【19】中華民國　　【12】專利公報　（U）

【11】證書號數：M574275
【45】公告日： 中華民國 108 (2019) 年 02 月 11 日
【51】Int. Cl.：　*G06F9/312　(2006.01)*

新型　　全 6 頁

【54】名　稱：具有混沌系統認證之儲存系統
【21】申請案號：107213237　　【22】申請日： 中華民國 107 (2018) 年 09 月 28 日
【72】新型創作人：顏錦柱 (TW) YAN, JUN-JUH；曹彥傑 (TW) TSAO, YEN-CHIEH；曾士哲 (TW) CHANG, HAO-HSUN；周昱宏 (TW) CHOU, YU-HONG；萬培彥 (TW) WAN, PEI-YEN；詹哲瑜 (TW) ZHAN, ZHE-YU
【71】申 請 人：樹德科技大學　SHU-TE UNIVERSITY
高雄市燕巢區橫山路 59 號
【74】代 理 人：葉大慧
(NOTE)備註：相同的創作已於同日申請發明專利(Another patent application for invention in respect of the same creation has been filed on the same date)

【57】申請專利範圍

1. 一種具有混沌系統認證之儲存系統，所述儲存系統包括一儲存裝置，該儲存裝置透過一智慧型行動裝置進行認證後，進行與一電腦的雙向資料存取，該具有混沌系統認證之儲存系統包括：一智慧型行動裝置，包括：一行動裝置藍芽模組，設置於該智慧型行動裝置；以及一行動應用程式，安裝於該智慧型行動裝置，該行動應用程式包括有一主亂數產生器模組以及一驗證模組；一儲存裝置，該儲存裝置透過該智慧型行動裝置進行認證後，進行與該電腦的雙向資料存取，包括：一殼體，具有一開口及一容置空間，該開口設於該殼體之一端且與該容置空間相連；一連接模組，設置於該開口位置處，該連接模組之一端可連接於該電腦；一處理器模組，設置於該容置空間；一雙向類比轉換模組，設置於該容置空間，連接於該連接模組；一快閃記憶體模組，設置於該容置空間，連接於該雙向類比轉換模組與該處理器模組；一儲存裝置藍芽模組，設置於該容置空間，連接於該處理器模組；以及一僕亂數產生器模組以及一同步控制器，設置於該容置空間，連接於該處理器模組；以及一雲端認證平台，與該智慧型行動裝置連接，包括：一管理網頁平台，用以供至少一使用者進行登錄；以及一使用者資料庫，連接於該管理網頁平台，且具有一儲存裝置資料庫；其中，首次使用該儲存裝置時，先進入該雲端認證平台執行一歸戶作業，使得該使用者可指定該驗證模組進行驗證；當該連接模組連接於該電腦，該儲存裝置藍芽模組與該行動裝置藍芽模組配對成功後，該主亂數產生器模組以及該僕亂數產生器模組藉由該同步控制器同步取得相同的隨機訊號，進行一加密傳輸比對認證，通過該驗證模組與該加密傳輸比對認證後，將該雙向類比轉換模組開啟，進行該快閃記憶體模組與該電腦的雙向資料讀取。
2. 如申請專利範圍第 1 項所述的具有混沌系統認證之儲存系統，其中，該歸戶作業為該使用者自該管理網頁平台登錄該使用者帳號、密碼至該使用者資料庫，以及輸入一產品金鑰查詢該儲存裝置資料庫後執行媒合。
3. 如申請專利範圍第 1 項所述的具有混沌系統認證之儲存系統，其中，該驗證模組可進行一聯網驗證或一無聯網驗證。
4. 如申請專利範圍第 3 項所述的具有混沌系統認證之儲存系統，其中，該聯網認證為該驗證模組至該使用者資料庫取得用戶資訊進行驗證，驗證完成，下載一產品金鑰；當該行

動應用程式與該儲存裝置達到同步，將該產品金鑰傳送給該儲存裝置執行該加密傳輸比對認證，執行成功該電腦開始對該儲存裝置做存取。

5. 如申請專利範圍第 3 項所述的具有混沌系統認證之儲存系統，其中，該無聯網認證為該行動應用程式自動下載一產品金鑰並加密保存在該驗證模組中，當該使用者選擇解鎖該儲存裝置時，該行動應用程式便會與該儲存裝置進行同步運算，透過預先下載的該產品金鑰，執行該加密傳輸比對認證，執行成功該電腦開始對該儲存裝置做存取。
6. 如申請專利範圍第 1 項所述的具有混沌系統認證之儲存系統，其中，該同步控制器將該主亂數產生器模組所產生的數值以及該僕亂數產生器模組所產生的數值，所述兩數值之誤差收斂到零。
7. 如申請專利範圍第 1 項所述的具有混沌系統認證之儲存系統，其中，該加密傳輸比對認證包括有一非線性加解密函數；將一產品金鑰自該主亂數產生器模組經由該非線性加解密函數進行加密，傳送到該僕亂數產生器模組後以該非線性加解密函數進行解密並得一解密密碼，比對該解密密碼與該產品金鑰相同即完成該加密傳輸比對認證。
8. 如申請專利範圍第 7 項所述的具有混沌系統認證之儲存系統，其中，該非線性加解密函數之方程式如下：

$$E(x,p,t) = x_1^2 + (1 + x_2^2)p$$

$$\hat{p} = D(\hat{x},p,t) = (E(x,p,t) - \hat{x}_1^2)/(1 + \hat{x}_2^2)$$

其中，E(x,p,t)為一非線性加密函數、D($\hat{x}$,p,t)為一非線性解密函數、p 為固定密碼、$\hat{p}$為解密密碼、x_i，i=1,2 為該主亂數產生器模組產生之數值以及$\hat{x}_i$，i=1,2 為該僕亂數產生器模組產生之數值。

9. 如申請專利範圍第 1 項所述的具有混沌系統認證之儲存系統，其中，該雲端認證平台可登錄複數個該儲存裝置，且以該行動應用程式進行管理。

圖式簡單說明

圖 1 為本創作具有混沌系統認證之儲存系統之系統方塊圖；圖 2 為本創作具有混沌系統認證之儲存系統之使用歸戶流程圖；圖 3 為本創作具有混沌系統認證之儲存系統之具連網驗證流程圖；圖 4 為本創作具有混沌系統認證之儲存系統之無聯網驗證流程圖；圖 5 為本創作具有混沌系統認證之儲存系統之混沌系統狀態響應類隨機亂數圖；圖 6 為本創作具有混沌系統認證之儲存系統之具同步控制器之混沌系統動態響應圖；圖 7 為本創作具有混沌系統認證之儲存系統之同步誤差動態響應圖；圖 8A 為本創作具有混沌系統認證之儲存系統之同步後主亂數產生器模組奇異吸子圖；圖 8B 為本創作具有混沌系統認證之儲存系統之同步後僕亂數產生器模組奇異吸子圖。

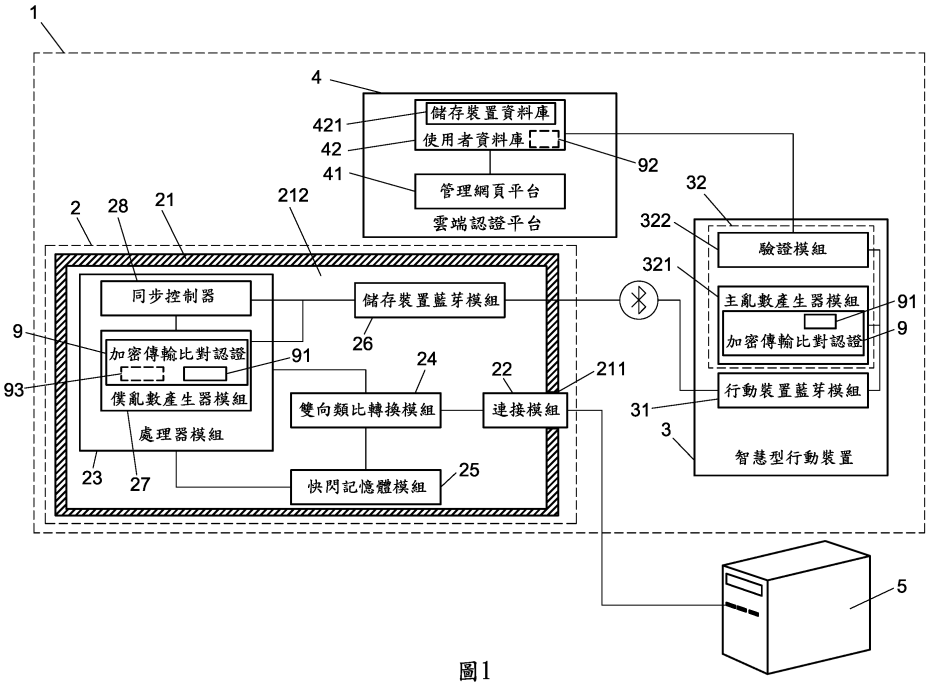
1
4
421
儲存裝置資料庫
42
使用者資料庫
92
41
管理網頁平台
雲端認證平台
2
28
21
212
32
322
驗證模組
321
主亂數產生器模組
91
加密傳輸比對認證
9
同步控制器
儲存裝置藍芽模組
9
加密傳輸比對認證
91
26
24
22
211
93
僕亂數產生器模組
雙向類比轉換模組
連接模組
31
行動裝置藍芽模組
處理器模組
3
智慧型行動裝置
23
27
快閃記憶體模組
25
5

圖1

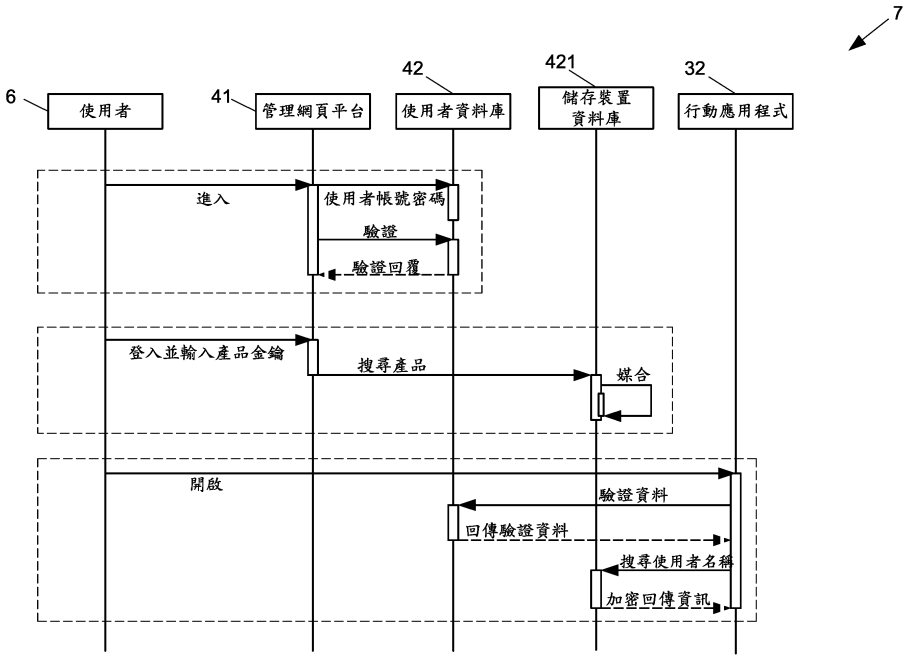
7
6
使用者
41
管理網頁平台
42
使用者資料庫
421
儲存裝置資料庫
32
行動應用程式
進入
使用者帳號密碼
驗證
驗證回覆
登入並輸入產品金鑰
搜尋產品
媒合
開啟
驗證資料
回傳驗證資料
搜尋使用者名稱
加密回傳資訊

圖2

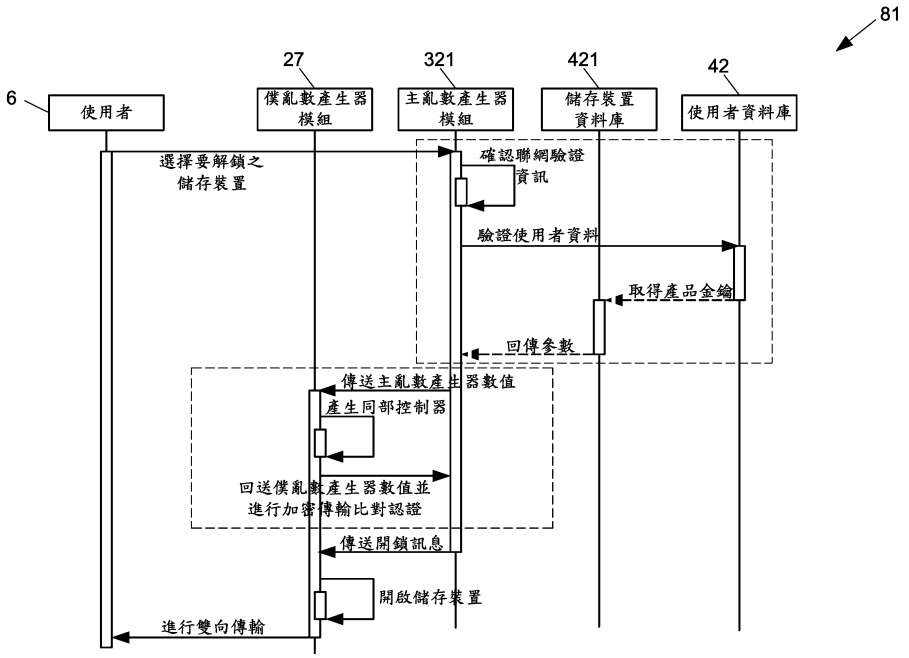
81
6
使用者
27
僕亂數產生器模組
321
主亂數產生器模組
421
儲存裝置資料庫
42
使用者資料庫
選擇要解鎖之儲存裝置
確認聯網驗證資訊
驗證使用者資料
取得產品金鑰
回傳參數
傳送主亂數產生器數值
產生同部控制器
回送僕亂數產生器數值並進行加密傳輸比對認證
傳送開鎖訊息
開啟儲存裝置
進行雙向傳輸

圖3

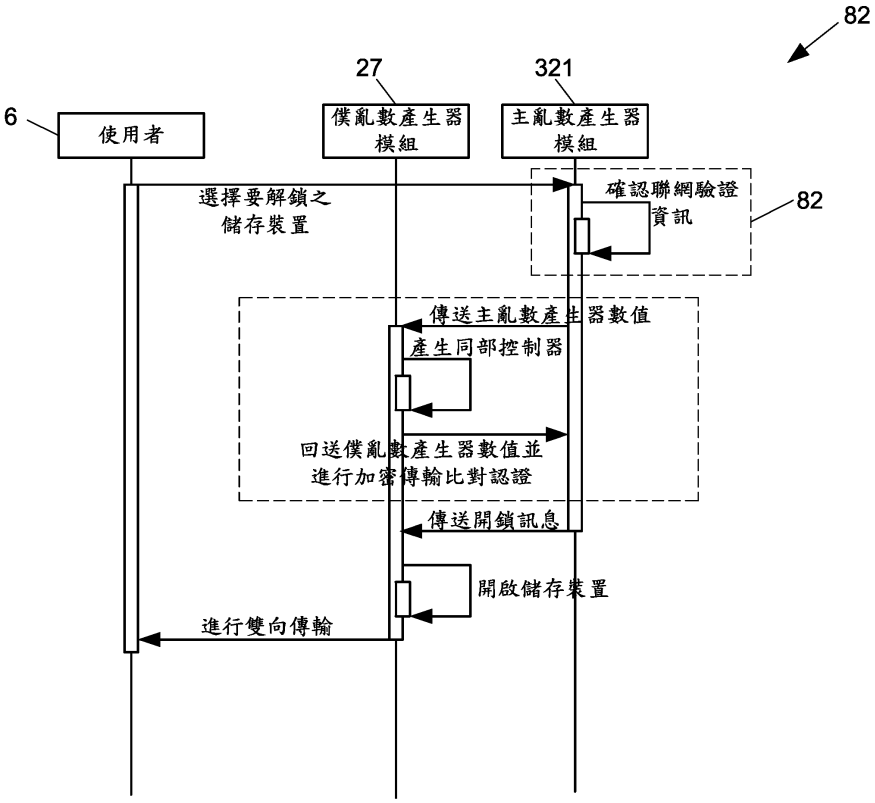
82
6
使用者
27
僕亂數產生器模組
321
主亂數產生器模組
選擇要解鎖之儲存裝置
確認聯網驗證資訊
82
傳送主亂數產生器數值
產生同部控制器
回送僕亂數產生器數值並進行加密傳輸比對認證
傳送開鎖訊息
開啟儲存裝置
進行雙向傳輸

圖4

(5)

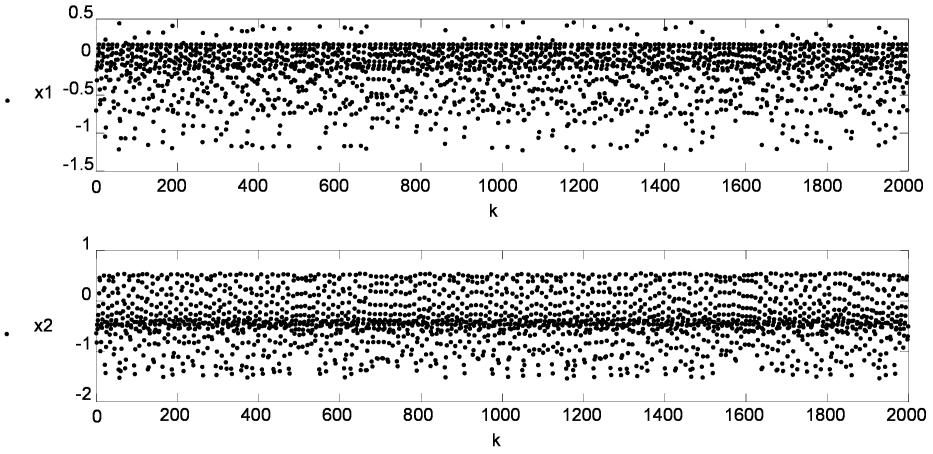

圖5

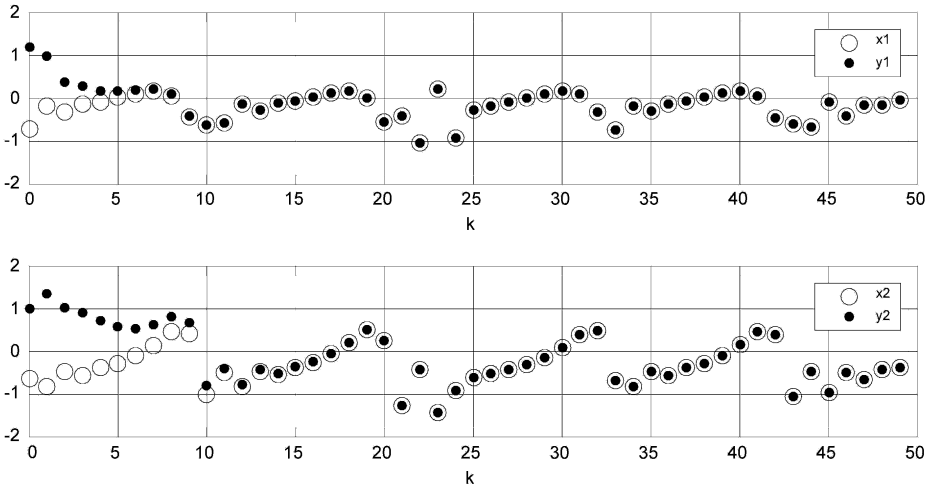

圖6

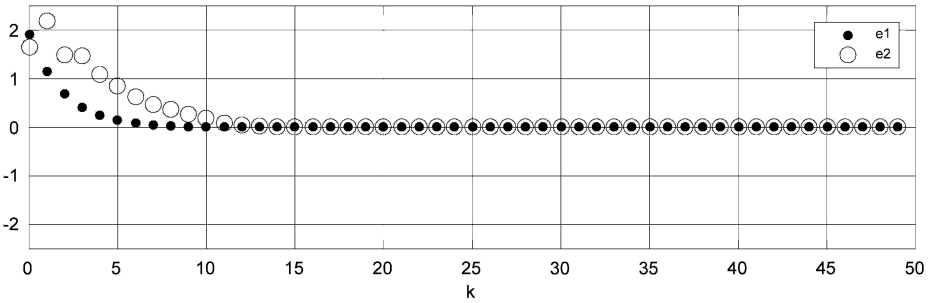

圖7

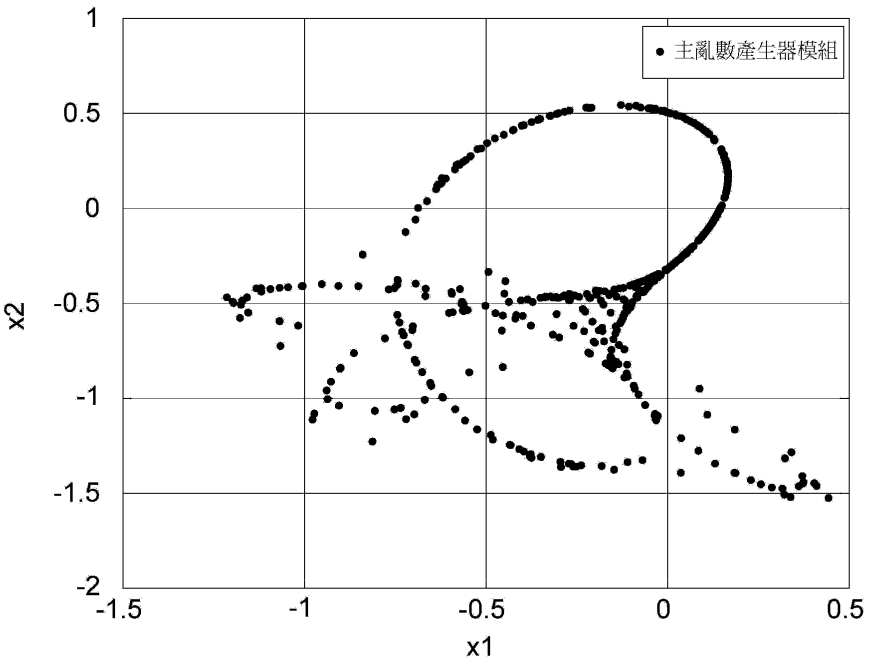
主亂數產生器模組
x2
x1
1
0.5
0
-0.5
-1
-1.5
-2
-1.5
-1
-0.5
0
0.5

圖8A

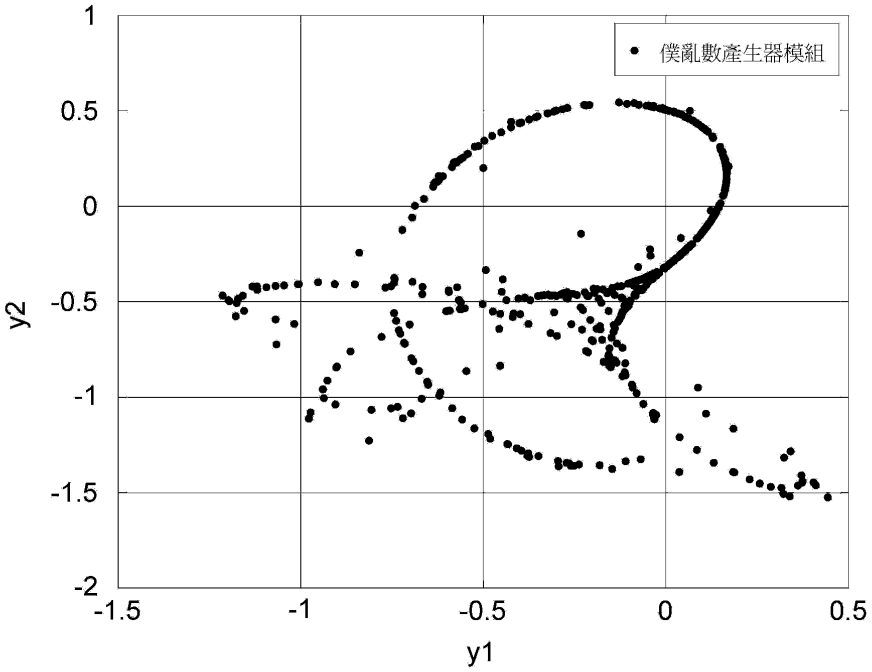
僕亂數產生器模組
y2
y1
1
0.5
0
-0.5
-1
-1.5
-2
-1.5
-1
-0.5
0
0.5

圖8B