Regular Paper

Communications of the CCISA
Vol. 30 No. 4 Nov. 2024

基於後量子密碼學之醫療資訊安全系統設計

蔡國裕 [1*]、林子煒 [2]、尤婕蓉 [3]、林玟欣 [4]
[1, 3, 4] 逢甲大學資訊工程學系、[2] 逢甲大學創能學院、[2] 逢甲大學資訊總處資訊安全中心
[1] kytsai@fcu.edu.tw、[2] tweilin@fcu.edu.tw、[3] d1051210@o365.fcu.edu.tw、
[4] d1104427@o365.fcu.edu.tw

摘要

近年來，受疫情影響，醫療領域被迫加速數位轉型，各醫療院所也因此推動系統智慧化，提升醫療服務品質。然而，近期多起資安事件暴露出系統漏洞，包括工作站遭攻擊者入侵、內部資料被竄改，嚴重威脅病患隱私與健康安全。此外，隨著量子電腦的興起，現行的加密機制可能無法抵禦其強大的計算能力。本研究採用後量子密碼學 (Post-Quantum Cryptography, PQC) 中的網格密碼學 (Lattice-based Cryptography) 設計並實作身分鑑別與金鑰交換機制。該機制利用使用者的身分識別碼與自設通行碼產生公私鑰，無需儲存私鑰，從而降低金鑰被竊取的風險。此外，本方法還可實現資料機密性、會議金鑰確認、使用者免存金鑰、雙向身分鑑別，並利用醫療物聯網 (Internet of Healthcare Things, IoHT) 進行定期身分鑑別與抗量子攻擊分析等功能。

關鍵詞：醫療資訊安全、後量子密碼學、網格密碼學、醫療物聯網

* 通訊作者 (Corresponding author.)

Regular Paper

Communications of the CCISA
Vol. 30 No. 4 Nov. 2024

Design a Secure Post-Quantum Cryptography-Based Medical Information System

Kuo-Yu Tsai[1*], Tzu-Wei Lin[2], Jie-Rong You[3], Wen-Xin Lin[4]
[1, 3, 4]Department of Information Engineering and Computer Science, Feng Chia University, Taiwan, [2]i. School, Feng Chia University, Taiwan, [2]Information Security Office, Office of Information Technology, Feng Chia University, Taiwan
[1]kytsai@fcu.edu.tw, [2]tweilin@fcu.edu.tw, [3]d1051210@o365.fcu.edu.tw, [4]d1104427@o365.fcu.edu.tw

Abstract

Medical and healthcare sectors have been doing digital transformation recently, and COVID-19 accelerated the progress. Digital transformation helps medical and healthcare institutes improve quality of services. However, cyber security threats follow because of vulnerabilities of information systems, such as data tempering, invasion, etc., and not only privacy but life of patient will be in danger. Moreover, modern cryptosystems nowadays may not be able to resist attacks from quantum computers in the future. Proposed scheme applies lattice-based cryptography, one of the post-quantum cryptography mechanisms, to achieve identity authentication and key exchange mechanism. Proposed scheme generates public and private key using identifier and password of users, and users do not have to store private key to reduce risk of key stolen. Proposed scheme achieves security features, such as confidentiality, session key confirmation, mutual authentication, key storing-free, periodically mutual authentication of devices of Internet of Healthcare Things, and resisting attacks from quantum computers.

Keywords: Medical information system, post-quantum cryptography, lattice-based cryptography, Internet of Healthcare Things

壹、前言

隨著資訊技術的進步，已進入物聯網 (Internet of Things，以下簡稱為 IoT) 時代，此技術正改變許多產業及工作領域的運作模式。IoT 透過網路將各種設備與傳感器連接，實現資料的收集與交換，從而達到自動化與智慧化管理。在醫療領域，結合 IoT 技術的醫療物聯網 (Internet of Healthcare Things，以下簡稱為 IoHT) 已成為提升醫療效率的重要工具 [8]。IoHT 技術能夠透過網路測量、傳輸並讀取病患的生理數據，例如護理人員使用推車電腦讀取病歷，或透過智慧血壓計測量血壓並將數據回傳至伺服器。然而，便利性也帶來資安風險。醫療機構儲存大量敏感資料，包括儀器測量數據、藥物資訊、醫療人員資料及病患個人資訊。如果這些資料未經妥善管理，將可能威脅病患的就醫權益，甚至危及生命安全。

近年來，醫療機構遭受攻擊的事件頻繁發生。2017 年，新北市三峽區的恩主公醫院曾遭遇 WannaCry 勒索病毒攻擊 [13]；去年，美國政府資助的牙科及口腔醫療保險服務系統遭受嚴重勒索攻擊，導致近 900 萬名病患的個人資訊外洩 [10]。這些事件突顯加強資訊保護的迫切性。儘管醫療機構積極構建資訊安全防護系統，IoHT 設備因資源有限且防護不足，仍然容易成為攻擊目標。尤其是在傳輸病患敏感資訊時，若缺乏適當的身分鑑別與存取權限管理，這些設備將更容易受到攻擊者的侵害。

再者，隨著量子電腦技術的逐步成熟，傳統加密方法如 RSA、Diffie-Hellman、橢圓曲線密碼系統的安全性正面臨挑戰，因為量子電腦強大的計算能力可能破解這些加密技術。為應對這一威脅，後量子密碼學 (Post-Quantum Cryptography，以下簡稱為 PQC) 逐漸成為研究的焦點。與現有加密技術相比，PQC 具備更強的安全性，能在現有計算機上運行，並具備抵禦量子電腦分析的能力。

本研究針對醫療領域的資訊安全問題，提出應用 PQC 技術建構能抵禦量子攻擊的安全機制。此機制旨在保護 IoHT 設備的資料傳輸的病患個資，並強化身分鑑別機制，確保醫療人員擁有合法的資料存取權限，防止攻擊者利用量子電腦破解 IoHT 設備的敏感資訊或醫療資訊系統中的機密資料。本協定可有效防止身分冒用與非法資料洩露，進而保障病患資料與隱私的安全。

貳、文獻探討

本章針對醫療資訊系統安全、後量子密碼學、網格密碼學進行探討。

2.1 醫療資訊系統安全

隨著資訊科技的進展，無論是 5G/6G 網路抑或是 IoT，皆促使醫療資訊系統不斷

進步，譬如電子健康病歷 (Electronic Health Record，以下簡稱為 EHR) 的發展。EHR 是一種電子化的健康紀錄系統，用於集中管理與儲存患者的醫療及健康相關資訊，取代傳統的紙本病歷，提供有效、便捷且安全的方式記錄、分享及存取患者的醫療數據。2003 年，學者 Wang 等人進行一項針對電子健康病歷的成本效益分析，結果顯示 EHR 系統的使用不僅可以降低醫療機構的營運成本，還能提升醫療服務品質與效率 [11]。然而，現今醫療資訊系統亦帶來諸多挑戰，包括資料管理、即時監控、系統架構等，而這些挑戰皆會影響醫療照護品質 [5][8][9]。於此同時，醫療資訊系統資料隱私安全相關議題也受到重視，而醫療資訊系統結合 IoT 的相關應用與安全議題，更是引起學術與實務的關注 [1][3][4][5]。

現今的醫療資訊環境中，病人越來越有意願使用穿戴式裝置進行自我健康管理，諸如智慧手錶、智慧手環等，此類穿戴式裝置被稱為 IoHT 設備。IoHT 設備不僅幫助使用者進行自我健康管理，亦可以傳送生理監測資料至合作的醫療院所，醫療人員可藉此追蹤與監控使用者的身體健康狀況。在 IoHT 環境中所傳送的資料，對使用者而言是機敏資料，因此如何維護 IoHT 環境的安全性成為極其重要的議題。

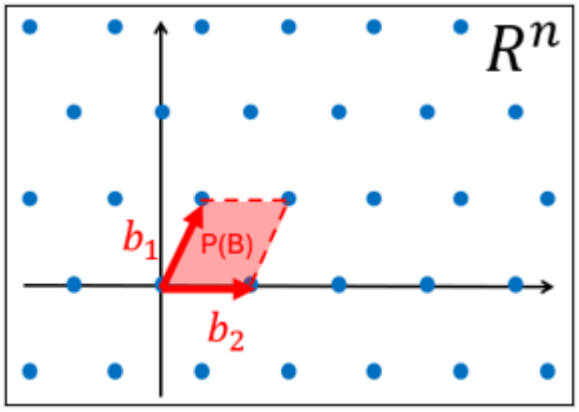
2.2 後量子密碼學

量子電腦的發展將會對資訊安全的維護帶來重大挑戰。根據 IBM 最新公告，預計在 2025 年實現超過 4000 量子位元的量子電腦 [12]，密碼學家因此開始關注其潛在風險。現行加密方法如 RSA、Diffie-Hellman、橢圓曲線密碼系統皆可能會被量子電腦使用 Shor 演算法破解。為了應對量子電腦的威脅，PQC 被視為可以抵擋量子電腦的攻擊而受到重視。學術界已深入研究 PQC 領域，並於 2006 年舉辦了首次後量子密碼學大會 (PQCrypto)。PQC 逐漸成為學術界的焦點，吸引許多研究機構投入該領域的研究 [6]。

PQC 因難以被量子電腦破解，能在現有計算機上運行，且可實作公開金鑰系統與數位簽章系統，具有實作上的便利性 [6]。PQC 可分為網格密碼學 (Lattice-Based Cryptography)、編碼密碼學 (Code-Based Cryptography)、多變數密碼學 (Multivariate Cryptography)、雜湊密碼學 (Hash-Based Cryptography) 及超奇異橢圓曲線同源密碼學 (Supersingular Elliptic Curve Isogeny Cryptography)。在量子計算威脅下，PQC 為資訊安全提供了比傳統密碼學演算法更強的保障，並能為各行各業構建更可靠的安全系統 [6]。

2.3 網格密碼學

網格密碼學是基於尋找特定向量的數學難題，可應用於產生公私鑰、進行身分鑑別與數位簽章。與其他加密方法相比，網格密碼學所產生的金鑰相對較短，特別適合用於資源有限的 IoT 設備 [7]。其定義為在 n 維空間中，透過 n 個基向量的任意線性組合形成的點的集合，這些點具有規律性且離散分佈，如圖一所示。其數學定義如下：



圖一：Lattice 圖示

- 基向量組合

$$B = \{b_1, b_2, b_3, \ldots, b_n\} \quad (1)$$

- Lattice

$$L = L(B) = \{\sum_{i=1}^{n} c_i b_i : c_i \in Z\} \quad (2)$$

- 基向量所圍出的空間

$$P(B) = B \cdot [-\frac{1}{2}, \frac{1}{2})^n = \{\sum_{i=1}^{n} \alpha_i \beta_i : -\frac{1}{2} \le \alpha_i \le \frac{1}{2}\} \quad (3)$$

- 每個點 (v) 與其對應的 $P(B)$ 組成此 n 維空間

$$R^n = \bigcup_{v \in L} (v + P(B)) \quad (4)$$

網格密碼學的安全性建立在矩陣與向量相關的數學難題之上，透過尋找特定向量或點來實現加解密過程。學者 Chaudhary 等人對現有的基於網格的公鑰加密系統 (Lattice-based Public Key Cryptosystem，LB-PKC) 進行探討 [2]，其中包括本研究使用的容錯學習問題 (Learning With Errors，以下簡稱為 LWE) 及其衍生的加解密與身分鑑別技術。LWE 透過增加干擾值提升計算困難度，藉以提高安全性，取 n 維方陣 $A \in Z_q^{n \times n}$，n 維向量 $(s, e, B(s, e, B \in Z_q^n))$，其中 e 為一極小值作為干擾值，最後將 (A, B) 設為公鑰，s 設為私鑰。其公式如下：

$$B = A \times s + e \quad (5)$$

學者 Chaudhary 等人研究這些技術的安全性，並評估其在 IoT 設備上運行的可行性與性能表現 [2]。

參、本研究提出之協定

本研究的協定共分為五個階段：初始化階段、使用者註冊階段、IoHT 設備註冊階段、使用者登入階段及 IoHT 設備鑑別階段。在用戶端，使用者負責註冊並登入系統以

查詢個人病歷資料；在設備端，IoHT 設備需進行註冊，並與醫院伺服器進行雙向鑑別與資料傳輸。符號說明如表一所示。

表一: 符號表

符號	定義
A_X	X 產生的矩陣，為公開參數
e_X	X 產生的向量，為一極小秘密參數
B_X	X 產生的向量，為公開參數
U	使用者
S	伺服器
I	IoHT
PK_X	X 的公鑰
SK_X	X 的私鑰
K_{XY}	X 與 Y 的會議金鑰
ID_X	X 的身分識別碼
PW_X	X 的通行碼
r_X	X 產生的隨機亂數

3.1 初始化階段

伺服器 S 需要使用身分識別碼 ID_S 與隨機產生的通行碼 PW_S，透過雜湊函數產生公私鑰並儲存於資料庫中，以便後續對使用者 U 與 IoHT 設備 I 進行身分鑑別及保護訊息傳遞。本階段伺服器 S 執行步驟如下。

步驟一：隨機產生通行碼 PW_S 並計算 SK_S。

$$SK_S = Hash(ID_S||PW_S) \tag{6}$$

步驟二：隨機產生亂數e_S並計算 (B_S, PK_S) 後，儲存 (PK_S, SK_S)。

$$B_S = ID_S \times SK_S + e_S \tag{7}$$

$$PK_S = (ID_S, B_S) \tag{8}$$

3.2 使用者註冊階段

使用者 U 在醫療資訊系統的註冊介面輸入基本資料與身分識別碼 ID_U，並自行設定通行碼 PW_U。伺服器 S 根據使用者 U 輸入的 ID_U 與通行碼 PW_U，經由雜湊函數產生公私鑰，並將公鑰儲存於資料庫中。註冊完成後，使用者 U 可使用身分識別碼 ID_U 與通行碼 PW_U 登入 EHR，查閱個人病歷資料。相關流程如圖二所示。詳細步驟如下。

步驟一：使用者 U 將 (ID_U, PW_U) 傳送給伺服器 S。

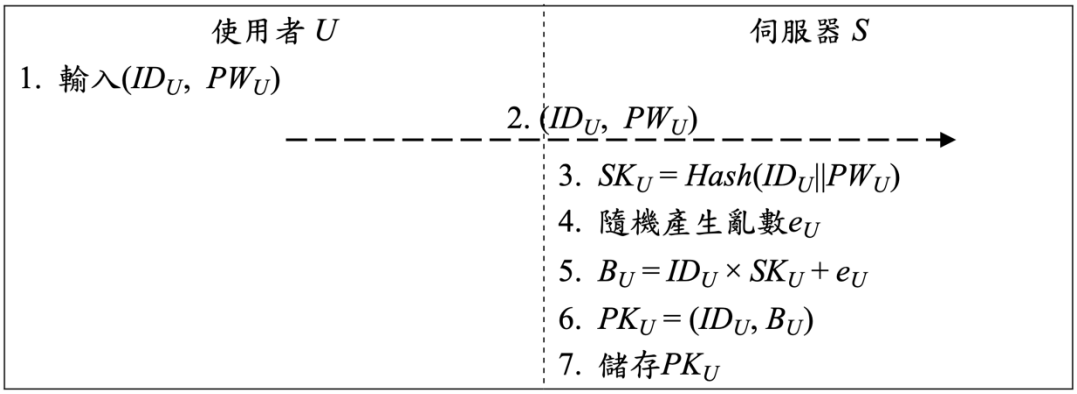
步驟二：伺服器 S 收到 (ID_U, PW_U) 後計算 SK_U。

$$SK_U = Hash(ID_U||PW_U) \tag{9}$$

步驟三：伺服器 S 隨機產生亂數e_U並計算 (B_U, PK_U) 後，儲存 PK_U。

$$B_U = ID_U \times SK_U + e_U \tag{10}$$

$$PK_U = (ID_U, B_U) \tag{11}$$



圖二：使用者註冊階段

3.3 IoHT 設備註冊階段

IoHT 設備 I 隨機產生通行碼 PW_I 並連同身分識別碼 ID_I 傳送至伺服器 S，伺服器 S 收到後透過雜湊函數產生公私鑰，將公鑰儲存於資料庫，並將私鑰回傳至 IoHT 設備 I，以便後續進行與伺服器 S 的身分鑑別。相關流程如圖三所示。詳細步驟如下。

步驟一：IoHT 設備 I 隨機產生通行碼 PW_I 後將 (ID_I, PW_I) 傳送給伺服器 S。

步驟二：伺服器 S 收到 (ID_I, PW_I) 後計算 SK_I。

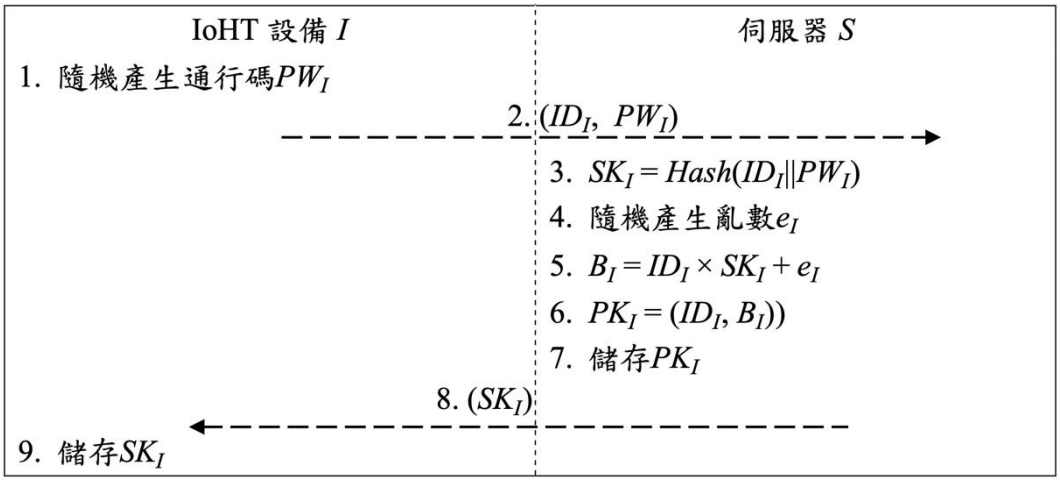
$$SK_I = Hash(ID_I||PW_I) \tag{12}$$

步驟三：伺服器 S 隨機產生亂數 e_I 並計算 (B_I, PK_I)。

$$B_I = ID_I \times SK_I + e_I \tag{13}$$

$$PK_I = (ID_I, B_I) \tag{14}$$

步驟四：伺服器 S 傳送 SK_I 給 IoHT 設備 I 儲存，伺服器 S 儲存 PK_I。



圖三：IoHT 設備註冊階段

3.4 使用者登入階段

使用者 U 登入時，首先輸入身分識別碼 ID_U 與通行碼 PW_U 並計算私鑰 SK_U，接著將ID_U使用伺服器 S 的公鑰 PK_S 加密後傳送至伺服器 S 進行驗證。伺服器 S 解密並確認無誤後，產生隨機亂數 r_S 與會議金鑰 K_{SU}，並使用使用者的公鑰 PK_U 加密後傳送給使用者 U。使用者 U 使用私鑰 SK_U 解密，得到隨機亂數 r_S 與會議金鑰 K_{SU}。然後，將隨機亂數 r_S 經過雜湊函數計算出雜湊值 $Hash(r_S)$ 並回傳伺服器 S。伺服器 S 使用隨機亂數 r_S 計算雜湊值，並與使用者 U 回傳的雜湊值 r_S 比對，若相同，則鑑別成功。相關流程如圖四所示。詳細步驟如下。

步驟一：使用者 U 輸入 (ID_U, PW_U) 後計算 SK_U 如算式(9)與 C_U，並將 C_U 傳送給伺服器 S。

$$C_U = PK_S(ID_U) \tag{15}$$

步驟二：伺服器 S 收到 C_U 後解密得到 ID_U' 並檢查。

$$ID_U' = SK_S(C_U) \tag{16}$$

步驟三：伺服器 S 隨機產生亂數 r_S 與會議金鑰 K_{SU}，並計算 C_S 後傳給使用者 U。

$$C_S = PK_U(r_S||K_{SU}) \tag{17}$$

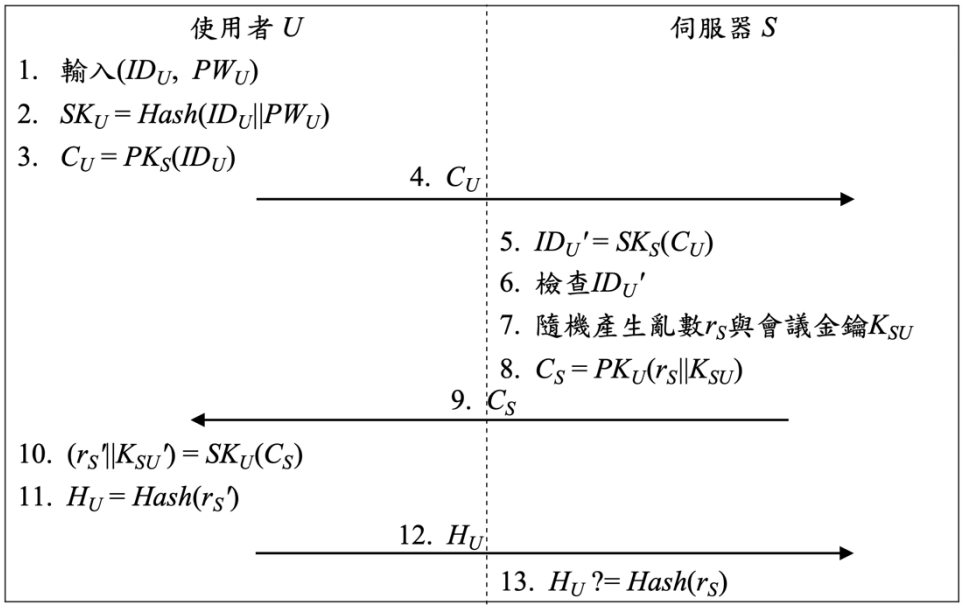
步驟四：使用者 U 收到 C_S 後解密得到 (r_S', K_{SU}')，並計算 H_U 後傳送給伺服器 S。

$$(r_S'||K_{SU}') = SK_U(C_S) \tag{18}$$

$$H_U = Hash(r_S') \tag{19}$$

步驟五：伺服器 S 收到 H_U 後驗證 H_U。若相同，則鑑別成功。

$$H_U \stackrel{?}{=} Hash(r_S) \tag{20}$$



圖四：使用者登入階段

3.5 IoHT 設備鑑別階段

IoHT 設備 I 註冊完成後，會定期與伺服器 S 進行雙向身分鑑別，以防止 IoHT 設備 I 或醫院伺服器 S 遭到冒用。首先，伺服器 S 對 IoHT 設備進行身分鑑別，伺服器 S 產生隨機亂數與會議金鑰，並將兩者使用 IoHT 設備 I 的公鑰加密後傳送至 IoHT 設備 I。IoHT 設備 I 用私鑰解密，獲得隨機亂數與會議金鑰，隨後將隨機亂數透過雜湊函數產生雜湊值，並隨機產生新的亂數。然後，IoHT 設備 I 將新的隨機亂數與雜湊值用伺服器的公鑰加密後傳送回伺服器。伺服器解密後，獲得雜湊值與 IoHT 設備 I 產生的隨機亂數，並將產生的隨機亂數進行雜湊，兩個雜湊值比對相同則驗證透過。接著，IoHT 對伺服器進行身分鑑別。伺服器 S 將 IoHT 設備 I 傳送的隨機亂數進行雜湊計算並傳回 IoHT 設備 I。IoHT 設備 I 同時對自己的驗證碼產生雜湊值，兩者進行比對，若相同，則鑑別成功。相關流程如圖五所示。詳細步驟如下。

步驟一：伺服器 S 隨機產生亂數 r_S 與會議金鑰 K_{SI}，並計算 C_S 後傳給 IoHT 設備 I。

$$C_S = PK_I(r_S||K_{SI}) \tag{21}$$

步驟二：IoHT 設備 I 收到 C_S 後解密得到 (r_S', K_{SI}')。

$$(r_S'||K_{SI}') = SK_I(C_S) \tag{22}$$

步驟三：IoHT 設備 I 隨機產生亂數 r_I、計算 H_I 與 C_I，並傳送 C_I 給伺服器 S。

$$H_I = Hash(r_S') \tag{23}$$

$$C_I = PK_S(r_I||H_I) \tag{24}$$

步驟四：伺服器 S 收到 C_I 後解密得到 (r_I', H_I') 並驗證 H_I'。

$$(r_I'||H_I') = SK_S(C_I) \tag{25}$$

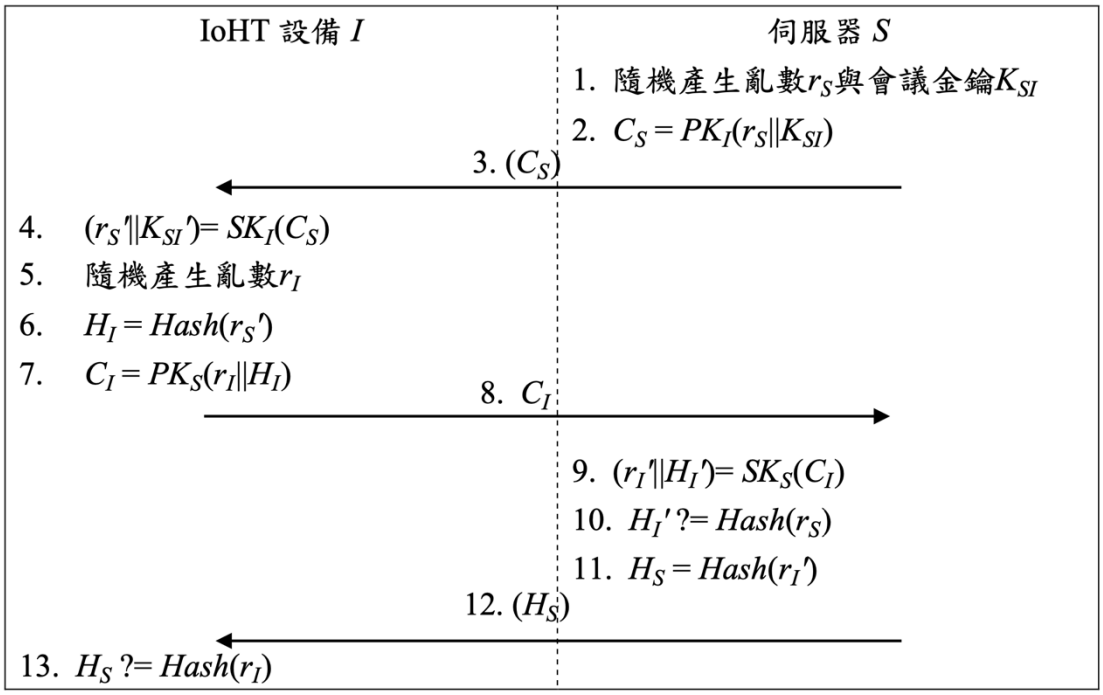
$$H_I' \text{?=} Hash(r_S) \tag{26}$$

步驟五：伺服器 S 計算 H_S 後傳給 IoHT 設備 I。

$$H_S = Hash(r_I') \tag{27}$$

步驟六：IoHT 設備 I 收到 H_S 後驗證 H_S。若相同，則鑑別成功。

$$H_S \text{?=} Hash(r_I) \tag{28}$$



圖五：IoHT 設備鑑別階段

肆、安全性分析

4.1 機密性

在使用者登入階段中，使用者 U 使用公鑰PK_S加密使用者的身分識別碼ID_U後傳送C_U至伺服器 S，而伺服器驗證成功後，隨機產生亂數r_S與會議金鑰K_{SU}，並使用使用者的公鑰PK_U加密後，將C_S傳送給使用者。當攻擊者攔截所有傳送訊息時，如果攻擊者欲解密取得ID_U 、r_S或K_{SU}時，由於攻擊者沒有私鑰，則攻擊者無法在多項式時間恢復加密的資訊。在 IoHT 設備 I 與伺服器 S 進行雙向身分鑑別流程中，伺服器 S 利用 IoHT 設備 I 之公鑰PK_I加密產生C_S，當 IoHT 設備 I 驗證成功後，利用伺服器 S 之公鑰PK_S加密產生C_I。當攻擊者攔截所有傳送訊息時，如果攻擊者欲解密取得r_I 、r_S或K_{SI}時，由於攻擊者沒有私鑰，則攻擊者無法在多項式時間恢復加密的資訊。

4.2 會議金鑰確認

在身分鑑別過程中，所傳送的資料包含會議金鑰。在使用者 U 登入過程中，使用者 U 回傳H_U，而伺服器 S 經由H_U ?= $Hash(r_S)$ 確認使用者 U 所接收的會議金鑰K_{SU}是正確。在 IoHT 設備 I 與伺服器 S 進行雙向身分鑑別鑑別流程中，IoHT 設備 I 回傳C_I，伺服器 S 解密經由H_I' ?= $Hash(r_S)$ 確認 IoHT 設備 I 所接收的會議金鑰K_{SI}是正確。

4.3 使用者免存私鑰

金鑰產生過程採用雜湊函數，使用者 U 輸入身分識別碼ID_U與通行碼PW_U，進而產生私鑰$SK_U = Hash(ID_U||PW_U)$，因此使用者 U 不需要儲存私鑰，只需記得自己所設定的(ID_U, PW_U)，提高私鑰的安全性與使用者的方便性。

4.4 雙向身分鑑別

IoHT 設備鑑別階段採用雙向身分鑑別機制，確保 IoHT 設備 I 與醫院伺服器 S 間的通訊安全。IoHT 設備 I 回傳C_I給伺服器，伺服器 S 解密取得(r_I', H_I') 並驗證H_I'確認 IoHT 設備 I 的身分；而伺服器 S 回傳H_S，IoHT 設備 I 經由H_S ?= $Hash(r_I)$ 確認伺服器 S 的身分。

4.5 IoHT 定期身分鑑別

所設計的協定中，IoHT 設備 I 可以定期與伺服器 S 進行身分鑑別，以持續確保系統的安全性。此動態鑑別方法可提升系統抵禦持續性威脅的能力。

4.6 抗量子分析

所設計的協定採用網格密碼學，不僅可應對當前的安全需求，更為未來可能出現的量子計算攻擊提供強而有力的防禦機制。在金鑰產生、加密及解密過程中，皆為基於網格密碼學的困難度，確保即使在量子計算普及後，系統的核心加密機制仍能保有安全性。

伍、結論

本研究針對醫療領域中數位化轉型所面臨的資安挑戰，提出一套基於 PQC 的解決

方案。探討隨著 IoHT 設備的普及，在資料保護方面所面臨的安全議題。採用 PQC 中的網格密碼學，設計並實作能夠有效抵抗量子電腦分析的安全協定。的研究成果主要包括兩個方面：用戶端及設備端。在用戶端，本研究利用雜湊函數產生公私鑰並進行身分鑑別機制，使用者不需要儲存私鑰。為了確保 IoHT 設備端，設計雙向身分鑑別機制，防止攻擊者假冒 IoHT 設備或伺服器。

[誌謝]

本研究部份成果由國科會 (計畫編號 MOST 112-2634-F-005-001-MBK 與 MOST 113-2634-F005-001-MBK) 支持。

參考文獻

[1] S. J. Bhasha and P. Sunita, “An IoT-based body area network in medical care system: Related challenges and issues,” *International Journal of Innovative Technology and Exploring Engineering*, 2019.

[2] R. Chaudhary, G. S. Aujla, N. Kumar, and S. Zeadally, “Lattice-based public key cryptosystem for Internet of things environment: Challenges and solutions,” *IEEE Internet Things Journal*, vol. 6, no. 3, pp. 4897–4909, 2019.

[3] S. A. Chaudhry et al., “An anonymous device to device access control based on secure certificate for Internet of medical things systems,” *Sustainable Cities and Society*, vol. 75, p. 103322, 2021.

[4] S. A. Chaudhry et al., “A lightweight authentication scheme for 6G-IoT enabled maritime transport system,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 2, pp. 2401–2410, 2023.

[5] M. Chen, J. Yang, J. Zhou, Y. Hao, J. Zhang, and C.-H. Youn, “5G-smart diabetes: Toward personalized diabetes diagnosis with healthcare big data clouds,” *IEEE Communications Magazine*, vol. 56, no. 4, pp. 16–23, 2018.

[6] Y.-J. Chen, C.-L. Hsu, T.-W. Lin, and J.-S. Lee, “Design and evaluation of device authentication and secure communication system with PQC for AIoT environments,” *Electronics* (*Basel*), vol. 13, no. 8, 2024.

[7] T. M. Fernández-Caramés, “From pre-quantum to post-quantum IoT security: A survey on quantum-resistant cryptosystems for the Internet of things,” *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6457–6480, 2020.

[8] C.-L. Hsu and T.-W. Lin, “ID-based proxy signature with key-insulated scheme for

portable healthcare devices in 5G-IoHT," *Journal of Internet Technology*, vol. 9, 2024.
[9] T.-W. Lin and C.-L. Hsu, "FAIDM for medical privacy protection in 5G telemedicine systems," *Applied Sciences*, vol. 11, no. 3, 2021.
[10] B. Toulas, "MCNA dental data breach impacts 8.9 million people after ransomware attack," *Bleeping Computer*. URL: https://www.bleepingcomputer.com/news/security/mcna-dental-data-breach-impacts-89-million-people-after-ransomware-attack/ (存取時間：2024/11/08)
[11] S. J. Wang et al., "A cost-benefit analysis of electronic medical records in primary care," *The American Journal of Medicine*, vol. 114, no. 5, pp. 397–403, 2003.
[12] IBM，"IBM 公布最新實用量子發展路線圖：2025 年推出超過 4,000 量子位的系統"，URL: https://taiwan.newsroom.ibm.com/2022-05-10-IBM-2025-4,000 (存取時間：2024/11/08)
[13] ETtoday 新聞雲，"恩主公醫院淪陷！「勒索病毒」入侵醫療推車電腦：檔案已鎖碼"，URL: https://www.ettoday.net/news/20170514/924318.htm (存取時間：2024/11/08)

[作者簡介]

蔡國裕先生 2009 年畢業於國立臺灣科技大學資訊管理系博士班，現於逢甲大學資訊工程學系擔任副教授，並兼任逢甲大學創能學院資訊學中心主任。主要研究領域為區塊鏈應用、物聯網應用與安全、行動裝置應用開發、電子商務應用，目前主要研究方向為電子貨幣、智能合約、物聯網之遠端居家照護應用、Android App 保護等。近年執行之相關計畫與物聯網及長照應用相關，希冀能經由資通訊技術之發展，協助解決未來長照發展可能面臨之相關議題。

林子煒先生分別於 2013 年與 2021 年取得長庚大學資訊管理系碩士學位與企業管理研究所博士班博士學位，自 2021 年 8 月起擔任逢甲大學創能學院助理教授，並於 2022 年 8 月起兼任逢甲大學資訊總處資訊安全中心主任。研究領域包括資訊安全、網路安全、密碼學、物聯網應用安全、雲端運算應用安全、醫療資訊系統、健康照護系統、行動商務、人工智慧等。

尤婕蓉小姐與林玟欣小姐目前皆為逢甲大學資訊工程學系學生，主要接觸與研究領域為後量子密碼學，並應用於醫療資訊安全領域以及遠端照護系統安全保護。