Regular Paper

Communications of the CCISA
Vol. 25 No. 4 Nov. 2019

應用於 5G 環境中之快速代理認證與可信賴資料加密協定

郭信男[1]、施宇澤[2]、莊額碩[3]、黃政嘉[4]、范俊逸[5*]
[1, 2, 3, 5]國立中山大學資訊工程學系
[4, 5]財團法人電信技術中心
[5]國立中山大學資訊安全研究中心
[5]國立中山大學智慧電子商務研究中心
[1]bluedunk@gmail.com、[2]steven8450@gmail.com、[3]zhaunges@gmail.com、
[4]jhengjia.huang@gmail.com、[5]cifan@mail.cse.nsysu.edu.tw

摘要

由於資訊科技的蓬勃發展，社會大眾對上網服務的需求亦逐漸增加，且伴隨著行動電信產業的進步，人們對於上網速率及效能的提升都有相對高的期待，因此語音傳輸的技術同時必須跟著演進，從原本提供數據服務業務且只能滿足簡單的通訊、簡訊、上網單一功能的 2G，到有較多媒體形式可處理的 3G 網路，此外，為滿足用戶們對於無線服務及更高速語音通話的需求，行動寬頻網路 4G LTE 也因應而生，並進一步研究出擁有更大頻寬、更高效能的 5G 網路。然而近期物聯網的興盛，同時提升人們對資訊傳輸的高依賴性，進而給 5G 環境帶來較大的負擔。針對此憂慮，本論文採用多個裝置在物聯網的環境中會互相通訊之特性，並結合類細菌網路的環境架構，於 5G 網路中建構一套能夠快速代理認證，同時包含可信賴之檔案加密協定的環境，使得資訊傳輸不再僅限於必須透過基地台，使用者亦可自行選擇所要傳輸的路徑，不過也因為在 5G 環境中每一位用戶都必須與基地台進行合法的認證，且難以去預防傳輸中的惡意節點或者特定人士的惡意行為，有使用上的資安問題及效能的擔憂。因應此問題，本論文於先前研究上結合委外運算的概念以及盲化資料的處理，設計出一套兼具輕量化和盲化特性之委外認證機制，使得各個裝置能透過安全的擴散式傳輸管道相互傳送資訊，同時確保傳送節點及數據來源是否合法。而沿襲先前之成果，此次計畫使用密文切割、重組以及整合的技術，同時包含門檻式機制(Threshold)容錯的特性，有效降低基地台運算及傳輸資訊之負擔，預計可以達到增加資訊傳輸效能之目的，並且提升網絡環境的整體服務品質。

關鍵詞：5G 行動網路技術、物聯網、類細菌網路、秘密分享技術、容錯機制

* 通訊作者 (Corresponding author.)

Regular Paper

Communications of the CCISA
Vol. 25 No. 4 Nov. 2019

Fast Proxy Authentication and Trusted Data Encryption Protocol Applied in 5G Environments

Hsin-Nan Kuo[1], Yu-Tse Shih[2], Er-Shuo Zhuang[3], Jheng-Jia Huang[4], and Chun-I Fan[5*]
[1, 2, 3, 5]Department of Computer Science and Engineering, National Sun Yat-sen University
[4,5] Telecom Technology Center
[5]Information Security Research Center, National Sun Yat-sen University
[5]Intelligent Electronic Commerce Research Center, National Sun Yat-sen University
[1]bluedunk@gmail.com、[2]steven8450@gmail.com、[3]zhaunges@gmail.com、
[4]jhengjia.huang@gmail.com、[5]cifan@mail.cse.nsysu.edu.tw

Abstract

Due to the rapid development of information technology, the demand for Internet services has gradually increased. With the advancement of the mobile telecommunications industry, people have relatively high expectations for the improvement of Internet speed and performance. Therefore, voice transmission technology must keep up with the speed of evolution. This evolution process is from 2G network that originally provided the data service business and can only satisfy the simple communication, SMS, and single function of the Internet, to the 3G network that can be processed in the multimedia form. In addition, to meet users' demand for wireless services and higher-speed voice calls, the mobile broadband network of 4G LTE has also evolved, and telecommunications providers further research into 5G networks with greater bandwidth and higher performance. However, the recent booming in IoT (Internet of Things) has also raised people's high dependence on information transmission, which has placed a heavy burden on the 5G network environment. For this concern, this paper combines the concept of Bacteria-inspired network with the feature that multiple devices can communicate with each other in the IoT environment, so that we can construct an environment with fast proxy authentications and a trustworthy file encryption protocol. The data transmission is no longer limited to having to pass through the base station, instead, the user can select the path for transmitting to be transmitted. However, each user must be legally authenticated with the base station in the 5G network environment, and it is difficult to prevent the malicious nodes in the transmission or the malicious behavior of specific people, so there are some worries about the security problems and performance. In response to this problem, this paper combined the concept of outsourcing computing with blind processing in the above project and built a set of outsourcing authentication mechanisms with both lightweight and blind data features, so that each device can transmit information to each other through a secure diffusion transmission pipeline, and we can ensure that the transmission node and data source are legitimate at the

same time. Following the above results, our project can effectively reduce the burden on the base station to calculate and transmit information by ciphertext cutting, recombination and integration technologies with threshold fault tolerance. It is expected that the purpose of transmitting the information efficiently can be achieved and the overall service quality of the network environment will be improved.

Keywords: 5G, Internet of Things, Bacteria-Inspired Communication, Secret Sharing, Fault Tolerance

壹、前言

近年來，社會大眾對上網服務的需求隨著資訊的蓬勃發展逐年增加，智慧型行動裝置也跟著多樣化和普及，經由網路資訊的技術，人們得以串聯各式各樣非連網的裝置設備，提升生活的豐富性以及便利性，也使得大眾與資訊科技的關係更加密不可分，進一步帶動了智慧型家電以及相關的遠端操控服務等等的興起，而為了滿足使用者的產品期待，終端使用設備不斷被改善，使得外觀及功能的設計更加精細，足以達到每個使用者的需求。儘管如此，由於人們對資訊傳輸的高依賴性，行動裝置數量開始大幅成長，連帶網路的頻寬需求增加，有線網路提供服務的效能開始受到影響，因此語音傳輸的技術勢必同時跟著演進，從單純提供數據服務業務，例如通訊、簡訊、上網單一功能的 2G，到了有較豐富媒體形式可處理的 3G 網路，之後為了滿足用戶們對無線服務及更高速語音通話的期待，行動寬頻網路 4G LTE 也因應而生，然而提供的網路頻寬依舊無法跟上使用者的需求，於是更大頻寬、更高效能的 5G 網路出現了。雖然 5G 網路的覆蓋性較廣，且擁有比 3G、4G 表現更卓越的效能及大頻寬的設計，但這也帶來了一些隱含的缺點，包含主幹基地台（Macro cell）為了服務數量增多的 5G 節點，必須花費較多效能，因此為降低主幹基地台（Macro cell）所需要的運算成本，使其能夠單純處理封包資料之傳輸，將與用戶認證的相關機制均轉移給枝幹基地台（Micro cell）、末端節點基地台（Pico cell）及用戶裝置來負責。

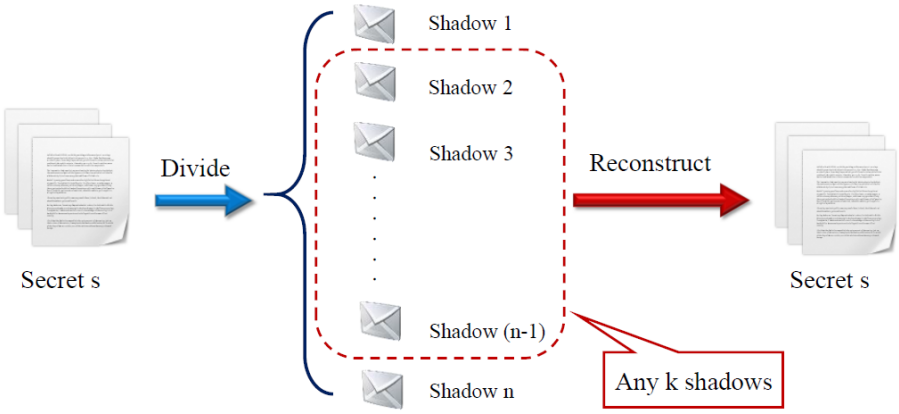
而伴隨著物聯網（Internet of Things, IoT）時代的來臨，智慧型家用電器以及行動式終端設備快速的發展，設備與設備間透過無線通訊協定彼此串聯互相交流，網際網路的使用不再被侷限於特定裝備，應用範圍擴及到手錶、眼鏡等隨手可見的裝置，逐漸達成現實世界數位化的理念。然而在大家享受科技帶來的便利之時，因為這些設備均需要大量的資訊供分析利用，傳送數據的過程中默默給 5G 網路帶來較大的負擔，從數據量增加造成基地台的頻寬受到影響，到使用者裝置數目增多，和 5G 網路本身傳輸距離較低，必須大面積部署相關的末端節點基地台和枝幹基地台，進而影響到基地台與裝置之間安全認證的頻率越來越高，以上種種因素都使得 5G 網路提供的服務品質受到影響。有鑑

於此，本論文預計結合類細菌網路(Bacteria-Inspired Network) 以及物聯網的終端使用設備互相通訊的特色，將用戶端裝置視為數據傳輸管道的節點，建構一個能夠快速代理認證，同時包含可信賴之檔案加密協定的環境，將數據傳輸的路徑擴大至除了基地台，任何得到基地台安全認證的使用裝置均能成為代理基地台及傳輸節點，大大的降低基地台所需承受的負荷，同時提高傳輸資訊的效能和整體服務的品質。

貳、文獻探討

2.1 秘密分享技術

秘密分享技術(Secret sharing)在 1979 年時分別由兩位學者 Adi Shamir [5]和 George Blakley [6]各自發表，其技術概念如圖(一)所示。其中動機源自於金鑰安全管理，經由運算，高機密性資料將能分享給所有參與者，因此這些參與者都會持有秘密的一部分，而當參與者的數量達到一定的門檻值（Threshold），就能還原此份高機密性資料的所有內容。Adi Shamir 首先提出一個稱為(k, n)門檻機制之秘密分享技術的基本觀念，主要原理為存在一個會選定主金鑰的分派者（dealer），再將一份具有機密之檔案隱藏在(k-1)次多項式的常數，並生成一個隨機的多項式係數 n，經由密碼技術處理後分割出 n 份 shadows 表示為子金鑰，最後必須從 n 個 shadows 中取出 k 份之門檻值才能夠重建多項式而重組出原始之機密檔案內容，若所得到的數量少於門檻值 k，將沒辦法得到機密檔案之原始內容；George Blakley 所提出之技術是基於幾何線性投影概率之方式，隱藏明文在 m 維空間的點之中，並隨機生成 n 個通過此隱藏明文之點的方程式當作 shadows，欲重新建構檔案時，必須從 n 個方程式中取出 m 個方程式，再解出 m 維的線性方程組來獲取明文的內容。



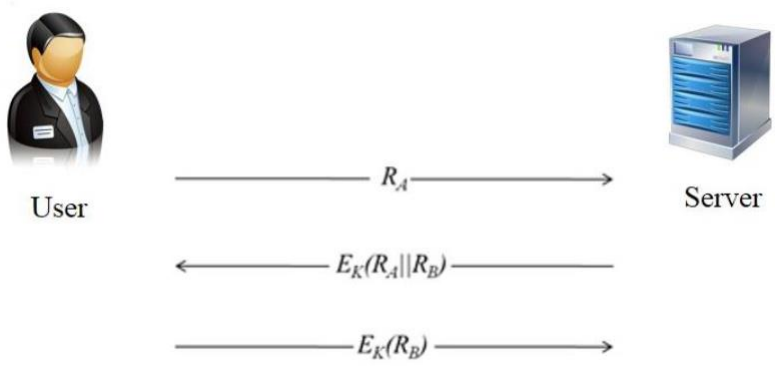
圖一：秘密分享圖

2.2 拜占庭容錯機制

拜占庭容錯機制（Practical Byzantine Fault Tolerant, 縮寫 PBFT）於 1999 年時由 Castro 和 Liskov 提出針對拜占庭將軍問題的實際解決方案[7][8]，主要是保證當有關聯的節點有潛在的故障損害時（就是所謂的拜占庭將軍問題），依舊可以在可靠的網路通訊下達成一致性，這樣的做法能確保當節點被惡意攻擊時，服務依然是可以照常運行的。PBFT 強調當有損害的節點小於 1/3，剩餘正常節點依舊有能力達成共識並可以一致的執行正常的結果，此核心理念用公式表示則為假設 n 表示一個系統內的總節點數量，系統內最終的容錯率將不超過$(n\text{-}1)/3$。

2.3 亂數認證

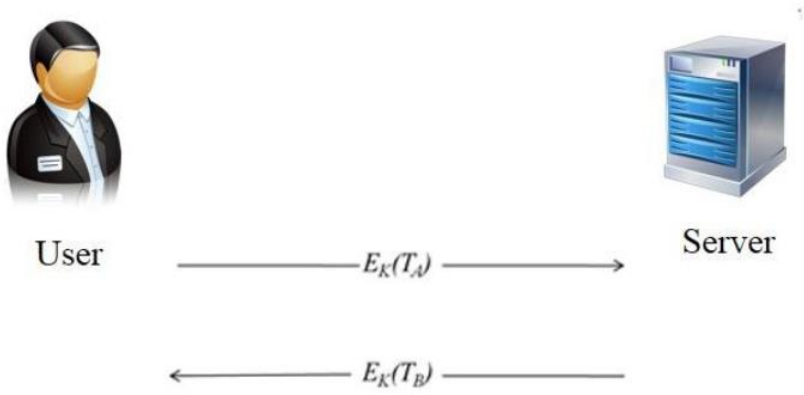
亂數認證(Nonce-based authentication)之示意圖如圖(二)所示，當雙方使用者於一開始的註冊階段便建立一把金鑰 k, 使用者會隨機的選擇 R_A 當作要傳給伺服器端的亂數，伺服器端接收到 R_A 之後，將 R_A 與之後選擇的 R_B 亂數用金鑰 k 加密。其中，E_k ( )表示以金鑰 k 執行對稱式加密，||單純表示連接兩個字串。當使用者接收到伺服器端傳來的密文 $E_k(R_A||R_B)$，會進行解密並確認 R_A 的存在，再加密且回傳從中取出的 R_B，直到伺服器端接受到此加密 R_B，再進一步去執行解密，同時驗證此密文是否與加密的 R_B 相等[9][10]。



圖二：亂數認證圖

2.4 時戳基底認證

如圖(三)所示，假設雙方已經於註冊階段雙方已經事先建立好一把金鑰 k，由於時戳是代表當前時間的戳記，所以首先使用者取得當前其系統的時間 T_A，並將 T_A 用 k 加密後送給伺服器，伺服器收到後解密確認 T_A 的時效性(Freshness)，接著伺服器也取得當前其系統的時間 T_B，同樣將 T_B 用 k 加密後回傳給使用者，而使用者也進行解密後確認 T_B 時效性的動作，完成雙方的認證。



圖三：時戳基底認證圖

上述三種認證方式其中以時戳認證之效率最好，但在時戳式認證中，首先必須先做到收送雙方時間同步化(Time Synchronization)，同步化後雙方才能夠藉由收到的時戳進行時戳時效性的判定；再者，在網路上資訊傳遞常會有傳遞延遲時間(Delay Time)，因此在時效性的判斷上會有一個門檻值，例如可以容許延遲多少時間，在此時間片段內收到的時戳都算通過驗證。因此門檻的訂定也有困難度存在，要以多少的時限做為門檻才適合，可能又必須依據在不同網路環境下不同的延遲時間而定，也就是時戳認證必須建立在雙方系統時間同步以及傳輸延遲時間穩定的條件下；亂數認證雖然不需要上述的條件，但其效果最差；一次性秘密認證為具有高效率且不需要強假設條件之協定。

一般來說，針對一個身份認證協定，有下列幾項具體的設計準則：

(1) 低運算量

在之前的內容中有提到過，雖然智慧卡具有記憶與運算的能力，但還是有所限制，因此分派給智慧卡的計算量必須有所限制，不能太大，以避免認證時間過長的問題。

(2) 驗證系統端的真偽

在之前談到的部分都屬於系統要確認使用者身份是否為合法使用者，但事實上，系統也有可能遭到假冒並與使用者進行溝通試圖獲取使用者的機密資訊，例如釣魚網站，因此最好也能夠驗證系統端，形成雙方互相驗證(Mutual Authentication)，上述針對參數交換式與時戳式認證所舉的例子，均能達到雙向認證。

(3) 可抵擋離線字典攻擊

由於離線字典攻擊要比線上字典攻擊更難以防範，因此要特別考量如何抵擋離線字典攻擊。

(4) 可抵擋重送攻擊

無特殊技能的攻擊者亦能實行重送攻擊，因此可抵擋重送攻擊已成為認證協定的基本要求。

(5) 不需要時間同步化與延遲時間的預測

時戳式認證中，認證雙方須事先將時間同步化，且需訂定適當的門檻值才能確保認

證之正確性，而門檻值則會因網路環境不同而有所差異，因此還是以使用參數交換式的認證機制為佳。

而時至今日，身份認證技術又有更進一步的突破，從原先的雙因子的認證機制加入了另外一項因子，就是把使用者生物特徵(例如指紋、虹膜)加入作為第三項的認證因子，其好處在於生物特徵具有比 Password 更高的亂度，也就是有別於 Password 會有可能因為字典攻擊而遭到破解的缺點，且某些生物特徵也不像智慧卡有容易遺失的可能性與風險。以下表(一)是簡略的三個因子間的比較表。

表一：各因子間的比較

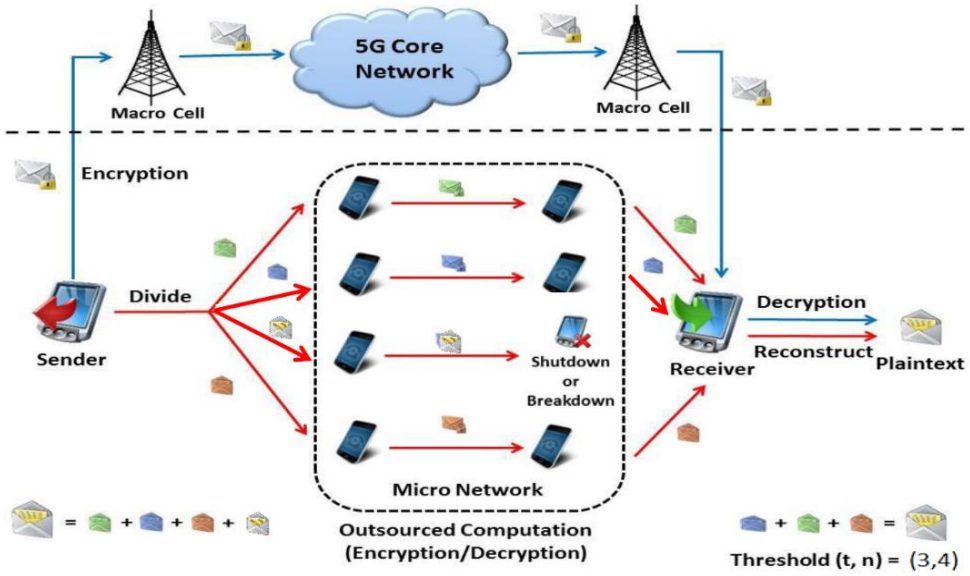
	優點	缺點
Password	易於更換 難以遺失	亂度低
智慧卡	可以更換 提供儲存能力	可能遺失
生物特徵	亂度高	不容易改變 可能遺失

參、研究方法

在 5G 網路結合類細菌網路環境中，由於檔案的快速散佈，檔案擁有者可以選擇直接傳輸密文資料，然而隨著鄰近轉送節點數量增加會使得通訊與儲存成本呈線性成長，造成行動裝置間的通訊與儲存成本急遽提高。檔案擁有者也可以選擇將密文進行分割之後再傳送，此方法雖能加速檔案傳送，卻有可能因為傳輸節點轉為休眠狀態或與設備的連結中斷，造成目標裝置無法順利重組檔案。因此，本論文預期對檔案分割方法進行研究，利用類細菌網路的多節點特性，增加檔案分割數量，讓分割後的子檔案，彼此涵蓋其它子檔案的資訊，使目標裝置在接收分割檔案時，區塊數量只需要達到允許的門檻值後便可進行容錯式的檔案重組，使目標裝置能順利接收檔案，同時減輕轉送檔案之節點的通訊與儲存成本。

植基於類細菌網路檔案的傳輸方式，首先將傳輸資料進行分割成數個加密子檔案，並且可各自經由不同節點之路徑抵達接收端的裝置，接下來接收端的裝置透過各節點之路徑所收集足夠多的分割檔案後利用門檻(Threshold)的方式進行重組及解密得到原始傳輸資料。如圖(四)所示，檔案發送端可以選擇兩種方式進行檔案傳輸，第一種方式為傳輸檔案行經一般的 5G 網路傳輸路徑抵達檔案接收端，第二種方式為在傳輸檔案之前將該檔案進行切割為多個加密子檔案，再分別經由不同的傳輸節點路徑抵達檔案接收端，倘若接收到的子檔案數量符合設定的門檻值，檔案接收端即能將分割子檔案重組回原始

傳輸檔案。在此例中，分割子檔案數目為 4，門檻值設定為 3，雖然傳輸過程中有一子檔案遭遇中斷或損壞的情況，但是檔案接收端收到的分割子檔案數量為 3，即符合門檻值，因此能夠順利的將分割子檔案重組還原為原始傳輸檔案。



圖四：情境示意圖

肆、結果與討論

相較於龐大的運算量而言，盲化且委外給較有能力之結點運算能大幅減少自身節點的運算時間且減輕了節點不少的負荷量，因此在有限的用戶行動裝置運算能力下，本論文將先前研究中所提的盲化委外運算與前次所做之簽章做結合成為一個新的運算機制，透過簡單的認證機制並可以輕鬆的完成委外運算，如此可以大幅的減少節點的負擔。同時，透過密文切割的方式來達成保護檔案隱私，並加入門檻式機制來協助解密及重組機密檔案內容，已達到高效能且高隱私保護的需求。

委外運算函數(Outsourcing())：

輸入：m, g where g is a generator for group G with prime order p, and $m \epsilon \mathbb{Z}_p$
輸出：$g^m \mod p$

步驟 1. 執行 Rand tool 取得一組 (α, g^α)。
步驟 2. 選取一個足夠小的數 r, e.g. $r \epsilon [1,10]$, 產生 $a = m - \alpha$ and $b = r(m - \alpha)$
步驟 3. 傳送(a, b) 給伺服器，獲得 $(c, d) = (g^a, g^b)$

步驟 4. 輸出$g^m = c(g^\alpha)$ if $\left(c(g^\alpha)\right)^r = b(g^\alpha)^r$

初始階段

Telcom 替每個 node 產生憑證和配一組非對稱式的公私鑰。

註冊階段

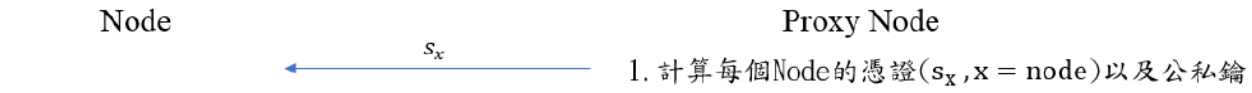
每個 node 傳送憑證給 proxy node，proxy node 將進行驗證，驗證完畢後，送回一個對稱式的長期金鑰(long-term key) K 給每一個 node，node 收到金鑰 K 後將儲存至記憶體之中。

認證階段

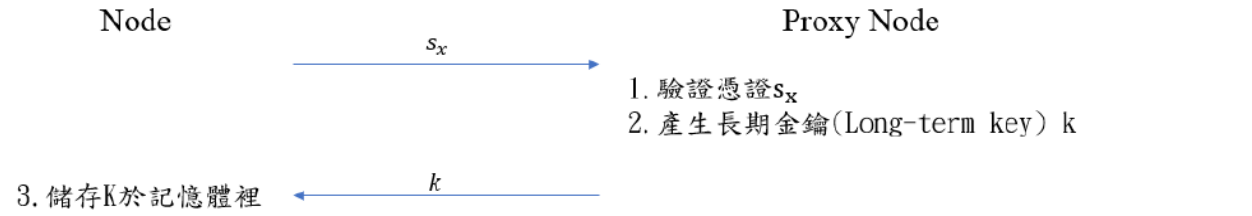
Node I 選擇一個亂數 r 以及 node I 憑證藉由長期金鑰 K 對稱式加密給 proxy node，proxy node 運用長期金鑰 K 解密並驗證確認是 node I。Proxy node 在選擇亂數 m 做 sign(r+m)以及 Hash(m)，proxynode 接著使用 K 加密 sign(r+m)、r 以及 Hash(m)，回傳給 node I。node I 將進行解密並確認 r 是否與前次送出有相同結果，並儲存 sign(r+m)、Hash(m)，由於 node I 沒有足夠的運算能力去驗證 proxy node 是否合法使用者，因此必須使用委外運算。

假設有一個不屬於這個網域的成員 node J，node J 具有高運算的能力，用戶便可以請求 node J 做進行委外運算，於是 node I 將本身憑證以及 sign(r+m)傳送給 node J，node J 收到資料後會先驗證 node I 憑證是否為 Telecom 所核發的憑證，如果是合法的使用者，node J 會呼叫 outsourcing 函式做運算輸入 sign(r+m)，運算後輸出 r+m，並回傳給 node I。node I 接收後把 r+m 減去 r 得到 m，並將 m 做 Hash，最後驗證 Hash(m)和 proxy node 送來的 Hash(m)是否一樣。

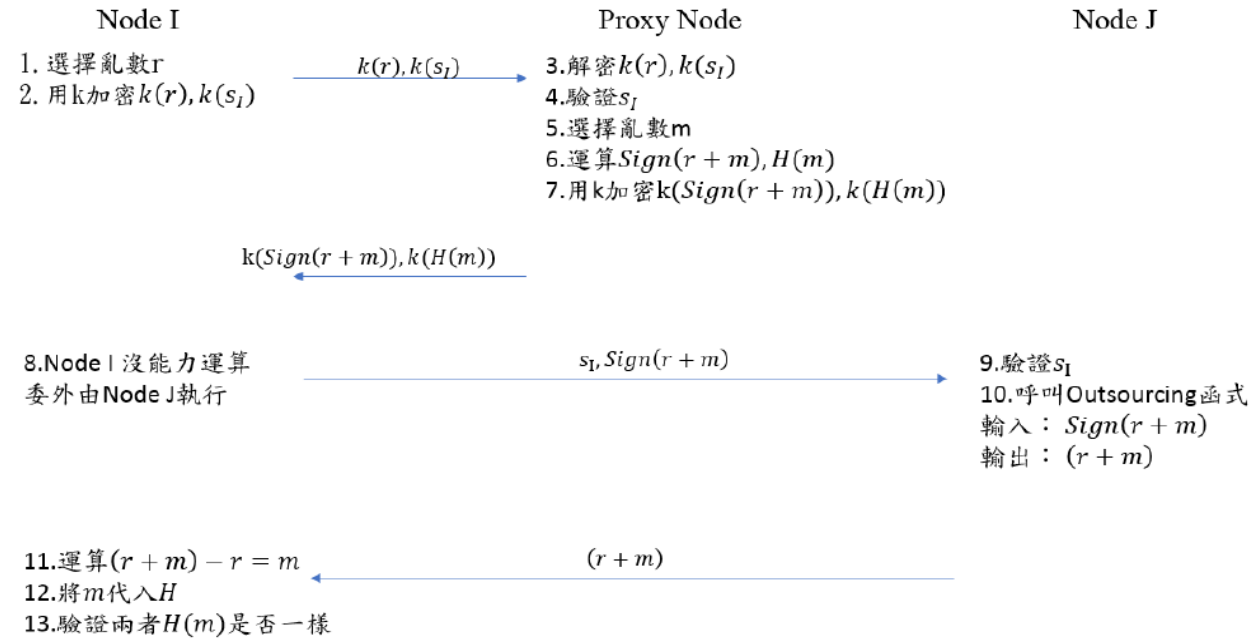
I. 初始階段:



II. 註冊階段:



III. 認證階段:



伍、結論

隨著科技快速的變遷，5G 網路結合物聯網的時代已悄悄來臨，然而本文發現其中有關資安及效能的隱憂，並且針對此相關問題，欲設計一套可於 5G 行動通訊系統運行的軟體定義無線類細菌網路平台之快速代理認證及可信賴資料加密協定。此論文沿襲先前關於輕量化和盲化特性之委外認證機制的成果，並加上密文切割來實踐保護檔案隱私性的目的，同時包含門檻式機制協助解密以及重組機密檔案之內容，達到高效能且高隱

私保護的需求。

本論文完成兼具輕量化與盲化的委外認證機制之後，採用密文切割、重組以及整合的技術，並結合門檻式機制與容錯特性，加強檔案傳輸的完整性與隱私性。此完善架構幫助基地台減輕運算資料上的負擔，進一步提供 5G 物聯網更安全穩固的服務品質，使用戶能有更高效率的網路環境，對大眾以及需求大幅增加的 5G 行動物聯網環境有相當的助益。

Acknowledgements:

This study was funded by the Ministry of Science and Technology of Taiwan (MOST 105-2221-E-110-053-MY2). This work was also supported by Taiwan Information Security Center at National Sun Yat-sen University (TWISC@NSYSU), the Information Security Research Center of National Sun Yat-sen University, Taiwan, and the Intelligent Electronic Commerce Research Center from The Featured Areas Research Center Program within the framework of the Higher Education Sprout Project by the Ministry of Education (MOE) in Taiwan.

參考文獻

[1] R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka and J. Molina, "*Controlling data inthe cloud: outsourcing computation without outsourcing control*," in Proc. of the 2009 ACM workshopon Cloud computing security. ACM, pp. 85-90, November 13, 2009

[2] A. Yao, "*Protocols for secure computations.*" In Proceedings of the IEEE Symposium on Foundationsof Computer Science, pp. 160-164, 1982.

[3] A. Yao, "*How to generate and exchange secrets.*" In Proceedings of the IEEE Symposium onFoundations of Computer Science, pp. 162-167, 1986.

[4] Chow, and Richard, "*Controlling data in the cloud: outsourcing computation without outsourcingcontrol.*" Proceedings of the 2009 ACM workshop on Cloud computing security. ACM, 2009.

[5] Shamir, Adi. "*How to share a secret.*" Communications of the ACM 22.11 (1979): 612-613.

[6] Blakley, George Robert. "*Safeguarding cryptographic keys.*" Proceedings of the national computerconference. Vol. 48. 1979.

[7] Castro, Miguel, and Barbara Liskov. "*Practical Byzantine fault tolerance.*" OSDI. Vol. 99. 1999.

[8] Castro, Miguel, and Barbara Liskov. "*Practical Byzantine fault tolerance and proactive recovery.*" ACMTransactions on Computer Systems (TOCS) 20.4 (2002): 398-461.

[9] Tsai, Jia Lun. "*Efficient Nonce-based Authentication Scheme for Session Initiation Protocol.*" IJNetwork Security 9.1 (2009): 12-16.

[10] Chuang, Ming-Chin, and Meng Chang Chen. "*An anonymous multi-server authenticated keyagreement scheme based on trust computing using smart cards and biometrics.*" Expert Systems withApplications 41.4 (2014): 1411-1418.