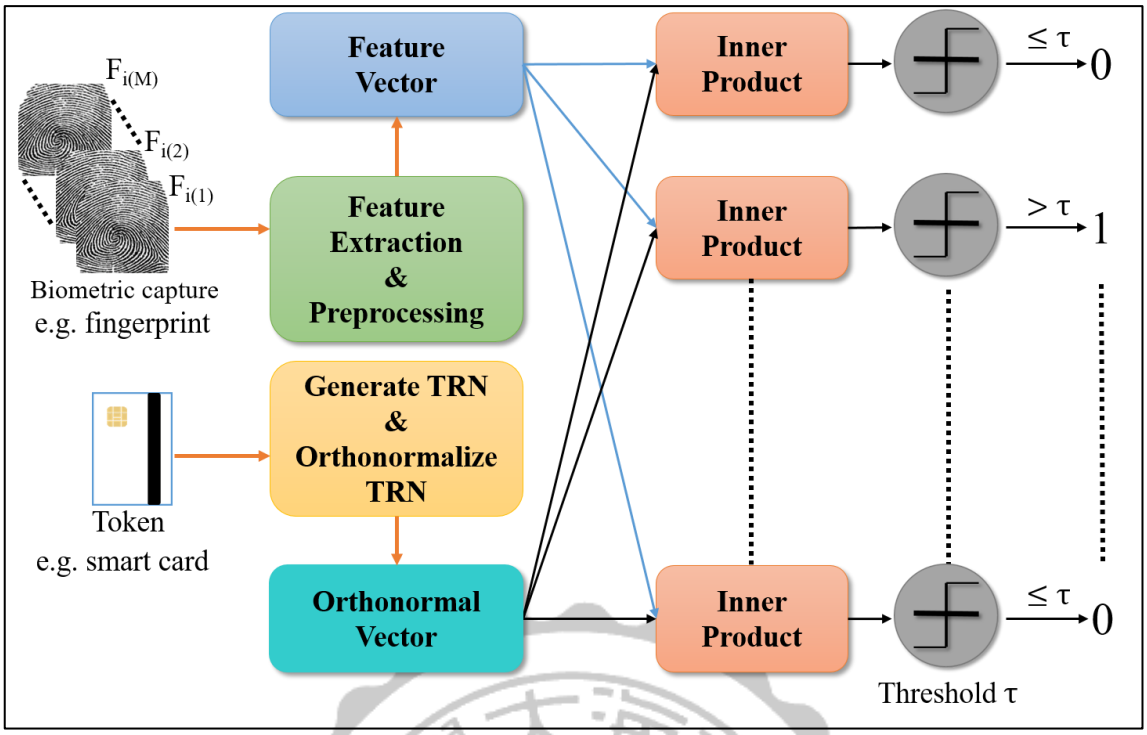

圖 2-3. 基礎生物雜湊演算程序圖

基礎的生物雜湊演算(如圖 2-3 所示)經過許多的討論與應用後，有一些研究指出其演算方法在現實情境中的應用存在缺陷[23][24]。在現實環境中若是攻擊者 A 取得了合法使用者 B 的權杖(Token)或者雜湊密鑰(Hash key)，生物雜湊演算的安全性將低於只使用原本的生物特徵辨識資訊。這說明在此認證演算中，Token 的重要性比生物辨識資訊還高，如此並不符合使用生物特徵模板技術作為身份認證的初衷。對於上述潛在的安全問題 Lumini 與 Nanni[25]提出改進的措施，他們認為當亂數 Token 被竊取的情況發生時，可以通過增加生物碼(Biocode)長度的方式，來提升生物辨識資訊在生物雜湊演算中的主導性，因此他們提出了四個可行的改進措施用以增加生物碼的長度：

- 正常化(Normalization)：在執行生物雜湊演算前，通過對生物特徵向量進行一般化，使得內積運算的結果坐落在[-1,1]之間。
- τ變異(Variation)：使用多個不同數值的τ，讓τ在其最大值和最小值之間變化 $\tau_{step} = \left(\tau_{max} - \tau_{min}\right)/P$，P 是一個自訂變數。
- 空間補充(Spaces augmentation)：由於投影空間的維度不能隨意增加，

所以使用 K 倍的投影空間來為每個使用者生成更長的生物碼，K 為一自訂變數。

- 特徵輪換(Features permutation)：另一種產生更長的生物碼而不需使用更多投影空間的方法是在投影計算時，輪換特徵向量裡的特徵係數。

如果上述所有的四種方式均被採用，將極大的增加生物碼的長度。並將最後的結果以漢明距離進行比較。他們的研究顯示當亂數 Token 被竊取時，基礎的生物雜湊演算和改善後的生物雜湊演算的效能相比，分別在 FVC2002 DB2 Databases 得到的結果為 15.0 以及 6.8(EER in %)。

另外 Belguechi 等人[26]測試了生物碼(Biocode)在 128 位元、256 位元、512 位元三種不同長度的情況下，對於各種攻擊的驗證錯誤率。實驗結果顯示當生物碼長度為 128 位元時，最有效的攻擊也是竊取 Token，有 0.28%的攻擊成功率；其次是暴力破解和竊取原始生物特徵模板，僅有 0.14%的攻擊成功率。而在長度 256 位元和 512 位元的情況下，將沒有任何攻擊可以成功通過辨識。這些研究證明了生物碼的長度是生物特徵雜湊演算強度的重要因素，因此本研究所使用的生物碼長度為 256 位元。

另外考慮到生物雜湊演算用於不同指紋提取技術的效能 Nanni 等人[17]的研究指出生物雜湊演算用於指紋的細節描述(Orientation-based minutia descriptor)的指紋模板比對上有著不錯的效能。細節描述的指紋模板是由指紋細節點提取方法(Minutiae points extraction)所產生的生物特徵模板。該方法是一種用於指紋特徵提取和比對的技術。它的優點在於指紋紋理方向的局部細節結構描述不隨旋轉和平移而變化。而在 Nanni 等人[17]的研究結果顯當使用 FVC2002 DB2 databases 進行測試時，分別在一般情況與最差的情況下(當 Token 被竊取時)得到的 EER 值為 1.81%以及 3.45%。

而之後 Nanni 等人的研究[27]中基於他們先前的研究[17]的基礎上，提出使用改善的生物雜湊演算方法，來完善的先前提出指紋辨識系統，其結果顯示當使用 FVC2002 databases 進行測試時，分別在一般情況與最差的情況下(當 Token 被竊取時)所得到的 EER 數值為 0%以及 2.42%。而本篇所提出的多重指紋辨識系統方法

是基於使用改進的生物雜湊演算[17]和[27]所使用的指紋提取技術的認證架構，並且依據之前的分析並控制計算成本的前提下，我們將預設生物碼(Biocode)的長度為 256 位元。需要注意到的是儘管透過生物雜湊演算所產生的生物碼(Biocode)是經過壓縮過的生物辨識資訊，但世界的人口總數介於 2^{32} 到 2^{33} 之間，而 256 位元長度的生物碼(Biocode)的可能性卻是 2^{256} 種之多，所以其雜湊碰撞(Collision)的可能性將微乎其微(因為非一般情況下雜湊函式的輸入和輸出有可能不是唯一的映射關係這種情況稱為「雜湊碰撞」)，因此資料量足以表示不同使用者之間的不同指紋特徵。

第五節 遠端使用者身份認證方法探討

我們回顧最近在雲端服務使用智慧卡認證的相關研究，在 2012 年，An[28]提出了使用智慧卡的基於生物識別的遠端使用者認證方法的改進，An 提出了一種增強的 Das 方法[29]，不僅可以承受各種攻擊，還可以在使用者和伺服器之間提供相互認證，並聲稱該方法對使用者假冒攻擊，伺服器假冒攻擊等是安全的。然而，Khan 與 Kumari[1]分析了 An 的認證方法的安全性，並表明該方法存在致命缺陷所以容易受到惡意攻擊，並且不能在使用者和伺服器之間提供相互認證。為了解決上述在 An 方法中所發現的安全缺陷，Khan 與 Kumari 提出了一種新的方法，並聲稱即使將智慧卡中存儲的秘密資訊暴露給攻擊者，新方法也是安全的。因此 Khan 與 Kumari 的方法非常有吸引力。不幸的是，Wen 等人[30]指出這個說法是錯誤的，Khan 與 Kumari 的方法無法承受各種攻擊如：離線密碼猜測攻擊、假冒襲擊、伺服器假冒攻擊等。

從上述的文獻探討中可以發現，採用密碼的使用者認證方法不免因為密碼本身存在的缺陷導致潛在的安全議題，並且難以透過增強和修改等方式彌補認證方法中存在的缺漏，所以本研究提出基於使用多重有序指紋模板取代單一指紋模板與使用者密碼的認證技術來改善上述之問題。與單一指紋模板相比，多重指紋模板具有排列的特性，須依正確的指紋輸入順序才可通過認證且相同的指紋資訊可重複輸入。此外從指紋資訊可能遭受洩漏的角度來看，要透過非法的方式盜取或複製多個使用者指紋的難度明顯的要比盜取或複製單一指紋要來的高出許多。更進一步與使用密碼相比，密碼需要依靠長度才得以保證其安全強度，但是過長的密碼卻

又難以記憶，然而使用有序的指紋只需記憶輸入的指紋序列之順序，其記憶難度將大大降低並產生高度複雜且安全的認證因子。例如當設定的指紋模板數是 6 時，其可能性便有 10^6 種的排列組合，但這邊我們需要強調的是這 10^6 種不同的序列全是使用者的指紋模板所構成，而跟密碼不同的是，生物特徵資訊難以窺視、幾乎無法複製、不能隨意共享轉發以及難以透過數位攻擊破壞。最後透過多重並有序的指紋模板還可以增加生物辨識系統的精度，與單一指紋模板相比，使用多重指紋模板資訊進行認證時，能有效降低錯誤接受率(FAR)。

第六節 指紋感測器

對於生物特徵識別技術來說，演算法和感應器皆是核心要素，所以指紋辨識器由軟體與硬體共同構成，硬體部分是指紋感應器(Fingerprint Sensor)，用於採集指紋，依照技術可分光學式(Optical)與電容式(Capacity)兩種，並依照掃瞄方式可分成滑動式與按壓式。

光學式的設計早於電容式，是透過光線讓指紋的紋路細節顯現出來。最早的光學式設計的基本架構是靠著光源、三稜鏡以及感光元件透過光源反射讓隆起線顯現出來，再透過感光元件擷取影像便能擷取指紋資訊。因為光學式設計手指接觸的是三稜鏡或是其它反射面，而非電容式昂貴的感應晶片，因此優點在於解析度高，影像取得快、不受電流穩定度影響、實例驗證數多、耐用度較高且成本低廉，但缺點在於體積大且耗電，此外光學辨識只能到達皮膚的表皮層，而不能到達真皮層，因此受手指表面是否乾淨影響較大。對於需大批量使用的機場等地，大多為光學式設計，例如美國海關。

而電容式則是透過手指的電荷變化、溫度差、壓力等方式掃瞄指紋紋路，也稱為半導體式、矽晶式等名稱。薄與小是電容式設計的優點。但成本相較於光學式設計更高，且裸露的感應器容易受到汗水等外在因素影響，導致耐用度較差因此電容感測器對手指的乾淨要求還是比較高，而且感測器表面使用矽材料，比較容易損壞。電容式指紋感測器也是現在應用最普遍的技術。現在電容感測器發展而來的生物射頻技術，更是大大改善了用戶的體驗。射頻感測器通過感測器發射微量的射頻信號，穿透手指的表皮層獲取裡層的紋路以獲取資訊。這種方法對手指的乾淨程度要

求較低。圖 2-4 與圖 2-5 分別顯示了光學式指紋感應器和電容式指紋感應器的原理。

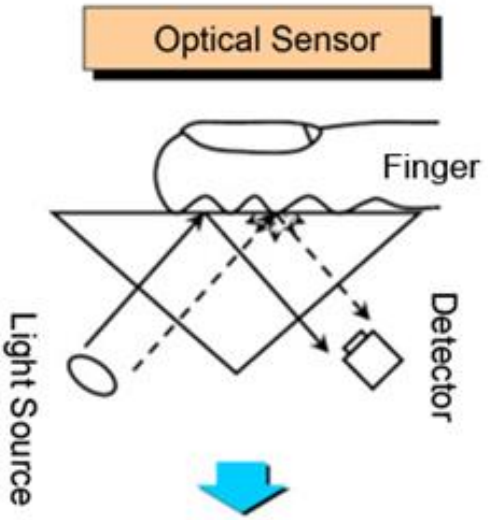

圖 2-4. 光學式指紋感測器[31]

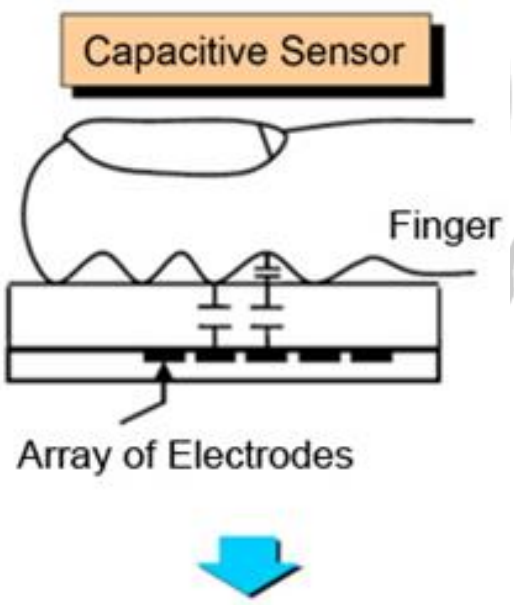

圖 2-5. 電容式指紋感測器[31]

而在最近高通（Qualcomm）於 MWC 2015 世界通訊展中發表「Snapdragon Sense ID」3D 超音波指紋辨識技術[32]。該技術與目前市面上常見的電容觸摸式指紋辨識技術不同，主要是透過超音波技術進行指紋掃瞄，技術原理是利用聲波直接穿透皮膚的外層，檢測手指 3D 細節和包括指紋脊和汗毛孔等獨特的指紋特徵，

建立難以模仿的指紋認證資訊。高通方面表示，Snapdragon Sense ID 技術能使用在玻璃、鋁、不銹鋼、藍寶石和塑膠材質的機身上，並且不會因為手上的髒污、汗水或清潔劑等干擾影響掃瞄結果。因此有效針對短時間擷取多個指紋辨識資訊，因而相關的指紋辨識技術將逐漸支持短時間重複掃描多個指紋資訊。

第三章 使用多重指紋序列的遠端認證方法

第一節 回顧 Khan 與 Kumari 的方法

在這個章節我們重新探討 Khan 與 Kumari 的認證方法[1]，其認證方法是改進 An 的認證結構。該方法由來自三方的參與者組成，使用者(U_i)，伺服器(S)和註冊中心(R)，其中 R 被認為是公正的可信方。在此節裡我們著重於 Khan 與 Kumari 的認證方法中的註冊階段、登錄階段以及認證階段，每階段的細節將在以下小節中詳細介紹。下表 3-1 為 Khan 與 Kumari 的方法中所使用的符號及其解釋。

表 3-1. Khan 與 Kumari 的方法中使用的符號表

符號	解釋
U_i	使用者 i
SC_i	使用者 i 的智慧卡
ID_i	使用者 i 的帳戶號碼
PW_i	使用者 i 的密碼
B_i	使用者 i 的生物辨識模板
n_i	使用者 i 於註冊過程中所選擇的隨機數
R	註冊中心
S	伺服器
x, y	註冊中心所持有的秘鑰
h(・)	一般單向雜湊演算

一、註冊階段

首先使用者 U_i 將他/她的智慧卡 SC_i 插入讀卡機中，接著使用者 Ui 首先選擇一個隨機數 n_i 並透過安全的通訊頻道傳送註冊資訊$\{ID_i, PW_i \oplus n_i, B_i \oplus n_i\}$至 R。當 R 收到來至 U_i 的註冊請求訊息後，依據 U_i 所傳送的註冊資訊產生出 $f_i = h(B_i \oplus n_i)$，$r_i = h(PW_i \oplus n_i) \oplus f_i$，$c_i = h(x \| y) \oplus f_i$ 和 $e_i = h(ID_i \| x) \oplus r_i$，並把產生出的參數 c_i，e_i 以及 h(・)存入 U_i 的 SC_i 中，並透過安全的通訊頻道傳送 f_i 至 U_i，其中 h(・)表示單向雜湊演算。當 U_i 收到 f_i 後，接著計算 $g_i = (ID_i \| PW_i) \oplus f_i$，$j_i = (ID_i \| PW_i) \oplus n_i$ 並將剛產生的 g_i 以及 j_i 存儲到 SC_i 中。所以現在 $SC_i = \{c_i, e_i, g_i, j_i, h(\cdot)\}$。

二、登入階段

當 U_i 請求登入 S 時，U_i 必須執行以下步驟：

● Step1 ：首先使用者 U_i 將他/她的智慧卡 SC_i 插入讀卡機中，並輸入使用者的 ID_i、PW_i 以及生物辨識資訊。

● Step2 ：之後從 SC_i 中讀出 g_i 以及 j_i 並透過運算 $f_i^* = (ID_i \| PW_i^*) \oplus g_i$ 和 $n_i^* = (ID_i \| PW_i^*) \oplus j_i$。當得到參數 f_i^* 以及 n_i^* 後，系統接著運算 $h(B_i \oplus n_i^*)$ 並把其結果與之前得到的 f_i^* 相比較是否相等，如果不相等則系統終止此次登入請求；如果相等，則 U_i 通過使用者生物辨識認證，接著 U_i 產生隨機數 R_i 並進行以下計算：

$$r_i = h(PW_i \oplus n_i) \oplus f_i,$$

$$T_1 = c_i \oplus f_i,$$

$$T_2 = e_i \oplus r_i,$$

$$T_3 = T_1 \oplus Ri,$$

$$T_4 = h(T_1 \| R_i) \oplus ID_i,$$

$$T_5 = h(T_2 \| R_i).$$

其中 R_i 是 U_i 生成的隨機數。

● Step3 ：隨後 U_i 送出登入請求資訊 $\{T_3, T_4, T_5\}$ 給 S。

三、認證階段

當 S 接收來自 U_i 的登入請求訊息 $\{T_3, T_4, T_5\}$ 後， U_i 與 S 為了進行相互認證將執行以下步驟：

● Step1 ：S 計算 $T_6 = h(x \| y)$，$T_7 = T_3 \oplus T_6$ 以及 $ID_i = T_4 \oplus (T_6 \| T_7)$。

● Step2 ：S 檢查 ID_i 的格式，如果它合法，則 S 計算 $T_8 = h(ID_i \| x)$ 並產生 $h(T_8 \| T_7)$ 並把其結果與之前得到的 T_5 相比較是否相等，如果不相等則 S 拒絕此次 U_i 的登入請求；如果相等則 S 產生隨機數 R_s 並計算 $T_9 = T_8 \oplus R_s$ 和 $T_{10} = h(T_8 \|$

R_s)。之後 S 送出回應訊息{T_9，T_{10}}給 U_i。

● Step3 ：當 U_i 收到來自 S 傳送的回復資訊{T_9，T_{10}}後，Ui 接著計算 $T_{11} = T_9 \oplus T_2$ 之後產生 $h(T_2 \| T_{11})$並把其結果與之前得到的 T_{10} 相比較是否相等，如果不相等則 U_i 終止此次的登入請求；如果不相等則 U_i 接著計算 $T_{12} = h(T_2 \| R_i \| T_{11})$，並將訊息{$T_{12}$}發送至 S。

● Step4 ：S 在接收到訊息{T_{12}}之後，S 產生 $h(T_8 \| T_7 \| Rs)$並把其結果與之前收到的 T_{12} 相比，如果不相等，則 S 拒絕 U_i 的登錄請求；如果相等，則 S 接受使用者此次的登錄請求。

四、Khan 與 Kumari 的方法的安全性分析

在以下的小節我們將分析 Khan 與 Kumari 所提出的方法並提出在特定的條件假設下分析他們的方法所可能存在的安全問題。

(一)、條件假設

在此小段中我們將假設並假設攻擊者可以通過監視功耗[28][33]獲取存儲在智慧卡中的秘密值，並攔截使用者與伺服器之間的通訊。

透過觀察電力的功耗[34][35]能得到一筆能量紀錄，便可間接地取得硬體在運作時所洩漏出的秘密資訊，而非使用一般暴力破解方式，因此又常稱之為能量攻擊(Power attack)或旁道攻擊(Side channel attack)。通常不特別說明時，能量攻擊的攻擊對象便是指智慧卡。

而能量攻擊又依不同的特性又分為簡單能量攻擊(Simple power attack)以及差分能量攻擊(Different power attack)，兩者分別說明如下。

(1) 簡單能量攻擊(Simple power attack)：

因硬體在進行不同的運算時會產生不同的能量消耗波形，所以當攻擊者知道硬體實作細節，且可以收集到一筆能量紀錄時，攻擊者便可以依此能量消耗波形得到一組連續的運算過程，再對照相對應的演算法即可推測出金鑰。如圖 3-1 為一筆能量紀錄的示意圖，其中橫軸表示時間，縱軸表示所消耗的能量。

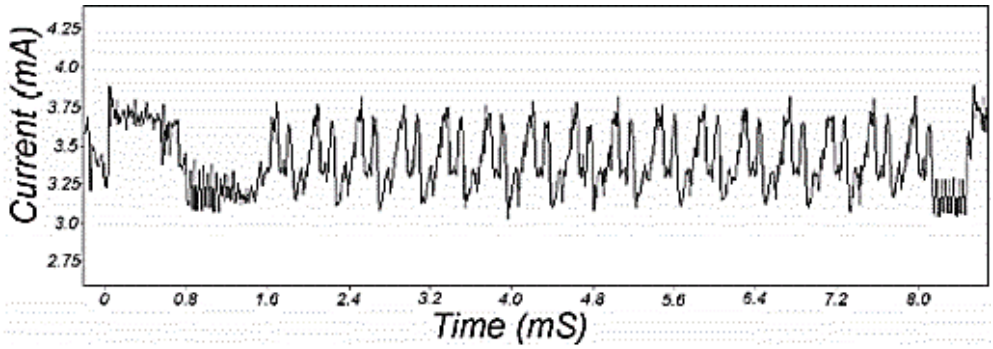

圖 3-1. 能量紀錄示意圖[23]

(2) 差分能量攻擊(Different power attack)：

攻擊者在知道密碼系統演算法的狀況下，就可事先猜測金鑰一部分的值，以其值來推算出某輸入在運算到某一步驟時期當時的值應該是多少，然後再依此數值對該輸入的能量紀錄來進行不同的分類。若猜測的金鑰是正確的，則不同分類的能量紀錄會顯現出預期的統計性質；如果所猜測金鑰是不正確的，則不會出現預期的統計性質，因此攻擊者可以判斷所猜測的金鑰是否正確。如圖 3-2 為使用差分能量攻擊法的能量示意圖，若是所猜測的值是正確的話，波形將會有明顯變化。

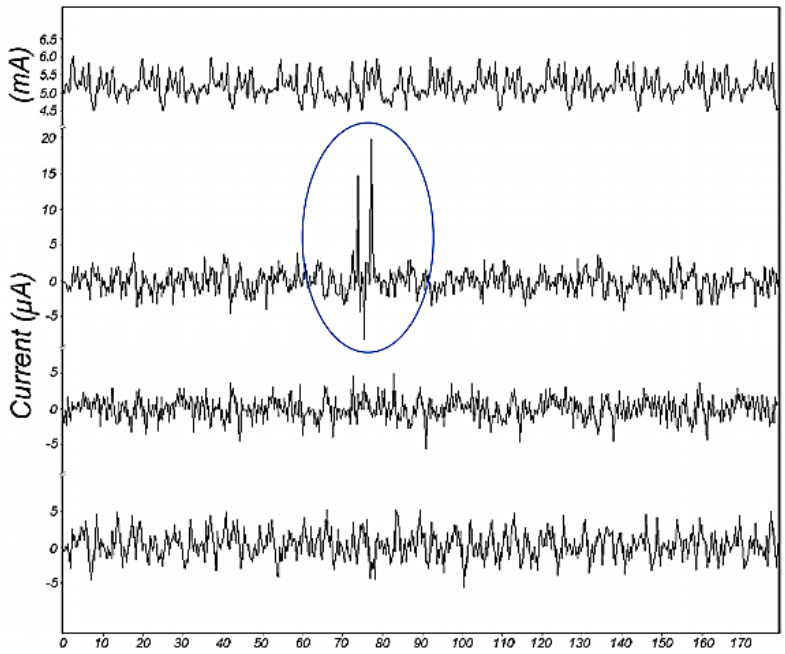

圖 3-2. 差分能量攻擊法的能量示意圖[33]

此外在安全性分析中我們將假設擊者可能擁有以下這些能力破解安全方法[25]：

A. 攻擊者在登錄和驗證階段對使用者和伺服器之間的通訊通道進行完全控制。那就是攻擊者可能跨通訊過程攔截、插入、刪除或修改任何訊息。

B. 攻擊者可能（i）竊取使用者的智慧卡，然後提取存儲在智慧卡中的秘密值,(ii)或竊取使用者密碼,但不能同時假設攻擊者可以達成(i)和（ii)。

顯然,如果使用者的智慧卡和密碼都被同時盜用,則無法防止攻擊者假冒使用者。因此，如果（i）和（ii）中只有一個事件發生，遠端使用者認證方法應該是安全的。

(二)、認證方法的安全性分析

在此小段中，我們基於上段的條件假設下，將逐步分析 Khan 與 Kumari 的方法中存在的安全問題[30]。

(1) 線上密碼猜測攻擊(Online password guessing attack)：如果存有惡意的使用者 A 透過能量分析等攻擊擷取存在於自己智慧卡中的秘密資訊{c_A，e_A，g_A，j_A，h(・)}便可以從這些祕密參數進行逆向演算得出 h(x || y)，並再次透過能量分析等攻擊擷取其他使用者 U_i 的智慧卡中的秘密資訊{c_i，e_i，g_i，j_i，h(・)}，接著利用之前所得到的關鍵參數 h(x || y)接著運算 $c_i \oplus$h(x || y)得到 f_i 以及運算 $g_i \oplus (ID_i || PW_i^*)$得到 f_A^*，其中 PW_i^*是攻擊者 A 所猜測的密碼。接著並檢查是否 f_i 與 f_A^*相等，如果相等則成功猜出使用者 U_i 所設定的密碼；如果不相等則重複密碼猜測運算 $g_i \oplus (ID_i || PW_i^*)$直到所運算出的 f_A^*與 f_i 相等。

(2) 使用者假冒襲擊(User impersonation attack)：在攻擊者 A 得到使用者 U_i 的 ID_i和 PW_i後，便可以進一步假冒使用者 U_i 與伺服器 S 進行認證通訊。在攻擊者 A 利用從使用者 U_i 得到的秘密參數{c_i，e_i，g_i，j_i，h(・)}運算 $n_i = j_i \oplus (ID_i || PW_i)$、$f_i = g_i \oplus (ID_i || PW_i)$、$r_i = h(PW_i \oplus n_i) \oplus f_i$，以及 $h(ID_i || x) = e_i \oplus r_i$。接著自己產生出一個隨機數 R_A 並運算出登入請求資訊 $T_3^* = h(x || y) \oplus R_A$、$T_4^* = (h(x || y) \oplus R_A) \oplus ID_i$ 以及 $T_5^* = h(h(ID_i || x) \oplus R_A)$，之後便可以

向伺服器 S 傳送登入請求資訊{T_3^*，T_4^*，T_5^*}。我們可以很容易的發現伺服器 S 會接受來自攻擊者 A 的登入請求並接續之後的認證通訊。

(3) 伺服器假冒襲擊(Server impersonation attack)：在先前的攻擊分析中我們發現攻擊者不僅可能可以得到使用者 U_i 智慧卡中的秘密資訊並逆向演算得關鍵參數 $h(x \| y)$外，還可能透過這些關鍵參數猜測出 U_i 的 PW_i 和 $h(ID_i \| x)$。接著攻擊者 A 便可以利用這些獲得的資訊與使用者 U_i 進行相互認證。利用運算 $T_9= h(ID_i \| x) \oplus R_A$ 以及 $T_{10}=h(h(ID_i \| x) \| R_A)$，其中 R_A 為攻擊者 A 所產生的隨機數。之後送出回覆訊息{T9，T10}。我們可以從上述的假設和分析中看出攻擊者 A 可以很輕易的假冒伺服器 S 並欺騙 U_i。

(4) 相互認證(Mutual authentication)：根據上述的分析，如果使用者 U_i 的智慧卡遺失或被竊取，則攻擊者 A 可以輕易地透過攻擊(2)猜出使用者 U_i 的 PW_i 和 $h(ID_i \| x)$。此外並利用攻擊(2)與(3)並可以執行使用者假冒攻擊和伺服器假冒攻擊。因此，Khan 與 Kumari 的方法無法提供相互驗證。

第二節 本文所提出的方法

在本節中將介紹我們所提出的結合智慧卡和可取消式的指紋模板序列辨識雲端認證方法使用了哪些技術、如何運作以及針對我們所提出的方法進行安全性分析，本篇論文將以 Khan 與 Kumari 的方法[1]為基礎，通過提出改進的使用者認證方法來消除他們方法的弱點。我們的方法共分為四個階段：註冊、登入、認證階段以及使用者指紋模板序列變更階段。該方法由來自三方的參與者組成：使用者(U_i)、伺服器(S)和註冊中心(R)，其中 R 被認為是公正的可信方。在本篇所提出的方法中，使用者於剛開始註冊時會先輸入 $1<M\leq N$ 的指紋個數所串成的指紋模板序列，其中 M 是使用者所輸入的指紋總數(如：$f_{i(1)} \| f_{i(2)} \| ... \| f_{i(M)}$)所串接而成的使用者指紋特徵模板序列，並且其值一定必須大於 1，因為與單一指紋模板相比，多重指紋模板具有排列的特性，且須依正確的指紋輸入順序才可通過認證且相同的指紋資訊可重複輸入。此外從指紋資訊可能遭受洩漏的可能性來看，要透過非法的方式盜取或複製多個使用者指紋的難度明顯的要比盜取或複製單一指紋要來的高出許多；其中 N 為指紋模板序列總數輸入的最大值，由系統制定，當 N 值越大時可以想見

指紋特徵模板序列將會更複雜，例如當設定的指紋模板數是 6 時，其可能性便有 10^6 種的排列組合，但這邊我們需要強調，這 10^6 種不同的序列全是使用者的指紋模板所構成，而跟密碼不同的是，生物特徵資訊難以窺視、幾乎無法複製、不能隨意共享轉發以及難以透過數位攻擊破壞。此外 R 將持有主密鑰 x，令 $E_K(\cdot)/D_K(\cdot)$ 表示加密函式和解密函式的對稱金鑰加密演算（例如 AES）。我們會在之後的小節中詳細展現出每個階段的過程。我們所提出的方法所使用的符號以及其解釋將列於表 3-2。

表 3-2. 本文方法所使用的符號表

符號	解釋
U_i	使用者 i
SC_i	使用者 i 的智慧卡
ID_i	使用者 i 的帳戶號碼
d_i	偽隨機亂數種子(Seed)，為生物雜湊演算之必要參數，透過隨機亂數種子來產生偽隨機向量集
τ_i	預設閥值，為生物雜湊演算之必要參數，生物雜湊演算將透過隨機亂數種子與預設閥值產生使用者特定之生物碼(Biocode)
$f_{i(k)}$	使用者 i 所輸入的第 k 個指紋特徵模板資訊
n_i	使用者 i 於註冊過程中所選擇的隨機數
c_i	註冊中心為使用者 i 所選擇的隨機數
t	時戳
R	註冊中心
S	伺服器
x	註冊中心所持有的秘鑰
$H_B(\cdot)$	生物雜湊演算函式，燒錄在特別的指紋辨識讀取裝置中
$h(\cdot)$	一般單向雜湊演算
$E_K(\cdot)$	用於加密的對稱加密演算，其中 K 為加密所使用的金鑰
$D_K(\cdot)$	用於解密的對稱加密演算，其中 K 為解密所使用的金鑰

請注意，本篇研究所提出之認證方法中用於保護使用者指紋特徵模板的生物雜湊演算方法所包含的使用者生物雜湊演算所使用到的參數如：為了產生偽隨機向量集所使用的偽隨機亂數種子(Seed)d_i 以及為了生成使用者特定之生物碼(Biocode)所使用的預設閥值τ_i 等資訊也將儲存於使用者的智慧卡中，其中偽隨機亂

數種子(Seed)d_i 與預設閥值τ_i 將由系統分別為使用者產生，並且也都將隨使用者的不同而不同。

一、註冊階段

最初，使用者 U_i 必須至註冊中心 R 註冊申請服務，整個註冊過程可以分為以下幾個步驟：

● Step1 ：首先使用者 U_i 將他/她的智慧卡 SC_i 插入讀卡機中，接著註冊中心 R 依據從智慧卡 SC_i 讀出的使用者 ID_i 後，為使用者產生一個偽隨機亂數種子(Seed)d_i 以及預設閥值(Threshold)τ_i，之後使用者 U_i 透過特別的指紋辨識裝置依序輸入使用者指紋模板序列：$f_{i(1)} \| f_{i(2)} \| \ldots \| f_{i(M)}$，並從指紋特徵輸入的過程中各別擷取出最先輸入的指紋模板資訊 $f_{i(1)}$以及最後輸入的指紋模板資訊 $f_{i(M)}$，隨後使用者 U_i 選擇一個隨機數 n_i，此隨機數 n_i 由使用者 U_i 於註冊時產生且一旦產生後並不改變，此隨機數是用於互斥或演算(XOR)後保護使用者敏感資訊(如使用者指紋模板之生物雜湊演算值或使用者於注冊時所選的隨機數 n_i)，並在之後用於登入時之智慧卡的生物辨識時使用，接著利用先前註冊中心 R 幫使用者 U_i 產生的生物雜湊演算參數：偽隨機亂數種子 d_i 與預設閥值τ_i 並結合生物雜湊演算(Biohashing)並分別計算出 $B_i = H_B(f_{i(1)}) \| H_B(f_{i(2)}) \| \ldots \| H_B(f_{i(M)})$、$b_F = H_B(f_{i(1)})$以及 $b_M = H_B(f_{i(M)})$，並在隨後個別產生出$(B_i \oplus n_i)$、$(b_F \oplus n_i)$以及$(b_M \oplus n_i)$，之後系統把 d_i、τ_i 與$(b_F \oplus n_i)$存入使用者 U_i 的智慧卡 SC_i 中。其中需要注意到的是隨機數 n_i 將不以明碼存入使用者的智慧卡中，所以攻擊者無法單純依靠能量攻擊或旁道攻擊取得 n_i 進行登入請求資訊的逆向演算，因為所有的重要演算都將需要使用到 n_i 詳細的過程將在下列的步驟中展現。

● Step2 ：接著系統選擇一個隨機數 c_i 作為註冊中心 R 為使用者 U_i 所產生的秘密金鑰，接著進行以下計算：

$$j_i = h(x \oplus c_i),$$

$$f_i = h(B_i \oplus n_i \| j_i),$$

$$r_i = h(b_M \oplus n_i) \oplus f_i,$$

$$e_i = h(ID_i \| x) \oplus f_i,$$

$$g_i = (b_M \oplus n_i) \oplus j_i.$$

其中 $h(ID_i \| x)$可以看成是註冊中心核發給使用者的身份憑證，因為只有註冊中心持有秘密值 x，所以只有合法的註冊中心才可以根據使用者 U_i 的 ID_i 產生 $h(ID_i \| x)$; f_i 是當使用者請求登入時用於檢驗使用者的生物辨識資訊的重要參數；$h(b_M \oplus n_i)$是用於與 f_i 進行互斥或演算(XOR)來保護重要資訊 f_i 使得攻擊者無法單純依靠能量攻擊或旁道攻擊取得 f_i。

● Step3 ：之後 R 把先前運算所產生的資訊$\{ID_i, j_i, r_i, e_i, g_i, h(\cdot)\}$存入 SC_i 中。此時使用者的智慧卡將含有$\{ID_i, j_i, r_i, e_i, g_i, h(\cdot), (b_F \oplus n_i), d_i, \tau_i\}$等資訊。圖 3-3 顯示了註冊階的段完整流程。

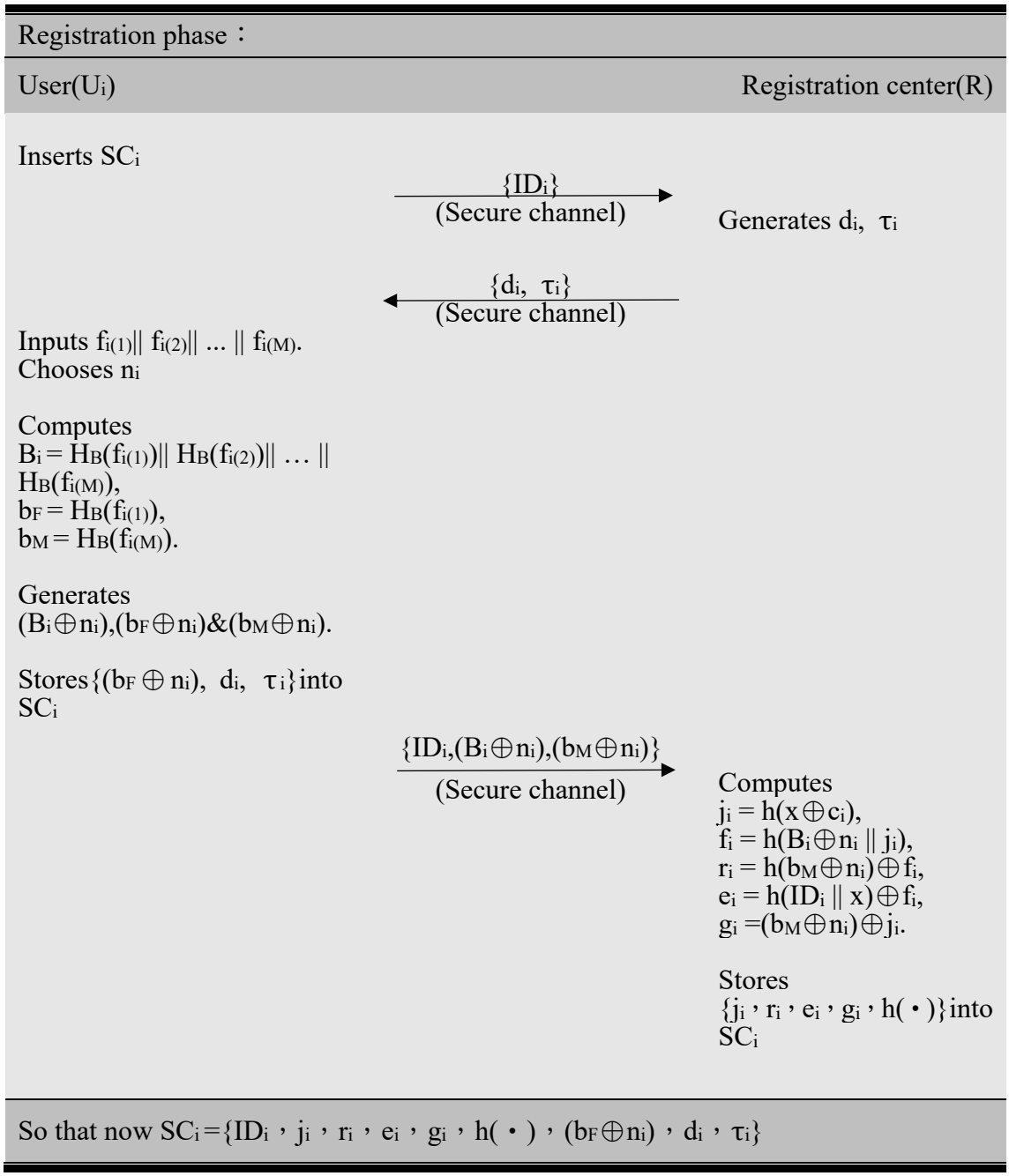

圖 3-3. 註冊階段程序

二、登入階段

當使用者 U_i 請求登入伺服器 S 時，使用者 U_i 必須執行以下步驟：

● Step1 ：首先使用者 U_i 將智慧卡 SC_i 插入讀卡機中，接著透過特別的指紋辨識裝置依序輸入使用者指紋模板序列：$f_{i(1)}|| f_{i(2)}|| ... || f_{i(M)}$，接著從指紋特徵輸入的過程中各別擷取出最先輸入的指紋模板資訊 $f_{i(1)}$以及最後輸入的指紋模板資訊 $f_{i(M)}$，並從使用者 U_i 的智慧卡 SC_i 中分別讀出偽隨機亂數種子 d_i 與預設閥

值τ_i，隨後利用先前讀出的生物雜湊演算參數 d_i 與τ_i 結合生物雜湊演算分別計算出 $B_i = H_B(f_{i(1)})\| H_B(f_{i(2)})\| \ldots \| H_B(f_{i(M)})$、$b_F = H_B(f_{i(1)})$、$b_M = H_B(f_{i(M)})$，並利用之前所獲得的 b_F 進行運算 $b_F \oplus (b_F \oplus n_i)$解出 n_i^*，請注意此 n_i 即為使用者於註冊時所選擇的隨機數並且不會因為之後的認證通訊而改變。

● Step2 ：之後使用者 U_i 的智慧卡 SC_i 透過運算 $b_M \oplus n_i^* \oplus g_i$ 計算出 j_i^*以及運算 $b_M \oplus n_i^* \oplus r_i$ 計算出 f_i^*。接著計算 $h(B_i \oplus n_i^*)$並把其結果與之前得到的 f_i^*相比較是否相等，如果不相等則系統終止此次登入請求；如果相等，則 U_i 通過使用者生物辨識認證。接著使用者產生隨機數 R_i 進行以下計算：

$$T_1 = e_i \oplus f_i(\text{Which is indeed } h(ID_i \| x)),$$

$$T_2 = E_{T_i}(R_i, t_i, j_i),$$

$$T_3 = h(T_1 \| R_i \| t_i \| j_i).$$

其中 t_i 是使用者 U_i 所產生的時戳；R_i 為 U_i 所產生的隨機數，與隨機數 n_i 不同的是 R_i 不是一個固定值，它是依照每次的使用者登入請求時產生，所以其值每次都不相同且僅用於該次登入請求通訊中所使用，同時也作為使用者的身份證明與會議密鑰；T_1 是用於對稱加密演算所使用的加密金鑰與解密金鑰；T_2 為使用對稱加密演算保護的一段訊息，其加密與解密的金鑰均為 T_1，只有同樣能產生解密金鑰的伺服器 S 才能解開其中的隱藏訊息，因此確保了通訊過程中資訊被攻擊者所攔截並解讀出其中的私密資訊；T_3 是用於驗證從 T_2 所解開的秘密資訊是否合法正確，因為 T_3 是由 T_2 中所含有的參數所運算出的雜湊值，因此只有合法的使用者 U_i 才可以透過所擁有的關鍵資訊(如 R_i 以及 j_i)與加密金鑰同時產生出 T_2 與 T_3。

三、認證階段

當 S 接收來自 U_i 的登入請求訊息$\{ID_i, T_2, T_3\}$後，U_i 與 S 為了驗證彼此身份將執行以下步驟：

● Step1 ：伺服器 S 接著計算下列數值：

$$KU_i = h(ID_i \| x),$$

$$(R_i^*, t_i^*, j_i^*) = D_{KUi}(T_2).$$

其中 KU_i 是伺服器 S 所產生的解密金鑰，用於解開來自使用者 U_i 所產生的加密訊息 T_2，同時也能確保發出登入請求訊息的來源端身份，因為只有合法的使用者 U_i 才會擁有該加密金鑰，此加密金鑰就是使用者 U_i 於註冊時由註冊中心 R 核發給使用者 U_i 的身份憑證。

● Step2 ：當伺服器 S 透過自己所產生的解密金鑰 KU_i 解開來自使用者 U_i 的加密訊息 T_2 後，第一步先驗證 t_i 的合法性，如果不合法則終止此次使用者登入請求;如果相等則接著計算 $h(KU_i \| R_i^* \| t_i^* \| j_i^*)$並把其結果與之前得到的 T_3 相比較是否相等，如果不相等則 S 拒絕此次使用者 U_i 的登入請求；如果相等則伺服器 S 產生隨機數 R_s 並接著計算下列數值：

$$T_4 = E_{KUi}(R_i, R_s, t_s),$$

$$T_5 = h(KU_i \| ID_i \| R_i \| R_s \| j_i \| t_s).$$

之後伺服器 S 送出回應訊息{T_4，T_5}給 U_i。其中 T_4 為伺服器 S 使用加密金鑰 KU_i 所加密的一段訊息，只有同樣擁有相同金鑰 T_1 的使用者 U_i 才能解密因此可以驗證伺服器 S 身份的合法性；T_5 是用於驗證從 T_4 所解開的加密資訊是否合法正確，因為 T_5 是由 T_4 中所含有的參數所運算出的雜湊值，因此只有合法的伺服器 S 才可以透過所擁有的關鍵資訊(如 R_i 以及 R_s)與加密金鑰同時產生出 T_4 與 T_5；R_s 為伺服器 S 所選擇的隨機數，與隨機數 R_i 相同 R_s 不是一個固定值，它是依照每次收到來自使用者所送出的登入請求時產生，所以其值每次都不相同且僅用於該次登入請求通訊中所使用，同時也作為伺服器的身份證明與會議密鑰；t_s 為 S 所產生的時戳。

● Step3 ：當 U_i 收到來自 S 傳送的回復資訊{T_4，T_5}後，U_i 接著運算 $D_{Ti}(T_4)$解密出(R_i^*, R_s^*, t_s^*)，接著驗證 t_s 的合法性，如果不合法則終止此次通訊;如果合法則繼續計算 $h(T_1 \| ID_i \| R_i^* \| R_s^* \| j_i \| t_s^*)$並和之前收到的 T_5 比較兩者是否相等，如果不相等則終止此次登入請求通訊；如果兩者相等則 U_i 接著設定 $SK=h(R_i$

$\| R_s$)。其中 SK 作為與 S 分享的會議密鑰，用於此次登入請求驗證通過後使用者 U_i 與伺服器 S 彼此間的通訊密鑰。其中 T_1、R_i^*以及 j_i 只有合法的伺服器 S 與合法的使用者 U_i 才會知道，因為 T_1 其實與 KU_i 相等是只有註冊中心 R 與伺服器 S_i 才會知道的祕密金鑰；R_i^*以及 j_i 是從合法的使用者 U_i 的加密訊息中所獲得，同樣也只有合法的伺服器才能成功解開加密訊息並獲得 R_i^*與 j_i，因此 T_1、R_i^*以及 j_i 將可證明伺服器的合法性，其後透過使用者 U_i 與伺服器 S 此次認證通訊中相互分享的關鍵資訊 R_i 與 R_s 作為互斥或演算(XOR)的密鑰，用來保護之後所傳遞的每個資訊，因此只有同樣擁有密鑰 R_i 與 R_s 的合法使用者 U_i 與合法伺服器 S 才能成功的還原並解讀彼此所傳遞的訊息。如圖 3-4 顯示了登入以及認證階段的詳細過程。

Login and authentication phase：		
User(U_i)/Smart card(SC_i)		Server(S)
Inserts SC_i. Inputs $f_{i(1)} \| f_{i(2)} \| \ldots \| f_{i(M)}$. Reads d_i, τ_i Computes $B_i = H_B(f_{i(1)}) \| H_B(f_{i(2)}) \| \ldots \| H_B(f_{i(M)})$, $b_F = H_B(f_{i(1)})$, $b_M = H_B(f_{i(M)})$. Generates $n_i^* = b_F \oplus (b_F \oplus n_i)$. Computes $j_i^* \leftarrow b_M \oplus n_i^* \oplus g_i$, $f_i^* \leftarrow b_M \oplus n_i^* \oplus r_i$. Checks if $h(B_i \oplus n_i^* \| j_i^*) = f_i^*$? If they are equal, select a random nonce R_i, and computes $T_1 = e_i \oplus f_i$, $T_2 = E_{T1}(R_i, t_i, j_i)$, $T_3 = h(T_1 \| R_i \| t_i \| j_i)$.	$\{ID_i, T_2, T_3\}$ (Insecure channel)	Computes $KU_i = h(ID_i \| x)$, $(R_i^*, t_i^*, j_i^*) = D_{KUi}(T_2)$. Checks the validity of t_i. If it is valid, and checks if $h(T_1 \| R_i^* \| t_i^* \| j_i^*) = T_3$? If they are equal, select a random nonce R_s, and computes $T_4 = E_{KUi}(R_i, R_s, t_s)$, $T_5 = h(KU_i \| ID_i \| R_i \| R_s \| j_i \| t_s)$.
Computes $(R_i^*, R_s^*, t_s^*) = D_{T1}(T_4)$. Checks the validity of t_s. If it is valid, and checks if $h(KU_i \| ID_i \| R_i^* \| R_s^* \| j_i \| t_s^*) = T_5$? If they are equal, sets $SK = h(R_i \| R_s)$ as the Session key shared with S.	$\{T_4, T_5\}$ (Insecure channel)	

圖 3-4. 登入與驗證階段程序

四、指紋模板序列變更階段

U_i 將 SC_i 插入讀卡機中，接著透過特別的指紋辨識裝置依序輸入使用者指紋模板序列：$f_{i(1)}^{old} \| f_{i(2)}^{old} \| \ldots \| f_{i(M)}^{old}$，並從指紋特徵輸入的過程中各別擷取出最先輸入的指紋模板資訊 $f_{i(1)}^{old}$ 以及最後輸入的指紋模板資訊 $f_{i(M)}^{old}$，接著進行以下步驟：

● Step1 ：系統從使用者 Ui 的智慧卡 SC_i 中分別讀出生物雜湊演算參數 d_i 與 τ_i，隨後利用先前讀出的參數 d_i 與 τ_i 並運用生物雜湊演算分別計算出 $B_i^{old} = H_B(f_{i(1)}^{old}) \| H_B(f_{i(2)}^{old}) \| \ldots \| H_B(f_{i(M)}^{old})$、$b_F^{old} = H_B(f_{i(1)}^{old})$與 $b_M^{old} = H_B(f_{i(M)}^{old})$，並利用之前所獲得的 b_F^{old} 進行運算 $b_F^{old} \oplus (b_F^{old} \oplus n_i)$解出 n_i，請注意此 n_i 即為使用者於註冊時所選擇的隨機數，並且不會隨著使用者的指紋模板序列更改而改變。

● Step2 ：之後系統透過運算 $b_M^{old} \oplus n_i \oplus g_i^{old}$ 計算出 j_i^* 以及運算 $b_M^{old} \oplus n_i \oplus r_i^{old}$ 計算出 f_i^{*old}。接著計算 $h(B_i^{old} \oplus n_i^* \| j_i)$並把其結果與之前得到的 f_i^{*old} 相比較是否相等，如果不相等則系統終止此次變更指紋模板序列之請求；如果相等，則 U_i 通過使用者身份認證，並依照系統提示輸入新的使用者指紋模板序列：$f_{i(1)}^{new} \| f_{i(2)}^{new} \| \ldots \| f_{i(M)}^{new}$，並從指紋特徵輸入的過程中各別擷取出最先輸入的指紋模板資訊 $f_{i(1)}^{new}$ 以及最後輸入的指紋模板資訊 $f_{i(M)}^{new}$ 並計算 $B_i^{new} = H_B(f_{i(1)}^{new}) \| H_B(f_{i(2)}^{new}) \| \ldots \| H_B(f_{i(M)}^{new})$、$b_F^{new} = H_B(f_{i(1)}^{new})$與 $b_M^{new} = H_B(f_{i(M)}^{new})$，之後透過先前運算獲得的 b_F^{new} 產生出$(b_F^{new} \oplus n_i)$以及$(b_F^{new} \oplus b_M^{new})$。並在隨後進行以下 SC_i 參數更新計算：

$$f_i^{new} = h(B_i^{new} \oplus n_i),$$

$$r_i^{new} = h(b_M^{new} \oplus n_i) \oplus f_i^{new},$$

$$e_i^{new} = h(ID_i \| x) \oplus f_i^{new},$$

$$g_i^{new} = (b_M^{new} \oplus n_i) \oplus j_i^{new}.$$

之後系統把更新的參數$\{r_i^{new}$，e_i^{new}，g_i^{new}，j_i^{new}，$(b_F^{new} \oplus n_i)\}$存回 SC_i 中。如圖 3-5 顯示了指紋模板序列變更階段的完整過程。

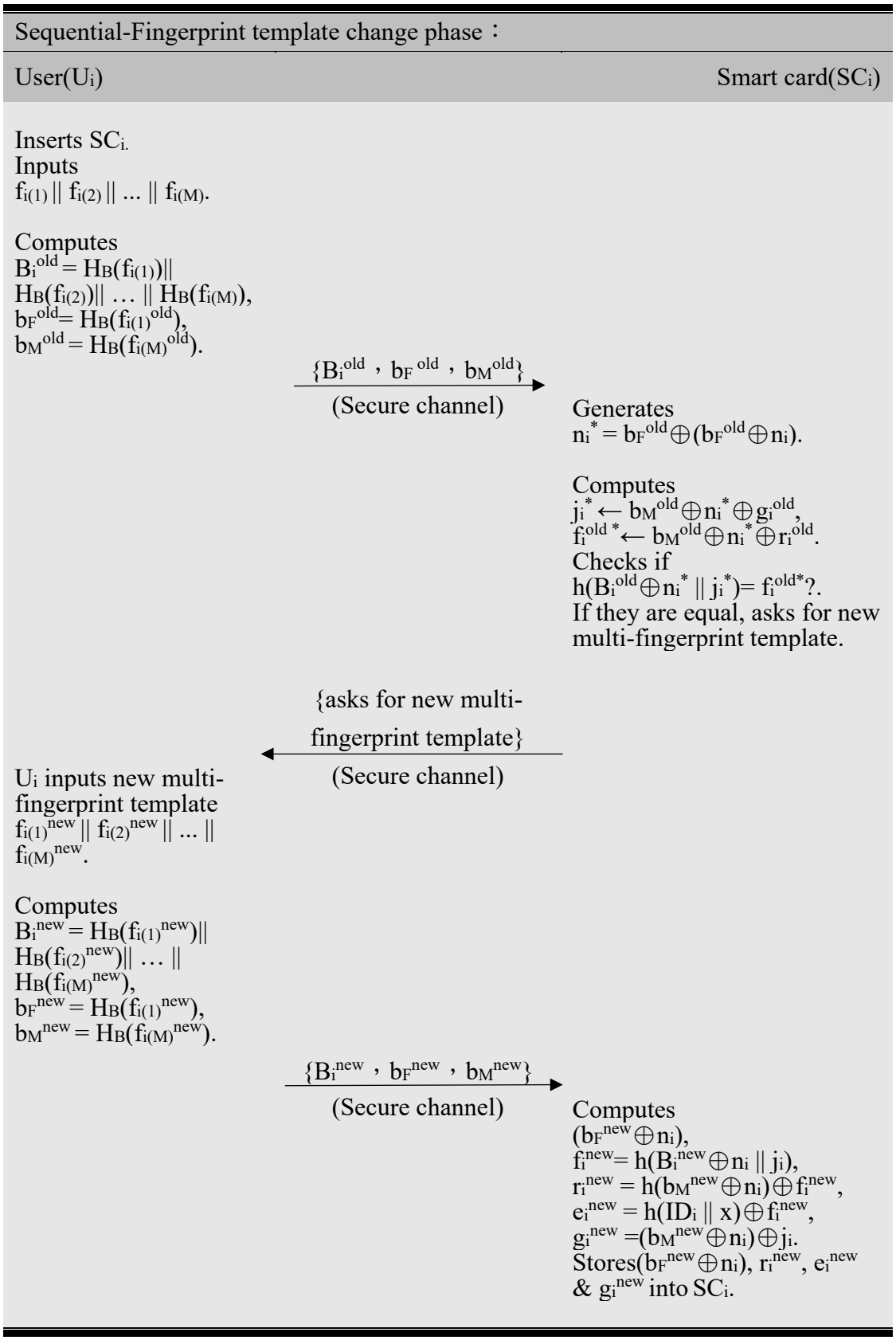

圖 3-5. 指紋模板序列變更階段程序

五、安全性分析

在此小節中將討論本文所提出之認證方法的安全性分析。我們將根據第參節裡的第四小段中的安全分析所提及的條件假設，我們同樣假設攻擊者能使用能量攻擊(Power Attack)或旁道攻擊(Side Channel Attack)破解使用者智慧卡中所儲存的秘密值，並且同樣假設攻擊者能在登錄和驗證階段對使用者和伺服器之間的通訊通道進行完全控制例如：通訊過程攔截、插入、刪除或修改任何訊息等等，並在最後分析顯示本文所提之方法可以有效抵抗密碼猜測攻擊、使用者或伺服器假冒襲擊、支持相互認證以及抵抗指紋模板盜取攻擊。

(1) 線上密碼猜測攻擊(Online password guessing attack)：我們假設，存有惡意的攻擊者 A_i，有辦法取得儲存在 U_i 的 SC_i 中的秘密資訊{ID_i，j_i，r_i，e_i，g_i，$h(\cdot)$，S_i，τ_i，$(b_F \oplus n_i)$}，然而在本研究所提出的協定中並不使用密碼，此外攻擊者 A_i 無法從上述所得到的秘密資訊獨立產生出登入請求訊息，因為要計算 $B_i \oplus n_i$ 攻擊者 A_i 並須先取得 n_i，然而攻擊者 A_i 並無法單獨產生出 n_i 因為攻擊者 A_i 並沒有使用者 U_i 的指紋 b_F，所以無法透過運算 $b_F \oplus (b_F \oplus n_i)$解出 n_i。

(2) 離線密碼猜測攻擊(Offline password guessing attack)：承上所述，在本研究所提出的協定中並不使用密碼，此外所有存於 SC_i 中的資訊都無法透過彼此互相做互斥或的運算得出其中的關鍵登入資訊因為要進行所有的認證運算以前需要先得到 n_i，然而攻擊者 A_i 並無法單獨產生出 n_i 因為攻擊者 A_i 並沒有使用者 U_i 的特定指紋 b_f，所以無法透過運算 $b_F \oplus (b_F \oplus n_i)$解出 n_i。

(3) 使用者假冒襲擊(User impersonation attack)：為了假冒 U_i，攻擊者 A_i 必須先產生 $T_1 = e_i \oplus f_i$，否則攻擊者 A_i 無法傳送合法的登錄請求訊息給 S，然而攻擊者 A_i 無法獨自產生出 f_i 因為攻擊者 A_i 並沒有使用者 U_i 的特定指紋 b_f 與 b_M，所以無法透過運算 $b_M \oplus n_i^* \oplus r_i$ 計算出 f_i^*。

(4) 伺服器假冒襲擊(Server impersonation attack)：攻擊者 A_i 為了假冒 S 必須有能力產生 $KU_i = h(ID_i \| x)$，而由於攻擊者 A_i 並無法取得 S 所持有的秘密金鑰 x，所以攻擊者 A_i 無法先運算出 $KU_i = h(ID_i \| x)$，所以攻擊者 A_i 無法假

冒 S。

(5) 相互認證(Mutual authentication)：由於上述的分析所以攻擊者皆無法假冒成合法的 U_i 以及 S，所以 U_i 以及 S 可以相互認證彼此身份。

(6) 內部攻擊(Inside attack)：本論文所提出的協定中，伺服器端並不需要儲存任何與使用者相關的資訊，與傳統基於使用密碼的身份認證相比，伺服器端的系統中將不需要維護與儲存密碼表，以及其他任何關於使用者身份認證的其他資訊，因此防止內部人員竊取與使用者相關的資料。

(7) 重送襲擊(Replay attack)：本研究所提出的認證協定中，每次需要進行身份認證時皆使用時戳 t_i、t_s 與隨機數 R_i、R_s，並透過對稱加密的演算方法加密時戳與隨機數等資訊，因此攻擊者 A_i 無法獨自產生出加密訊息，且每次加密之後的數值皆會不同因為時戳與隨機數每次皆不相同，所以攻擊者 A_i 無法透過單純的擷取通訊時的訊息實施重送攻擊。

(8) 指紋模板盜取攻擊(Stolen fingerprint template attack)：首先使用者的指紋模板皆使用生物雜湊演算所保護，此外在本論文的雲端認證方法中，指紋模板的計算並不交給雲端伺服器，因此雲端伺服器的內部人員也無法竊取，因此無法仿冒成使用者登入，因此本論文所提出的認證方法可以抵抗指紋模板盜取攻擊。

第三節 認證方法的分析比較

在此節中我們將比較 Li 與 Hwang 的方法、Das 的方法、An 的方法、Khan 與 Kumari 的方法以及 Wen 等人的方法以及本文所提出的認證方法的安全性分析與計算成本分析。在本篇所提出的方法中，使用者於剛開始註冊時會先輸入 $1 < M \leq N$ 的指紋個數所串成的指紋模板序列，其中 M 是使用者所入的指紋總數(如：$f_{i(1)} || f_{i(2)} || ... || f_{i(M)}$)所串接而成的使用者指紋特徵模板序列，並且其值一定必須大於 1；N 為系統所制定的指紋序列個數最大值，有別於相關研究中所探討的認證方法，本研究所提出之方法使用多重指紋序列取代密碼的使用，除此之外，本研究加入生物雜湊演算(Biohashing)的使用，因此本研究將會出現特有的運算成本，將在以下的分析

中詳細展現。

一、認證方法的安全性分析

在表 3-3 我們將比較並分析上述方法的各項安全性。並且顯示了 An 的方法以及 Khan 與 Kumari 的方法僅能防止內部攻擊與重送攻擊；Wen 等人的方法雖然顯示出能防止多項安全攻擊但卻無法防止指紋模板盜取攻擊且該方法仍需使用者額外記憶密碼來做為身份認證時的關鍵因子。而本篇所提出的方法則可以抵禦密碼猜測攻擊、防止使用者或伺服器假冒攻擊、支持相互認證、防止內部攻擊、防止重送攻擊、防止指紋模板盜取攻擊，並支持無使用者密碼認證。

表 3-3. 安全性分析

安全性分析	Li-Hwang [5]	Das [29]	An [28]	Khan-Kumari [1]	Wen et al. [30]	本論文所提出
A1	No	No	No	No	Yes	N/A
A2	No	No	No	No	Yes	N/A
A3	No	No	No	No	Yes	Yes
A4	No	No	No	No	Yes	Yes
A5	No	No	No	No	Yes	Yes
A6	No	No	Yes	Yes	Yes	Yes
A7	No	No	Yes	Yes	Yes	Yes
A8	No	No	No	No	No	Yes
A9	No	No	No	No	No	Yes

A1：線上密碼猜測攻擊，A2：離線密碼猜測攻擊，A3：使用者假冒襲擊，A4：伺服器假冒襲擊，A5：相互認證，A6：內部攻擊，A7：重送攻擊，A8：指紋模板盜取攻擊，A9：支持無使用者密碼認證。

二、運算成本分析

在表 3-4 中，我們比較了上述方法與本研究所提出的方法的各個階段的計算成本分析。我們比較了單向雜湊演算、生物雜湊演算以及對稱加密解密演算的計算成本。其中 C_h 表示為單向雜湊函數運算成本，一般而言單向雜湊演算的時間複雜度為 O(n)，其中 n 為所輸入的資訊長度，而互斥或運算(XOR)的計算成本將不會出現在表中，因為與單向雜湊演算的時間成本相比，互斥或運算(XOR)的計算成本可以忽略；C_{ED} 表示為對稱式加解密演算的運算成本，本研究所提出之方法透過對稱式加密演算的使用保護所傳送之訊息不會被非法窺伺與惡意串改。此外需要注意到在本篇所提出的方法中使用多重指紋序列取代密碼的使用，因此本研究加入生物雜湊演算(Biohashing)來保護使用者的指紋辨識資訊並令產生的指模辨識模板具有可取消性，所以本研究將會出現特有的運算成本將會比其他方法多出 $M \cdot C_{H_B}$ 的計算量，其中 M 為使用者於註冊時所登錄的指紋序列個數；C_{H_B} 代表使用生物雜湊演算(Biohashing)所產生的特有運算成本。

接下來我們將詳細列出本篇所提的使用多重指紋序列的認證方法與其他傳統使用單一生物辨識資訊並結合使用者密碼的認證方法兩者的運算成本比較，在註冊階段的計算成本中，若不考慮生物雜湊演算的計算成本，本篇研究所提的方法和 Khan 與 Kumari 的方法以及 Wen 等人的方法相同。雖然本篇研究所提出之方法多了 M+2 次的生物雜湊演算但請注意到註冊階段的計算成本將僅執行一次。在登入與認證階段中也可以注意到，本篇研究所使用的單向雜湊演算也比 Khan 與 Kumari 的方法以及 Wen 等人的方法少，並且在對稱加密演算的計算量上也小於等於 Wen 等人的方法。需要注意到我們所使用的方法有別於 Li 與 Hwang 的方法、Das 的方法、An 的方法以及 Khan 與 Kumari 的方法，除了加入生物雜湊演算外還使用了對稱式加密演算保護每次通訊中所傳遞的訊息，因此與上述的其他方法相比我們的方法將會多出對稱式加密解密的運算成本。

表 3-4. 計算成本分析

計算成本分析	Li-Hwang [5]	Das [29]	An [28]	Khan-Kumari [1]	Wen et al. [30]	本論文所提出
P1	$3C_h$	$3C_h$	$3C_h$	$4C_h$	$4C_h$	$4C_h + M \cdot C_{H_B}$
P2	$2C_h$	$2C_h$	$3C_h$	$3C_h$	$2C_h+1C_{ED}$	$2C_h + M \cdot C_{H_B} +1C_{ED}$
P3	$5C_h$	$8C_h$	$6C_h$	$7C_h$	$10C_h+9C_{ED}$	$5C_h+3C_{ED}$
Total	$10C_h$	$13C_h$	$12C_h$	$14C_h$	$16C_h+10C_{ED}$	$11C_h+ 2M \cdot C_{H_B} +4C_{ED}$

P1：註冊階段，P2：登入階段，P3：認證階段

C_h：單向雜湊函數運算成本，C_{H_B}：生物特徵雜湊函數運算成本，

C_{ED}：對稱式加解密演算成本

由表 3-1 與表 3-4 中我們比較了 Li 與 Hwang 的方法、Das 的方法、An 的方法、Khan 與 Kumari 的方法以及 Wen 等人的方法，可以看出雖然我們所提出的方法需要額外的生物雜湊演算與對稱式加密解密的運算成本，但考慮到本篇研究所提出的方法的安全性與支持無密碼認證，將可以發現在盡量維持計算成本的前提下，我們提出了更安全並且可以減輕使用者額外記憶密碼的身份認證系統。

第四章 結　論

本研究基於個人指紋是獨特且易於使用的，且指紋識別技術已被廣泛應用，並隨著時間的演進指紋掃描器逐漸支持多重指紋辨識掃描等因素，因此本研究提出基於使用多重指紋序列模板取代單一指紋模板與使用者密碼的雲端智慧卡認證方法。在相關研究中我們列舉出了生物辨識技術的眾多優勢如：不會丟失或遺忘、難以複製或共享、幾乎無法被猜到以及不容易被其他人破壞等因素，此外透過相關認證機制的回顧與分析，我們重新探討了 Li 與 Hwang 的方法、Das 的方法、An 的方法、Khan 與 Kumari 的方法以及 Wen 等人的方法，並針對 Khan 與 Kumari 的方法進行深入的安全性分析，我們發現認證機制隨著時間不斷被後續的學者改進，但仍然難以解決使用密碼本身所存在的缺陷如：密碼輕易的被猜測、密碼在使用時被窺視、以及輕易的被分享複製轉發等問題，除此之外也因為使用密碼的認證方法的結構中存在著缺陷，所以當攻擊者使用能量攻擊或旁道攻擊時，難以抵禦線上密碼猜測攻擊與離線密碼猜測攻擊，進而無法有效的防止使用者假冒攻擊、伺服器假冒攻擊並提供強而有力的相互認證。

基於上述的理由，增加以往生物辨識模板的使用與比重，透過多重且可重複的指紋模板序列，以此提高認證安全性並藉由多重指紋模板的排列複雜度，取代傳統基於使用密碼的認證方法。在本論文的遠端認證方法中，使用高安全性的生物雜湊演算和單向雜湊函數確保使用者認證資料的隱密性、使用者生物特徵的私密性與可取消性。此外在本論文的遠端認證方法中，可取消式指紋模板的計算並不透過雲端伺服器，因此無法從雲端伺服器內部非法竊取使用者的指紋模板辨識資訊，並且透過多重指紋模板序列的排列複雜度加上相同的指紋特徵資訊可以重複輸入的結構，藉此提高認證安全性。另外如果從指紋資訊可能遭受洩漏的角度來看，要透過非法的方式盜取或複製多個使用者指紋的難度明顯的要比盜取或複製單一指紋要來的高出許多。

本篇所提出的方法中，使用者於剛開始註冊時會先輸入 $1<M\leq N$ 的指紋個數所串成的指紋模板序列，其中 M 是使用者所輸入的指紋總數(如:$f_{i(1)}||f_{i(2)}||...||f_{i(M)}$)所串接而成的使用者指紋特徵模板序列，並且其值一定必須大於 1，因為與單一指紋模板相比，多重指紋模板具有排列的特性，且須依正確的指紋輸入順序才可通過

認證且相同的指紋資訊可重複輸入。此外從指紋資訊可能遭受洩漏的可能性來看，要透過非法的方式盜取或複製多個使用者指紋的難度明顯的要比盜取或複製單一指紋要來的高出許多；其中 N 為指紋模板序列總數輸入的最大值，由系統制定，當 N 值越大時可以想見指紋特徵模板序列將會更複雜，例如當設定的指紋模板數是 10 時，其可能性便有 10^{10} 種的排列組合，但這邊我們需要強調，這 10^{10} 種不同的序列全是使用者的指紋模板所構成，而跟密碼不同的是，生物特徵資訊難以窺視、幾乎無法複製、不能隨意共享轉發以及難以透過數位攻擊破壞。此外我們使用生物雜湊演算保護使用者的指紋模板資訊讓指紋模板具有可取消性，讓使用者可以使用相同指紋資訊註冊多種不同的雲端服務，另外假使當使用者的指紋辨識模板資訊不幸遭到竊取或破壞，也可以透過修改生物雜湊演算的參數重新使用相同指紋資特徵資訊產生新的指紋辨識模板。此外本研究所提出的方法中所使用的生物雜湊演算所產生的生物碼(Biocode)的預設長度為 256 位元。需要注意到的是儘管透過生物雜湊演算所產生的生物碼(Biocode)是經過壓縮過的生物辨識資訊，但世界的人口總數介於 2^{32} 到 2^{33} 之間，而 256 位元長度的生物碼(Biocode)的可能性卻是 2^{256} 種之多，所以其雜湊碰撞(Collision)的可能性將微乎其微(因為非一般情況下雜湊函式的輸入和輸出有可能不是唯一的映射關係這種情況稱為「雜湊碰撞」)，因此資料量足以表示不同使用者之間的不同指紋特徵資訊。

因此本篇研究所提出的使用多重指紋序列的遠端認證機制主要有以下 5 點貢獻：

(1) 透過多重序列指紋模板的使用取代使用者密碼，以達成更安全、更高效、更易用且更完善的認證有效性。

(2) 多重序列指紋模板的使用大幅度增加了攻擊者透過盜取使用者指紋進行非法存取的難度。

(3) 使用生物雜湊演算生成的指紋模板具有可取消性，讓使用者可以使用相同指紋資訊註冊多種不同雲端服務。

(4) 即使當使用者的智慧卡遺失或被盜取，攻擊者也無法透過能量攻擊或旁道攻擊取得行動裝置中的秘密值後假冒使用者通過身份驗證。

(5) 提供了指紋模板變更階段，此外假使當產生之指紋辨識模板不幸遭到竊取或破壞，也可以透過修改生物雜湊演算的參數重新使用相同指紋特徵資訊產生新的指紋辨識模板。

隨著基礎指紋辨識硬體的普及與日新月異，以及更多的雲端服務存取，使用者身份認證的安全性與重要性將與日俱增，透過提高指紋辨識在認證機制的使用與比重，不僅提供更高的安全性，亦提供使用者使用上的便利性與身份認證的不可否認性，此外不難看出未來身份認證的重要因子將逐漸放在個體生物特徵資訊上，因為基礎生物辨識硬體的建置與普及，將會有越來越多的應用結合生物特徵辨識作為使用者身份認證的關鍵因子，未來希望能夠將本論文的研究成果更廣泛的整合在電子商務相關應用上，如智慧卡形式的電子錢包、ATM 提款機等等。

參考文獻

[1] M. K. Khan and S. Kumari, "An Improved Biometrics-Based Remote User Authentication Scheme with User Anonymity," BioMed Research International, vol. 2013, 2013.

[2] S. Prabhakar, S. Pankanti and A. K. Jain, "Biometric recognition: security and privacy concerns," IEEE Security & Privacy, vol. 99, no. 2, March - April 2003.

[3] A. K. Jain, A. Ross and S. Prabhakar , "An introduction to biometric recognition," IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 4 - 20, January 2004.

[4] A. K. Jain, "Biometric recognition: how do I know who you are?," in 2004. Proceedings of the IEEE 12th Signal Processing and Communications Applications Conference, 2004.

[5] C.-T. Li and M.-S. Hwang, "An efficient biometrics-based remote user authentication scheme using smart cards," Journal of Network and Computer Applications, vol. 33, no. 1, pp. 1 - 5, January 2010.

[6] M. Jakobsson, Mobile Authentication Problems and Solutions, 1 ed., Springer-Verlag New York, 2013, pp. XIV, 113.

[7] N. Ismail, "In the modern era biometrics should replace passwords," 13 February 2017. [Online]. Available: http://www.information-age.com/biometrics-replace-passwords-123464420/. [Accessed 7 July 2017].

[8] D. Benini, "Why Biometrics Will Replace the Password for Mobile Banking," 25 May 2017. [Online]. Available: https://www.aware.com/biometrics-replace-password-mobile-banking/. [Accessed 9 July 2017].

[9] A. K. Jain and K. Nandakumar, "Biometric Template Security," EURASIP Journal on Advances in Signal Processi, vol. 2008, no. 113, January 2008.

[10] Z. Jin, A. B. J. Teoh, T. S. Ong and C. Tee, "Fingerprint template protection with minutiae-based bit-string for security and privacy preserving," Expert Systems with Applications, vol. 39, no. 6, pp. 6157 - 6167, May 2012.

[11] V. M. Patel, N. K. Ratha and R. Chellappa, "Cancelable Biometrics: A review," IEEE Signal Processing Magazine, vol. 32, no. 5, pp. 54 - 65, September 2015.

[12] N. K. Ratha, S. Chikkerur and J. H. Connell, "Generating Cancelable Fingerprint Templates," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 29, no. 4, April 2007.

[13] E. Chandra and K. Kanagalakshmi, "Cancelable biometric template generation and protection schemes: A review," 3rd International Conference on Electronics Computer Technology (ICECT), vol. 5, pp. 15 - 20, April 2011.

[14] A. T. B. Jin, D. N. C. Ling and A. Goh, "Biohashing: two factor authentication featuring fingerprint data and tokenised random number," Pattern Recognition, vol. 37, no. 11, p. 2245 – 2255, 11 2004.

[15] A. B. J. Teoh, A. Goh and D. C. L. Ngo, "Random multispace quantisation as an analytic mechanism for biohashing of biometric and random identity inputs," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 28, no. 12, pp. 1892 - 1901, December 2006.

[16] A. K. Das and A. Goswami, "A robust anonymous biometric-based remote user authentication scheme using smart cards," Journal of King Saud University - Computer and Information Sciences, vol. 27, no. 2, pp. 193 - 210, April 2015.

[17] L. Nanni, S. Brahnam and A. Lumini, "Biohashing applied to orientation-based minutia descriptor for secure fingerprint authentication system," Electronics Letters, vol. 47, no. 15, pp. 851 - 853, July 2011.

[18] W. Xiaomin, X. TaiHua and Z. Wenfang , "Chaos-based biometrics template protection and secure authentication," in State of the art in Biometrics, vol. 15, J. Yang and L. Nanni, Eds., InTech, 2011, pp. 293 - 314.

[19] N. Radha and K. Subramanian, "An Evaluation Of Fingerprint Security Using Noninvertible Biohash," International Journal of Network Security & Its Applications (IJNSA), vol. 3, no. 4, July 2011.

[20] L. Nanni and A. Lumini, "Empirical tests on BioHashing," Neurocomputing, vol. 69, no. 16, pp. 2390 - 2395, October 2006.

[21] R. Belguechi, E. Cherrier, C. Rosenberger and S. Ait-Aoudia, "Operational bio-hash to preserve privacy of fingerprint minutiae templates," IET Biometrics, vol. 2, no. 2, pp. 76 - 84, June 2013.

[22] R. Belguechi and C. Rosenberger, "A Study on the Convergence of FingerHashing and a Secured Biometric System," Proceedings of the 2nd conferences Internationale On Computer Science and its Applications (CIIA'09), May 2009.

[23] D. Maio and L. Nanni, "Multihashing, human authentication featuring biometrics data and tokenized random number: A case study FVC2004," Neurocomputing, vol. 69, no. 1 - 3, pp. 242 - 249, December 2005.

[24] A. Kong, . K.-H. Cheung, D. Zhang, M. Kamel and J. You, "An analysis of BioHashing and its variants," Pattern Recognition, vol. 39, no. 7, p. 1359 – 1368, July 2006.

[25] A. Lumini and L. Nanni, "An improved BioHashing for human authentication," Pattern Recognition, vol. 40, no. 3, pp. 1057 - 1065, March 2007.

[26] R. Belguechi, E. Cherrier and C. Rosenberger, "Texture based fingerprint BioHashing: Attacks and robustness," 5th IAPR International Conference on Biometrics (ICB), pp. 196 - 201, March 2012.

[27] L. Nanni, A. Lumini and S. Brahnam, "A secure multimatcher system for fingerprint verification," in proceedings 2013 Annual Meeting of the Northeast Decision Sciences Institute (NEDSI), pp. 511 - 522, April 2013.

[28] Y. An, "Security Analysis and Enhancements of an Effective Biometric-Based Remote User Authentication Scheme Using Smart Cards," Journal of Biomedicine

and Biotechnology, vol. 2012, no. 2012, June 2012.

[29] A. K. Das, "Analysis and improvement on an efficient biometric-based remote user authentication scheme using smart cards," IET Information Security, vol. 5, no. 3, pp. 145 - 151, September 2011.

[30] F. Wen , W. Susilo and G. Yang, "Analysis and Improvement on a Biometric-Based Remote User Authentication Scheme Using Smart Cards," Wireless Personal Communications: An International Journal, vol. 80, no. 4, pp. 1747 - 1760, February 2015.

[31] D. Hsu, "Fingerprint Sensor Technology And Security Requirements," [Online]. Available: http://www.kilopass.com/fingerprint-sensor-technology-and-security-requirements/. [Accessed 08 July 2017].

[32] J. Avari, "Qualcomm Snapdragon Sense ID 3D Fingerprint Technology Unveiled at MWC 2015," 02 March 2015. [Online]. Available: http://gadgets.ndtv.com/mobiles/news/qualcomm-snapdragon-senseid-3d-fingerprint-technology-unveiled-at-mwc-2015-666263. [Accessed 12 July 2017].

[33] P. C. Kocher , J. Jaffe and B. Jun, "Differential Power Analysis," in CRYPTO '99 Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology, 1999.

[34] R. McEvoy, M. Tunstall, C. C. Murphy and W. P. Marnane, "Differential Power Analysis of HMAC Based on SHA-2, and Countermeasures," in WISA 2007: Information Security Applications, 2007.

[35] O. Benoît and T. Peyrin, "Side-Channel Analysis of Six SHA-3 Candidates," in CHES 2010: Cryptographic Hardware and Embedded Systems, CHES 2010, 2010.