【19】中華民國　　【12】專利公報　（B）

【11】證書號數：I940394
【45】公告日： 中華民國 115 (2026) 年 09 月 21 日
【51】Int. Cl.：　*H04L9/00 (2022.01)*　*H04L9/32 (2006.01)*
H04L9/08 (2006.01)　*G06F21/33 (2013.01)*
發明　全 8 頁

【54】名　稱：後量子密碼身分認證系統以及後量子密碼身分認證方法
【21】申請案號：114144082　【22】申請日： 中華民國 114 (2025) 年 11 月 12 日
【72】發 明 人： 張宏昌 (TW) CHANG, HUNG-CHANG；簡志軒 (TW) JIAN, JHIH-SYUAN；
金慶柏 (TW) CHIN, CHING-PO
【71】申 請 人： 華碩電腦股份有限公司　ASUSTEK COMPUTER INC.
臺北市北投區立德路 15 號
【74】代 理 人： 李長銘
【56】參考文獻：

CN	116996229A	US	2024/0380611A1
WO	2021/128988A1	WO	2025/157070A1

審查人員：賴文能

【57】申請專利範圍

1. 一種後量子密碼身分認證系統，包含:
一使用者終端，包含:
一使用者介面模組，適於啟動一註冊程序並接收身分識別資訊；
一後量子密碼運算模組，電性耦接於該使用者介面模組，適於產生對應於該身分識別資訊之一第一公鑰、一第一私鑰、一第二公鑰以及一第二私鑰，其中，該第一私鑰對應於該第一公鑰，該第二私鑰對應於該第二公鑰；
一安全金鑰儲存單元，電性耦接於該後量子密碼運算模組，適於儲存該第一私鑰以及該第二私鑰；
一註冊請求產生模組，電性耦接於該使用者介面模組以及該後量子密碼運算模組，適於將該身分識別資訊、該第一公鑰以及該第二公鑰組織成一註冊請求訊息，其中，該後量子密碼運算模組使用該第一私鑰對該註冊請求訊息簽署，而產生一數位簽章；以及
一終端通訊模組，電性耦接於該註冊請求產生模組以及該後量子密碼運算模組，適於將該註冊請求訊息以及該數位簽章向外傳送；以及
一認證伺服器，通訊連接於該使用者終端，且包含:
一請求接收與分派模組，適於接收該註冊請求訊息以及該數位簽章；
一後量子密碼驗證模組，電性耦接於該請求接收與分派模組，適於利用該註冊請求訊息中之該第一公鑰驗證該數位簽章之有效性；
一後端資料庫；以及
一後端資料庫介面模組，電性耦接於該後量子密碼驗證模組以及該後端資料庫，適於在該數位簽章驗證有效時，將該註冊請求訊息中之該身分識別資訊關聯於該第一公鑰以及該第二公鑰，並將該第一公鑰以及該第二公鑰儲存於該後端資料庫；
其中，該第一公鑰以及該第一私鑰係用於身分認證，該第二公鑰以及該第二私鑰係用於執行一金鑰交換程序以產生一會話金鑰。
2. 如請求項 1 所述之後量子密碼身分認證系統，其中，該使用者終端係透過一安全通道通訊連接於該認證伺服器。

3. 如請求項 2 所述之後量子密碼身分認證系統，其中，該安全通道係利用傳輸層安全性協定(TLS)建立之一加密通道。
4. 如請求項 1 所述之後量子密碼身分認證系統，更包含一憑證頒發機構，通訊連接於該認證伺服器，且具有一簽章私鑰，該認證伺服器適於在該數位簽章驗證有效時向該憑證頒發機構提交一憑證簽署請求(CSR)，該憑證頒發機構適於因應該憑證簽署請求利用該簽章私鑰簽發一數位憑證並傳送至該認證伺服器，其中，該憑證簽署請求包含該第一公鑰以及該第二公鑰，該數位憑證包含該第一公鑰以及該第二公鑰。
5. 如請求項 4 所述之後量子密碼身分認證系統，其中，該數位憑證係儲存於該後端資料庫。
6. 如請求項 1 所述之後量子密碼身分認證系統，其中，該第一公鑰以及該第二公鑰係對應於不同之後量子密碼演算法。
7. 一種後量子密碼身分認證方法，適用於一後量子密碼身分認證系統，該後量子密碼身分認證系統包含一使用者終端以及一認證伺服器，該使用者終端包含一使用者介面模組、一後量子密碼運算模組、一安全金鑰儲存單元、一註冊請求產生模組以及一終端通訊模組，該認證伺服器係通訊連接於該使用者終端，且包含一請求接收與分派模組、一後量子密碼驗證模組、一後端資料庫介面模組以及一後端資料庫，該後量子密碼身分認證方法包含:
利用該使用者介面模組，啟動一註冊程序並接收身分識別資訊；
利用該後量子密碼運算模組，產生對應於該身分識別資訊之一第一公鑰、一第一私鑰、一第二公鑰以及一第二私鑰，其中，該第一私鑰對應於該第一公鑰，該第二私鑰對應於該第二公鑰；
利用該安全金鑰儲存單元，儲存該第一私鑰以及該第二私鑰；
利用該註冊請求產生模組，將該身分識別資訊、該第一公鑰以及該第二公鑰組織成一註冊請求訊息；
利用該後量子密碼運算模組使用該第一私鑰對該註冊請求訊息簽署，而產生一數位簽章；
利用該終端通訊模組，將該註冊請求訊息以及該數位簽章傳送至該認證伺服器；
利用該請求接收與分派模組，接收該註冊請求訊息以及該數位簽章；
利用該後量子密碼驗證模組，利用該註冊請求訊息中之該第一公鑰驗證該數位簽章之有效性；以及
利用該後端資料庫介面模組，在該數位簽章驗證有效時，將該註冊請求訊息中之該身分識別資訊關聯於該第一公鑰以及該第二公鑰，並將該第一公鑰以及該第二公鑰儲存於該後端資料庫；
其中，該第一公鑰以及該第一私鑰係用於身分認證，該第二公鑰以及該第二私鑰係用於執行一金鑰交換程序以產生一會話金鑰。
8. 如請求項 7 所述之後量子密碼身分認證方法，其中，利用該終端通訊模組，將該註冊請求訊息以及該數位簽章傳送至該認證伺服器之步驟包含利用該終端通訊模組建立一安全通道通訊連接於該認證伺服器。
9. 如請求項 8 所述之後量子密碼身分認證方法，其中，該安全通道係利用傳輸層安全性協定(TLS)建立之一加密通道。
10. 如請求項 7 所述之後量子密碼身分認證方法，其中，該後量子密碼身分認證系統更包含一憑證頒發機構，該憑證頒發機構具有一簽章私鑰，該後量子密碼身分認證方法更包含:

利用該認證伺服器，在該數位簽章驗證有效時，向該憑證頒發機構提交一憑證簽署請求(CSR)；以及

因應該憑證簽署請求，利用該憑證頒發機構，利用該簽章私鑰簽發一數位憑證並傳送至該認證伺服器；

其中，該憑證簽署請求包含該第一公鑰以及該第二公鑰，該數位憑證包含該第一公鑰以及該第二公鑰。

11. 如請求項 10 所述之後量子密碼身分認證方法，更包含利用該後端資料庫介面模組，將該數位憑證係儲存於該後端資料庫。

12. 如請求項 7 所述之後量子密碼身分認證系統，其中，該第一公鑰以及該第二公鑰係對應於不同之後量子密碼演算法。

13. 如請求項 7 所述之後量子密碼身分認證方法，其中，該後量子密碼身分認證系統更包含一伺服器通訊模組以及一會話管理模組，該後量子密碼身分認證方法更包含:

利用該使用者介面模組接收一身分識別符以產生一登入請求，該登入請求包含該身分識別符；

利用該終端通訊模組將該登入請求傳送至該認證伺服器；

利用該請求接收與分派模組接收該登入請求；

利用該後端資料庫介面模組，根據該登入請求中之該身分識別符於該後端資料庫中進行檢索；

若找到對應於該身分識別符之該第一公鑰以及該第二公鑰，利用該後量子密碼驗證模組產生一挑戰訊息，該挑戰訊息包含一挑戰值；

利用該伺服器通訊模組將該挑戰訊息傳送至該使用者終端；

利用該終端通訊模組接收該挑戰訊息，並利用該後量子密碼運算模組由該安全金鑰儲存單元讀取該第一私鑰；

利用該後量子密碼運算模組，使用該第一私鑰對該挑戰訊息進行簽署，而產生一數位簽章；

利用該使用者終端，將該數位簽章作為一認證回應傳送至該認證伺服器；

利用該後量子密碼驗證模組，使用對應於該身分識別符之該第一公鑰驗證該數位簽章對於該挑戰訊息的有效性；以及

若該數位簽章對於該挑戰訊息是有效的，利用該會話管理模組建立一認證會話。

14. 如請求項 13 所述之後量子密碼身分認證方法，其中，若該數位簽章對於該挑戰訊息是有效的，利用該會話管理模組建立該認證會話之步驟更包含:

使用該第二公鑰以及該第二私鑰啟動該金鑰交換程序，以產生該會話金鑰。

15. 如請求項 14 所述之後量子密碼身分認證方法，其中，使用該第二公鑰以及該第二私鑰啟動該金鑰交換程序以產生該會話金鑰之步驟包含:

利用該後量子密碼驗證模組，使用該第二公鑰產生一共享秘密以及對應於該共享秘密之一密文；

利用該認證伺服器將該密文傳送至該使用者終端；

利用該後量子密碼運算模組，使用該第二私鑰對該密文進行解封裝；以及

若解封裝成功，該使用者終端以及該認證伺服器依據該共享秘密，產生該會話金鑰。

16. 一種後量子密碼身分認證方法，適用於一後量子密碼身分認證系統，該後量子密碼身分認證系統包含一使用者終端以及一認證伺服器，該後量子密碼身分認證方法包含:

該使用者終端接收身分識別資訊；

該使用者終端利用至少一後量子密碼演算法產生對應於該身分識別資訊之一第一公鑰、一第一私鑰、一第二公鑰以及一第二私鑰，其中，該第一私鑰對應於該第一公鑰，該第二私鑰對應於該第二公鑰；

該使用者終端將該第一私鑰以及該第二私鑰儲存至一安全金鑰儲存單元；

該使用者終端將該身分識別資訊、該第一公鑰以及該第二公鑰組織成一註冊請求訊息傳送至該認證伺服器進行註冊；以及

該使用者終端以及該認證伺服器利用該第一公鑰以及該第一私鑰係進行身分認證，並利用該第二公鑰以及該第二私鑰執行一金鑰交換程序以產生一會話金鑰。

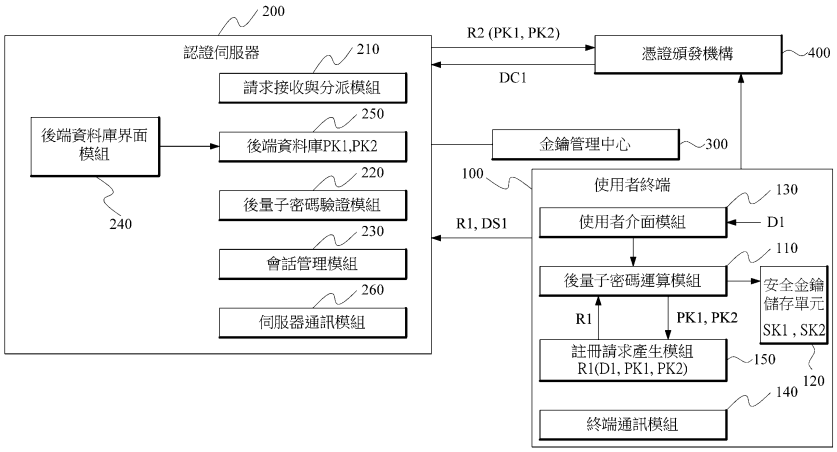
圖式簡單說明

第一圖係依據本案一實施例所提供之後量子密碼身分認證系統的架構示意圖；

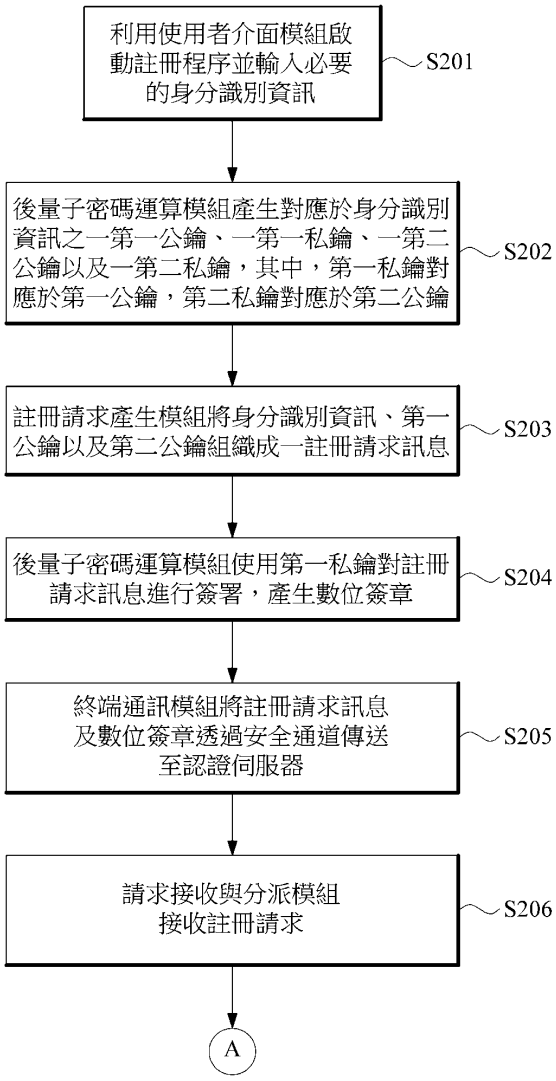
第二 A 與二 B 圖係依據本案一實施例所提供之後量子密碼身分認證方法之註冊階段的詳細步驟流程圖；

第三 A 與三 B 圖係依據本案一實施例所提供之後量子密碼身分認證方法之認證/登入階段的詳細步驟流程圖；以及

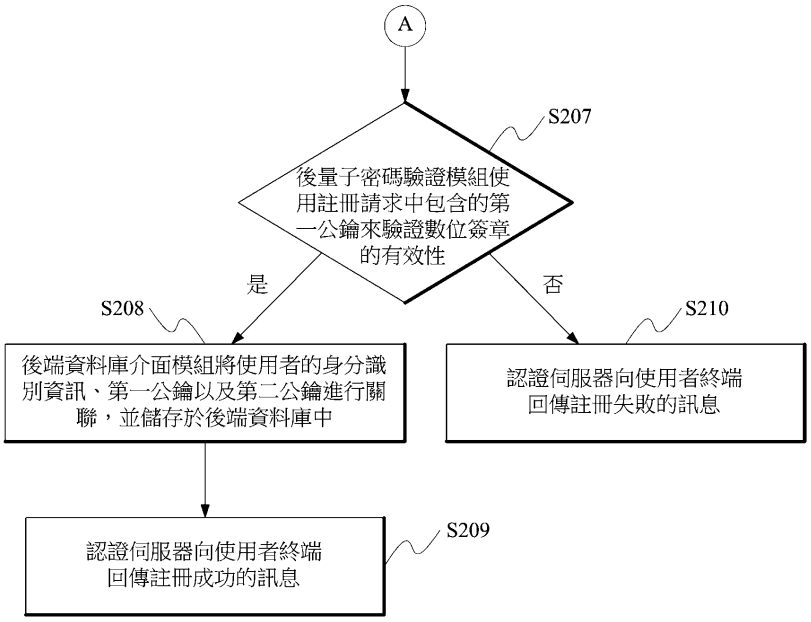
第四圖顯示依據本案一實施例所提供之後量子密碼數位憑證之簡化資料結構。



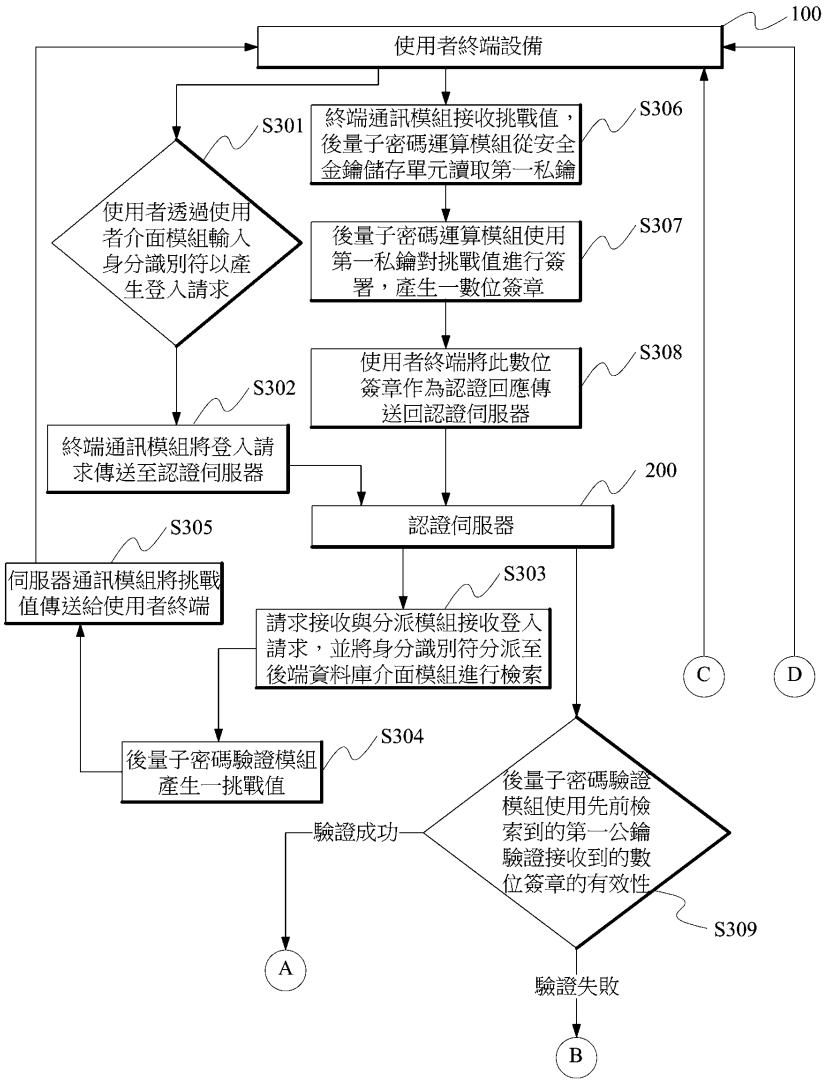
第一圖


利用使用者介面模組啟動註冊程序並輸入必要的身分識別資訊
S201
後量子密碼運算模組產生對應於身分識別資訊之一第一公鑰、一第一私鑰、一第二公鑰以及一第二私鑰，其中，第一私鑰對應於第一公鑰，第二私鑰對應於第二公鑰
S202
註冊請求產生模組將身分識別資訊、第一公鑰以及第二公鑰組織成一註冊請求訊息
S203
後量子密碼運算模組使用第一私鑰對註冊請求訊息進行簽署，產生數位簽章
S204
終端通訊模組將註冊請求訊息及數位簽章透過安全通道傳送至認證伺服器
S205
請求接收與分派模組接收註冊請求
S206
A

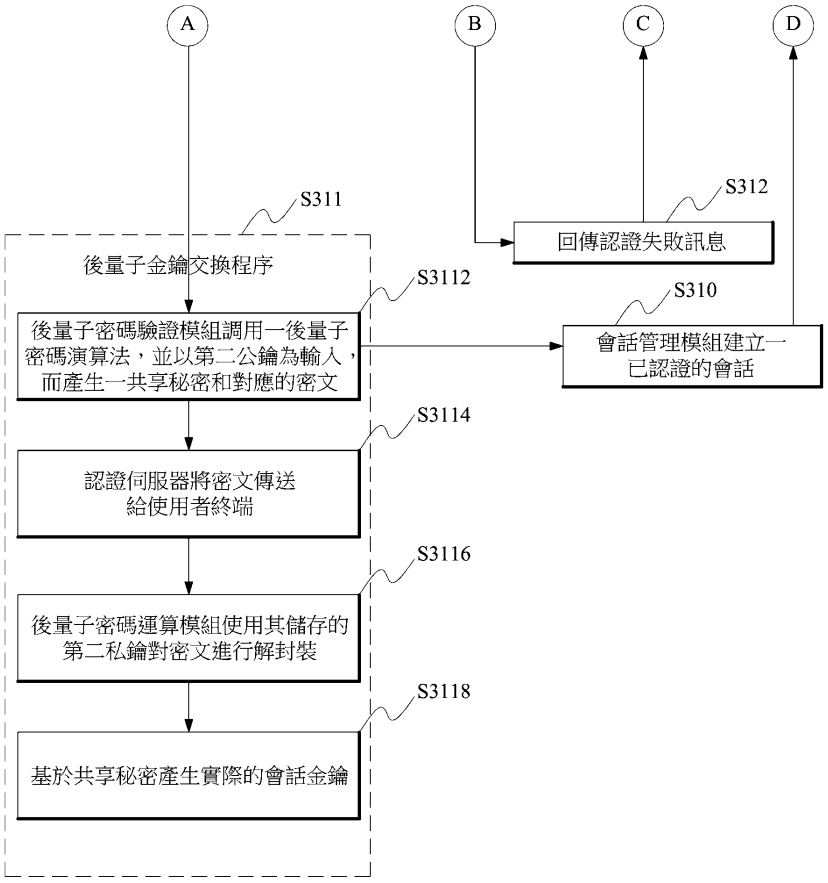
第二A圖


A
S207
後量子密碼驗證模組使用註冊請求中包含的第一公鑰來驗證數位簽章的有效性
是
否
S208
後端資料庫介面模組將使用者的身分識別資訊、第一公鑰以及第二公鑰進行關聯，並儲存於後端資料庫中
S210
認證伺服器向使用者終端回傳註冊失敗的訊息
S209
認證伺服器向使用者終端回傳註冊成功的訊息

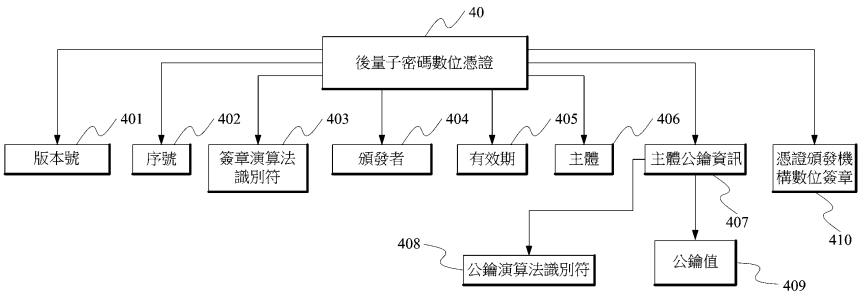
第二B圖


100
使用者終端設備
S301
使用者透過使用者介面模組輸入身分識別符以產生登入請求
S306
終端通訊模組接收挑戰值，後量子密碼運算模組從安全金鑰儲存單元讀取第一私鑰
S307
後量子密碼運算模組使用第一私鑰對挑戰值進行簽署，產生一數位簽章
S308
使用者終端將此數位簽章作為認證回應傳送回認證伺服器
S302
終端通訊模組將登入請求傳送至認證伺服器
200
認證伺服器
S305
伺服器通訊模組將挑戰值傳送給使用者終端
S303
請求接收與分派模組接收登入請求，並將身分識別符分派至後端資料庫介面模組進行檢索
C
D
S304
後量子密碼驗證模組產生一挑戰值
後量子密碼驗證模組使用先前檢索到的第一公鑰驗證接收到的數位簽章的有效性
S309
驗證成功
驗證失敗
A
B

第三A圖


A
B
C
D
S311
後量子金鑰交換程序
S3112
後量子密碼驗證模組調用一後量子密碼演算法，並以第二公鑰為輸入，而產生一共享秘密和對應的密文
S3114
認證伺服器將密文傳送給使用者終端
S3116
後量子密碼運算模組使用其儲存的第二私鑰對密文進行解封裝
S3118
基於共享秘密產生實際的會話金鑰
S312
回傳認證失敗訊息
S310
會話管理模組建立一已認證的會話

第三B圖


40
後量子密碼數位憑證
401
版本號
402
序號
403
簽章演算法識別符
404
頒發者
405
有效期
406
主體
主體公鑰資訊
憑證頒發機構數位簽章
407
408
公鑰演算法識別符
公鑰值
409
410

第四圖