公告本

384591

申請日期	86.7.25
案號	86110567
類別	H04L 9/14

（以上各欄由本局填註）

A4
C4

384591

發明 ~~新型~~ 專利說明書

一、發明新型名稱	中文	識別卡安全控管方法
	英文	
二、發明創作人	姓名	1 樊國楨 2 陳彥學 3 宋振華
	國籍	中華民國
	住、居所	1 新竹縣寶山鄉寶新路 147 巷 53 號 2 台南市大興街 150 巷 38 號 3 台北市內湖區內湖路三段 72 巷 61 號二樓
三、申請人	姓名（名稱）	財團法人工業技術研究院
	國籍	中華民國
	住、居所（事務所）	新竹縣竹東鎮中興路四段 195 號
	代表人姓名	孫　震

五、發明說明（ 1 ）

本發明係有關於一套識別卡(token card)安全控管方法，特別係有關於利用密碼學加解密、數位電子簽章技術、以及分散機密的觀念來加以保護網路作業環境下安全性及可靠度之控管方法。此種識別卡可以是軟式磁片、IC 卡、ZIP 或 MO 等等屬於可攜式之所有儲存裝置(儲存媒體)。

由於網際網路之商業應用日益普及與盛行，網路辦公室與電子銀行也隨著快速發展，而其電子資訊傳送之正確性則端賴密碼元件，以及其安全控管機制運作之高度保密性來保障所有人之權益。

就網路作業環境而言，使用者必須藉其各別之識別裝置、登錄機器、操作軟體、及一般協定等之統合運作，而可以讓使用者在其用戶端成功地登錄並完成驗證。而使用者在接取(access)網路時，卻也是最容易洩露其本身之機密，所以在網路系統下，用戶端往往是防護最少的部份，而容易為入侵者所截取而用以破解系統。

此外，由於在網路上資料之互通有無，所以使用者在其登錄端(用戶端)所使用之軟體，也常遭受到電腦病毒之潛在威脅。目前對於軟體的保護，除以防毒軟體來防止程式被侵入，並無明顯的方法可以偵測軟體是否已為病毒所篡改。

在儲存媒體(儲存裝置)方面，一般於學理上之討論皆假設儲存媒體是非常安全的，如利用 IC 卡或簽章卡，但是此類設備其價格較高，且須購買額外之設備，所以短期內無法大量推廣。而磁片是一便宜且普及的儲存媒

五、發明說明（２）

體，但是其安全性低，目前有以PKCS#5方式用以增加磁片安全之方法，然而其卻往往容易被字典攻擊法所破解。

而現行之網路安全機制中，用以確保安全性的秘密金鑰若因種種因素而遺失的話，將會使得加密的資料無法獲得，徒增困擾。所以在網路安全傳輸上，金鑰之回復系統是有其必要性。

在網路文件交換環境中，文件之效力可能相當的久，在科技快速進展的現代，電子文件被篡改和冒名之可能性相當大。所以設計一套電子公文擁有權的驗核機制，使得即使在簽章金鑰被破解的情形下，仍然不會有被偽簽的危險，以提供發文端必要之保護，是有其必要性的。

有鑑於此，本發明針對上述網路應用所可能遭遇之問題，提出一套識別卡安全控管方法，其包括以下部份：

一、檢驗系統中檔案有無遭篡改的檢查機制，用以偵測系統內檔案有無遭受入侵者亦或病毒侵入。

二、植基相互認證系統的控管機制，用以防制入侵者對已加密之資料進行字典或蠻橫找尋攻擊法，並進而防止使用者在使用不安全的機器上進行登入。

三、使用於簽章控管的群體導向數位簽章機制，藉由使用者完成與伺服端認證後，文件由使用者簽過後，須再經由伺服端簽過，用以防止使用者在無意下，或操作錯誤下簽出文件。

五、發明說明（３）

四、金鑰回復機制，當使用者金鑰遺失或有爭端發生時，而需由公正之第三者舉證時，可藉以導出金鑰。

五、回復金鑰加解密機制。

六、所有權驗核機制，用以確保他人無法仿冒，或是在已發出的文件間插入其他偽造的文件。

為讓本發明之上述目的、特徵、和優點能更明顯易懂，下文特針對上述各部份之控管方式，舉出較佳實施例，並配合所附圖式，做詳細說明如下。

圖示之簡單說明：

第 1 圖係顯示一軟體之目錄架構圖。

第 2A ~ 2B 圖係顯示本發明第二實施例之動作過程簡圖。

第 3A ~ 3B 圖係回復金鑰加解密機制，分別為資料傳送及驗證程序和金鑰及密文回復程序。

實施例一：(檢驗系統檔案有無遭篡改的檢查機制)

一種識別卡安全控管方法，用以偵測並防止用戶端電腦系統中之檔案遭受入侵者篡改或病毒損害，此控管方法在用戶端電腦系統上之運作機制包含如下兩個程序：檢驗軟體安裝程序；以及程式偵試程序。

檢驗軟體安裝程序包括如下之步驟：

對於欲控管之軟體的根目錄下各子目錄底下之每一檔案及目錄，利用"安全雜湊函數"以產生相對應之第一檔案雜湊值，並儲存於用戶端電腦系統上；

分別將各該子目錄中之每一第一檔案雜湊值加以結

五、發明說明（4）

合，再利用安全雜湊函數產生相對應之第一目錄雜湊值，並將此第一目錄雜湊值分別儲存於各該子目錄中。如此重覆，一層層對該根目錄下的各層下子目錄作相同之動作，以得到各相對應之檔案雜湊值及目錄雜湊值，並分別儲存於用戶端電腦系統及各子目錄中，直到位於該根目錄下所有之子目錄均有其相對之目錄雜湊值，再於此根目錄下，將此根目錄下之所有目錄雜湊值加以結合，並利用安全雜湊函數產生一第一根目錄雜湊值；利用用戶端的私密金鑰而將上述根目錄雜湊值加以簽章，並將上述簽章結果儲存於用戶之一可攜式儲存裝置(即識別卡)中；並將程式檢驗程式儲存於該可攜式儲存裝置中，此時可將該儲存裝置設成唯讀，而完成此檢驗軟體安裝程序。

而程式偵試程序則包括以下步驟：

執行一程式檢驗程式；該檢驗程式將用戶端欲偵試之軟體的根目錄下子目錄中每一檔案，利用安全雜湊函數產生相對應之第二檔案雜湊值，並檢查其與儲存於用戶端之上述第一檔案雜湊值是否相等，若不相等則表示欲偵試之軟體中的程式有遭竄改或是版本不符而停止此偵試程序；否則上述檢驗程式再以如前述安裝程序之過程，而分別將各子目錄中之檔案雜湊值加以結合，再利用安全雜湊函數產生相對應之第二目錄雜湊值，並將該第二目錄雜湊值與分別儲存於上述各子目錄中第一目錄雜湊值加以比較，若不相等則表示欲偵試之軟體中的程

五、發明說明（5）

式有遭竄改或是版本不符而停止此偵試程序。

對各層下子目錄重覆上述之檢查動作，直到位於根目錄下所有之子目錄均有其相對之第二目錄雜湊值且均通過驗證，再於根目錄下將上述根目錄下之目錄雜湊值加以結合，並再利用安全雜湊函數產生一第二根目錄雜湊值，將其與儲存於用戶端之第一根目錄雜湊值相比較，若不相等則表示欲偵試之軟體中的程式有遭竄改或是版本不符而停止此偵試程序。最後對第二根目錄雜湊值加以簽章，並自上述可攜式儲存裝置中讀出第一根目錄湊值之簽章結果，驗正兩者是否相符合，若不符合則表示用戶端之程式有遭篡改或是版本不符之情形。

假設欲控管之軟體的檔案結構如第 1 圖所示。於檢驗軟體安裝程序中，首先對欲控管之軟體的根目錄下，各目錄底下之檔案或目錄 A ~ G 進行雜湊運算而得雜湊值 hs(A)~hs(G)，並將 hs(A)~hs(G)值存於用戶端之電腦系統中。將 I 子目錄下之雜湊值 hs(A)和 hs(B)相結合後，例如是取互斥運算，再對其進行雜湊運算而得子目錄雜湊值 hs(I)，同理也可得子目錄雜湊值 hs(II)，再將這些子目錄雜湊值存於各自之子目錄中。

將子目錄 III 下之雜湊值 hs(I)、hs(E)、和 hs(F)相結合後，再對其進行雜湊運算而得子目錄雜湊值 hs(III)，同理將子目錄IV下之雜湊值 hs(II)、和 hs(G)相結合後，再對其進行雜湊運算而得子目錄雜湊值 hs(IV)，亦將這些子目錄雜湊值存於各自之子目錄中。最後，將雜湊值

五、發明說明（ 6 ）

hs(III)、和 hs(IV)相結合後，再進行雜湊運算而得一根目錄雜湊值 hs(root)。

最後，以用戶端的私密金鑰而將上述根目錄雜湊值 hs(root)加以簽章，並將上述簽章結果儲存於用戶之可攜式儲存裝置中；再將程式檢驗程式儲存於上述可攜式儲存裝置中，則完成檢驗軟體安裝程序。

於程式偵試程序中，先執行上述程式檢驗程式，該檢驗程式將用戶端欲偵試之軟體根目錄下子目錄中每一檔案，利用安全雜湊函數產生相對應之雜湊值 hs*(A)~hs*(G)，並分別一對一檢查其與儲存於用戶端之雜湊值 hs(A)~hs(G)是否相等，若不相等則欲偵試之軟體的程式有遭篡改或是版本不符而停止此程序。

否則上述偵試程式再以如安裝程序之過程，而分別產生 hs*(I)~hs*(IV)、以及 hs*(root)，再分別一對一檢查其與儲存於用戶端之雜湊值 hs(I)~hs(IV)、hs(root)是否相等若不相等則欲偵試之軟體的程式有遭篡改或是版本不符而停止程序。最後，對上述根目錄雜湊值 hs*(root)加以簽章，並自上述可攜式儲存裝置中讀出第一根目錄湊值之簽章結果，驗正兩者是否相符合，若不符合則表示欲偵試之軟體之程式有遭篡改或是版本不符之情形，而完成驗證之程序。

由上可知，經由逐層之檢查，可將所有所有檔案結構上之任何變動均查覺出來，故而讓使用者得知用戶端的程式是否有遭篡改或是版本不符之情形發生。

五、發明說明（7）

實施例二：(植基相互認證系統的控管機制)

請參照第 2A ~ 2C 圖，其表示本實施例動作過程之簡圖，下文將配合第 2A ~ 2C 來說明本實施例。

本發明之一種植基相互認證系統的控管機制，主要係利用伺服端、用戶端及其可攜式儲存裝置間之密碼相互認證方法，藉以防止入侵者對可攜式儲存裝置中已加密之機密資料進行字典或蠻橫找尋攻擊法，並進而防止用戶使用不安全的機器進行登入。

上述控管方法在用戶端電腦系統上之運作機制包含如下三個程序：

I.註冊程序，初次登錄使用時之控管方法。

II.認證程序，使用者完成註冊程序後，再次登錄使用時之控管方法。

III.更換密碼程序。

請參照第 2A 圖，註冊程序包括如下步驟：

[a]用戶端利用其識別碼 ID、一會談金鑰 TK(有時亦稱為通訊基碼)、一第一驗證因子 N1、及相關資料，合併產生一用戶端第一簽體(TK+ID+N1)，用戶端對該用戶端第一簽體以伺服端之公開金鑰 K_{SP} 進行加密，而得用戶端第一密件 C1=EN(K_{SP} , TK+ID+N1)，將該用戶端第一密件 C1、識別碼 ID、一註冊請求 Reg_req，及相關資料傳送至伺服端。

[b]伺服端接收到上述註冊請求 Reg_req 後，以伺服端私密金鑰 K_{SS} 解開上述用戶端第一密件 C1 而獲得前述

五、發明說明（８）

之會談金鑰 TK、第一驗證因子 N1、及識別碼 ID 等相關資料。

伺服端產生一加密金鑰 SK、一第二驗證因子 N2、及一整數 n，伺服端以上述之加密金鑰 SK、整數 n、第一驗證因子 N1、第二驗證因子 N2、以及相關資料合併產生一伺服端第一簽體(n+N2+N1+SK+Time1+Salt)，以上述會談金鑰 TK 對上述伺服端第一簽體加密而得一伺服端第一密件 S1=(TK, n+N2+N1+SK+Time1+Salt)，再將 S1 回傳給用戶端，其中 Time1 為系統時間，而 Salt 為一加鹽值，此加鹽值可使之每次輸出不同的值。

[c]用戶端完成接收後，以上述之會談金鑰 TK 解開上述伺服端第一密件 S1，而得上述整數 n、上述加密金鑰 SK、上述第一驗證因子 N1 與第二驗證因子 N2，系統時間 Time1、及加鹽值 Salt。用戶端檢查上述第一驗證因子(N1)是否為原先所送之值，並檢查系統時間 Time1 以驗證傳輸時間是否在合理之範圍內，驗證正確後用戶端將使者個人密碼 PWD 合併加鹽值 Salt 進行 n 次雜湊運算而得一密碼封包 OTP=Hn(Salt+PWD)；

[d]用戶端以上述密碼封包 OTP、上述第二驗證因子 N2、及系統時間 Time2 為用戶端第二簽體(OTP+N2+Time2)，利用上述會談金鑰(TK)對上述用戶端第二簽體進行加密而得一用戶端第二密件 C2=EN(TK，OTP+N2+Time2)後，將 C2 回傳送給伺服端。

[e]伺服端接收到上述用戶端第二密件 C2 後，以上

五、發明說明（9）

述之會談金鑰 TK 解開上述第二密件 C2，而得上述之密碼封包 OTP，伺服端並驗證上述第二驗證因子是否為原先所送之值，並檢查系統時間 Time2 以驗證傳輸時間是否在合理之範圍內，若正確無誤則將上述之密碼封包 OTP、以及整數 n 儲存於伺服端，並產生一註冊標記 Reg_yes。伺服端利用上述密碼封包 OTP、註冊標記 Reg_yes、及系統時間 Time3 為伺服端第二簽體(OTP + Req_yes + Time3)，以上述會談金鑰對上述伺服端第二簽體進行加密而得一伺服端第二密件 S2=EN(TK, OTP +Req_yes + Time3)，再將 S2 回傳給用戶端。

[f]用戶端以會談金鑰解開上述伺服端第二密件 S2，而接收上述註冊標記 Reg_yes 確認註冊無誤，且已檢查系統時間 Time3 以驗證傳輸時間是否在合理之範圍內後，即自行產生一用戶端金鑰 CK 並且對使用者密碼 PWD 進行雜湊運而導出一密碼金鑰 PWK=H(PWD)。使用上述加密金鑰 SK 與密碼金鑰 PWK，將上述用戶端金鑰 CK 加密成為用戶端密文 ECK 並將其結果存於用戶端上。另外亦使用上述用戶端金鑰 CK 與密碼金鑰 PWK 對使用者之私密資料 DK 加密成為一密鑰密文 EDK，並將其存於可攜式儲存裝置上，而完成註冊之程序。

請參照第 2B 圖，完成註冊程序後，使用者再次登入使用時，認證程序包括如下步驟：

[a]用戶端將其識別碼 ID，一第三驗證因子 N3、與此程序所要使用之會談金鑰 TK1 合併產生一用戶端第三

五、發明說明（10）

簽體(TK1+ID+N3)，用戶端對上述用戶端第三簽體以伺服端之公開金鑰 K_{SP} 進行加密，而得用戶端第三密件 C3=EN(K_{SP} , TK2+ID+N3)，並將上述用戶端第三密件 C3、上述識別碼 ID、一確認請求 Auth_req，及相關資料傳送至伺服端。

[b]伺服端接收到確認請求 Auth_req 後，以伺服端私密金鑰 K_{SS} 解開上述用戶端第三密件 C3 而獲得上述之會談金鑰 TK1、第三驗證因子 N3、及識別碼 ID 等相關資料，伺服端並由儲存裝置中找出使用者於上述註冊程序中所對應之密碼封包 OTP、以及整數 n 等相關資料。若整數 n 小於 2 則用戶端之使用者須重新註冊，若整數 n 不小於 2，則伺服端產生一小於 n 的整數 k 及 m 而 m＝n - k。

再將會談金鑰 TK1、整數 m、第三驗證因子 N3 及相關資料合併為伺服端第三簽體(m + N3 + Time4 + Salt)，以會談金鑰 TK1 對其加密而得伺服端第三密件 S3 = EN(TK1 ,m+N3+Time4+Salt)，並將伺服端第三密件 S3 回傳給用戶端。

[c]用戶端完成接收後，以上述之會談金鑰 TK1 解開上述伺服端第三密件 S3，而得上述整數 m、上述第三驗證因子 N3，用戶端檢查上述第三驗證因子 N3 是否為原先所送之值，並檢查系統時間 Time4 以驗證傳輸時間是否在合理之範圍內。

驗證正確後用戶端將使者輸入之個人密碼 PWD 合

五、發明說明（11）

併加鹽值 Salt 後再進行 m 次雜湊運算而得一第一封包 OTP1=Hm(Salt+PWD)，並產生一第四驗證因子 N4，其中上述加鹽值 Salt 即為註冊程序時之加鹽值。

[d]用戶端以上述第一封包 OTP1、上述第四驗證因子(N4)、及相關之資料合併為用戶端第四簽體(OTP1+N4+Time5)，利用上述會談金鑰 TK1 對上述用戶端第四簽體進行加密而得一用戶端第四密件 C4=EN(TK1 , OTP1+N4+Time5)後，將 C4 回傳送給伺服端。

[e]伺服端接收到上述用戶端第四密件 C4 後，以上述之會談金鑰 TK1 解開上述第四密件，而得上述之第一封包 OTP1，伺服端並驗證上述第四驗證因子(N4)是否為原先所送之值，並檢查系統時間 Time4 以驗證傳輸時間是否在合理之範圍內，若正確無誤則伺服端對上述第一封包 OTP1 再進行 k 次雜湊算，其運算結果 Hk(OTP1)與註冊程序中儲存於伺服端之密碼封包 OTP 比對是否相同，驗證正確後即儲存整數 m 於伺服端而取代原先之整數 n，同時儲存 OTP1 取代原來之 OTP，之後將上述註冊程序中產生之加密金鑰 SK、密碼封包 OTP1、及驗證成功之訊息 Auth_yes 合併為伺服第四簽體(OTP1+SK+Auth_yes+Time6)，將其以會談金鑰 TK1 加密後得 S4=EN(TK1 , OTP1+SK+Auth_yes+Time6)後再回傳給用戶端。

[f]用戶端以會談金鑰 TK1 解開上述加密資料 S4

五、發明說明（12）

後，而分別得到加密金鑰 SK、密碼封包 OTP1、及驗證成功之訊息 Auth_yes，並檢查系統時間 Time6 以驗證傳輸時間是否在合理之範圍內，待確定驗證成功後，即對使用者密碼 PWD 進行雜湊運而導出一密碼金鑰 PWK=H(PWD)，用戶端使用上述加密金鑰 SK 與密碼金鑰 PWK 對存於用戶端上之密文 ECK 解密以得到上述之註冊程序中之用戶端金鑰 CK。

使用上述用戶端金鑰 CK、密碼金鑰 PWK 和加密金鑰 SK 對存於可攜式儲存裝置中之密文 ECK 解密而得到使用者之私密資料 DK，如此即完成證驗之過程，之後用戶端之使者即可以利用其私密資料 DK 執行欲進行之動作。

請參照第 2C 圖，當使用者欲更改密碼時，其更換密碼程序包括如下步驟：

[a]用戶端將其識別碼 ID，一第五驗證因子 N5、與此程序所要使用之會談金鑰 TK2 合併產生一用戶端第五簽體(TK2+ID+N5)，用戶端對上述用戶端第五簽體以伺服端之公開金鑰 K_{SP} 進行加密，而得用戶端第五密件 C5=EN(K_{SP}, TK2+ID+N5)，並將上述用戶端第五密件 C5、上述識別碼 ID、一密碼更換請求 CP_req，及相關資料傳送至伺服端。

[b]伺服端接收到密碼更換請求 CP_req 後，以伺服端私密金鑰 K_{SS} 解開上述用戶端第五密件 C5 而獲得上述之會談金鑰 TK2、第五驗證因子 N5、及識別碼 ID 等相

五、發明說明（13）

關資料，伺服端並找出使用者於上述註冊程序中所對應之整數 n 資料，伺服端再產生一正整數 m=n-k、及整數 I，其中 k 也為整數，再將整數 m、I、第五驗證因子 N5 及相關資料合併為伺服端第五簽體(m+I+N5+N6+Time7+Salt1+Salt2)，以會談金鑰 TK2 對其加密而得伺服端第五密件 S5=EN(TK2，m+I+N5+N6+Time7+ Salt+Salt1)，並將伺服端第五密件 S5 回傳給用戶端。

[c]用戶端完成接收後，以上述之會談金鑰 TK2 解開上述伺服端第五密件 S5，而得上述整數 m、I、上述第五驗證因子 N5，用戶端檢查上述第五驗證因子 N5 是否為原先所送之值，且檢查系統時間 Time7 是否在合理之範圍內，驗證正確後用戶端將使者輸入之個人密碼 PWD 合併加鹽值 Salt1 進行 m 次雜湊運算而得一第一封包 OTP1=Hm(Salt+PWD)，同時對使用者所輸入之新密碼 NPWD 進行 I 次雜湊運算，而得一第二封包 $OTP2 = H_I(Salt1 + NPWD)$。

[d]用戶端以上述第一封包 OTP1、第二封包 OTP2，及上述第六驗證因子 N6、及相關之資料合併為用戶端第六簽體(OTP1+OTP2+N6+Time8)，利用上述會談金鑰 TK2 對上述用戶端第六簽體進行加密而得一用戶端第六密件 C6=EN(TK2，OTP1+OTP2+N6+Time8)後，將 C6 回傳送給伺服端。

[e]伺服端接收到上述用戶端第六密件 C6 後，以上述之會談金鑰 TK2 解開上述第六密件 C6，而得上述之第

五、發明說明（14）

一封包 OTP1 和第二封包，伺服端並驗證上述第六驗證因子 N6 是否為原先所送之值，且檢查系統時間 Time6 是否在合理之範圍內；若正確無誤則伺服端對上述第一封包 OTP1 進行 k 次雜湊算，其運算結果與註冊程序中儲存於伺服端之密碼封包比對是否相同，驗證正確後即儲存整數 I 於伺服端而取代原先之整數 n，也將第二封包儲存於伺服端，並產生一新加密金鑰 NSK，將註冊程序產生之加密金鑰 SK 和新加密金鑰 NSK、以及第一封包 OTP1 與第二封包 OTP2、及更換成功之訊息 CP_yes 合併為伺服第六簽體(OTP1 + OTP2 + SK + NSK + CP_yes + Time9)，將其以會談金鑰加密後回傳給用戶端。

[f]用戶端以會談金鑰 TK2 解開上述加密資料後，而分別得到加密金鑰 SK、新加密金鑰 NSK，第一封包 OTP1 和第二封包 OTP2、及更換成功之訊息 CP_yes，確定更換成功後，且檢查系統時間 Time9 是在合理之範圍內後。

先以 PWK 及 SK 解出存於用戶端的密文 ECK，再用 CK 合併使用者的個人密碼所導出的金鑰 PWK 以及 SK 解出原先加密存於可攜式儲存裝置中的密鑰密文 EDK，之後用戶端即自行產生一用戶端新金鑰(NCK)，利用先前獲得之 NSK 與使用者之新密碼 NPWD 而導出的 NPWK 加密 NCK 儲存於用戶端上，再以 NPWK、NSK 及 NCK 加密 DK 而將結果存於可攜式儲存裝置中。

實施例三之一：(使用於簽章控管的群體導向數位簽章機制)

五、發明說明（15）

一種識別卡安全控管方法，為多重簽章方式之群導向數位簽章系統下，用以防止用戶在無意下簽出文件之控管方法，其包括如下步驟：當要簽出文件時，以用戶端使用者之私密金鑰先行對上述文件簽章而得一第一簽章，再以伺服端之私密金鑰對上述第一簽章再行簽章而得到一第二簽章，而完成簽章之過程；以及在驗證過程中，將上述第二簽章先以伺服端之公開金鑰解開而得一驗證簽章，再將上述驗證簽章以使用者之公開金鑰解開而得一驗證文件，比較上述第一驗證文件與上述原先送出之文件是否相同，若正確則表示簽章係為正確無誤。

下文中以 RSA 簽章系統下建構本發明簽章控管系統之實施例。

於 RSA 系統之多重簽章方式之群導向數位簽章系統下，用以防止用戶在無意下簽出文件之控管方法，其包括如下步驟：

用戶端與伺服端之公開金鑰分別為 up 及 sp，其模數為 Nu 和 Ns，而其相對應之之私密金鑰分別為 us 和 ss；

在簽章過程時，首先以用戶端的私密金鑰 us 對文件 M 簽章而得 $SIG1=M^{us} \bmod Nu$，再用伺服端的私密金鑰 ss 對 SIG1 簽章而得 $SIG2=SIG1^{ss} \bmod Ns$；

在驗證過程時，收文者要驗證文件 M 之簽章 SIG2 時，先用伺服端的公開金鑰 sp 計算 $SIG2^{sp} \bmod Ns$ 而解得 SIG1，再以用戶端之公開金鑰 up 計算 $SIG1^{up} \bmod Nu$ 而解得一待驗證值 M1；

五、發明說明（16）

檢查 M1 與文件 M 是否相等，若相等則 SIG2 才是正確的簽章，否則不是正確簽章。

由上述可知，本機制其文件之簽出須先經由用戶端簽章後，再經由伺服端簽過一次，所以具有雙重驗證之功能，所以不會發生因使者疏忽下或操作錯誤之情形下，而簽出文件。

實施例三之二：(使用於簽章控管的群體導向數位簽章機制)

一種識別卡安全控管方法，為在群體簽章方式之群導向數位簽章系統下，用以防止用戶在無意下簽出文件之控管方法，其方法為：

伺服端與用戶端使用者兩者對外只有一共通公開金鑰，伺服端與用戶端使用者各有其私密金鑰和與其私密金鑰相對應之公開金鑰，上述共通公開金鑰係由伺服端公開金鑰與使用者公開金鑰而得，而欲簽出之文件須先經使用者之私密金鑰簽過後，再由伺服端之私密金鑰簽過才可送出，當要驗證所簽出文件之簽章時則須使用上述共通公開金鑰對所簽出之文件解密後加以比對即可。

下文將以 ElGamal 之變型系統建構本發明簽章控管系統之實施例。

一種識別卡安全控管方法，植基於 ElGamal 之變型系統，為在群體簽章方式之群導向數位簽章系統下，用以防止用戶在無意下簽出文件之控管方法，上述系統存在一生成子 g 及一大質數 P，用戶端使用者之私密金鑰為

五、發明說明（11）

us，而其相對應之公開金鑰為 up=g^{us} mod P，伺服端私密金鑰為 ss，而其相對之公開金鑰為 sp=g^{ss} mod P，而兩者對外之共通公開金鑰為 Y=(up×sp) mod P，上述控管方法之特徵在於：當用戶端之使用者欲簽出文件(M)時，用戶端與伺服端依下列步驟進行簽章過程及驗證過程：

I. 簽章過程時：

[a]用戶端與伺服端分別產生隨機變數 k1 及 k2；

[b]用戶端計算 r1=g^{k1} mod P，同時伺服端也計算 r2=g^{k2} mod P，之後用戶端與伺服端互相交換 r1 及 r2；

[c]用戶端與伺服端均計算 R=(r1×r2) mod P；

[d]用戶端先驗證 sp^{M} 與($r2^{R}\times g^{ss}$)mod P 是否相等，若兩者相等則用戶端計算 S1=(us×M-k1×R)mod (P-1)；及

[e]伺服端驗證 up^{M} 與($r1^{R}\times g^{us}$)mod P 是否相等，若兩者相等則伺服端計算 S2=(ss×M-k2×R) mod (P-1)，若不相等則結束簽章程式重頭進行；否則 SIG=(R, S = (S1+S2) mod P-1)即作為對文件 M 之簽章。

II. 在驗證過程時：

以共通公開金鑰 Y 驗證 Y^{M} mod P 是否與 $R^{R}\times g^{S}$ mod P 相等，若相則表示 SIG 為文件 M 之正確簽章，否則不是正確的簽章。

由上述可知，本機制其文件之簽出，須先經由用戶端簽章後，再經由伺服端簽過一次，所以具有雙重驗證之功能，所以不會發生因使者疏忽下或操作錯誤之情形下，而簽出文件。

五、發明說明（18）

實施例四之一：(金鑰回復機制)

一種識別卡安全控管方法，可藉以建構成使用於儲存裝置之金鑰回復系統，上述系統可建置於一金鑰交換系統其已公佈一公開值(M)，以及具有第一金鑰回復中心(TKRC1)及第二金鑰回復中心(TKRC2)之作業環境下，上述金鑰回復系統之控管方法如下步驟：

[a]用戶端與伺服端先執行如第二實施例所示，相互認證之程序，認證完成後伺服端可得一加密金鑰(SK)及儲存裝置上之私密資料(DK)，並由自己所選之密碼而獲得 PWK。

[b]用戶端產生兩大質數 p 和 q，其中 p×q=N，N 為一模數。

[c]用戶端與第一金鑰回復中心(TKRC1)利用上述金鑰交換系統或是執行上述相互認證之程序而獲得一第一共享金鑰(SK1)，同時亦與第二金鑰回復中心(TKRC2)進行相同之程序而獲得一第二共享金鑰(SK2)。

[d]第一與第二金鑰回復中心(TKRC1 和 TKRC2)分別產生一第一媒介數(R1)和第二媒介數(R2)，再分別利用其與用戶端間之第一和第二共享金鑰(SK1 和 SK2)，而對上述之第一與第二媒介數加密後，傳送給用戶端。

[e]用戶端接到上述第一和第二媒介數後，藉兩者以產生一公開金鑰(PK)，若無法產生上述公開金鑰(PK)則重覆步驟 c、d、e 直到可以得出一公開金鑰為止；其中上述公開金鑰 PK 符合下列之式子，PK×(f(R1 , R2)) = 1

五、發明說明（19）

mod F(N)，其中 F(N)=(p-1) × (q-1)或 F(N)為(p-1)和(q-1)之最小公倍數，而用戶端相對於 PK 之私密金鑰為 S = f(R1,R2) mod F(N)。而上述 f(R1,R2)可依需要選擇為 R1+R2 或 R1×R2。

[f]用戶端計算 M^{PK} mod N 而得一生成子 C，並將上述生成子 C、公開金鑰 PK、及模數 N 傳送給上述第一金鑰回復中心(TKRC1)，及第二金鑰回復中心(TKRC2)，並將上述公開金鑰 PK、模數 F(N)傳送至一認證中心 CA。

[g]第一金鑰回復中心(TKRC1)計算 $M1 = C^{R1}$ mod N 後，並將其傳送給第二金鑰回復中心(TKRC2)，同時，第二金鑰回復中心(TKRC2)計算 $M2=C^{R2}$ mod N，並將其傳送給第一金鑰回復中心(TKRC1)；

[h]第一金鑰回復中心(TKRC1)計算 $M1^* = C^{R1}$ mod N、或 $M1^* =(C^{R1}\times C^{R2})$mod F(N)其端視所選擇之 f(R1 , R2)而定，並驗證檢查 M1*是否等於 M，同時，第二金鑰回復中心(TKRC2)計算 $M2^* = C^{R2}$ mod N、或 $M2^* =(C^{R2}\times C^{R1})$mod F(N)其端視所選擇之 f(R1 , R2)而定，並驗證檢查 M2*是否等於 M，若通過驗證，則其中第一和第二金鑰回復中心分別利用其各自之的私密金鑰對公開金鑰 PK 及模數 N 簽章後再將其傳送至上述認證中心 CA。

[i]上述認證中心收到第一和第二金鑰回復中心對公開金鑰 PK 及模數 N 之簽章後，待驗證通過後即對 PK 及 N 作一憑證證明，再回傳給用戶端之使用者；

五、發明說明（20）

[j]用戶端則可使用加密金鑰 SK，私密資料 DK 及 PWK 加密用戶之私密金鑰 S 及其他個人私密金鑰。

如上所述，當用戶之金鑰遺失或有爭端，而必須由第三者舉證時，即由第一和第二金鑰回復中心及認證中心呼叫出相關之資料，如 R1 和 R2 藉 S=(R1×R2)mod F(N)、或 S=(R1+R2)mod F(N)其端視所選之 f(R1 , R2)而定，以導出用戶端私密金鑰 S。

實施例四之二：(金鑰回復機制)

一種識別卡安全控管方法，可藉以建構成使用於儲存裝置之金鑰回復系統，上述系統可建置於一金鑰交換系統其已公佈一公開值(M)，以及具有第一金鑰回復中心(TKRC1)及第二金鑰回復中心(TKRC2)之作業環境下，上述金鑰回復系統其植基於解離散對數困難度的密碼系統已存在一大質數 P 及產生子 g，其控管方法如下步驟：

[a]用戶端與伺服端先執行一如第二實施例之相互認證之程序，認證完成後伺服端可得一加密金鑰(SK)及儲存裝置上之私密資料(DK)，並由自己所選之密碼而獲得之 PWK。

[b]用戶端與第一金鑰回復中心(TKRC1)利用上述金鑰交換系統或是執行上述相互認證之程序而獲得一第一共享金鑰(SK1)，同時亦與第二金鑰回復中心(TKRC2)進行相同之程序而獲得一第二共享金鑰(SK2)。

[c]第一金鑰回復中心(TKRC1)產生一第一媒介數(R1)，利用其與用戶端間的共享金鑰 SK1 加密後傳送給

五、發明說明（21）

用戶端，並計算 $C1=g^{R1} \bmod P$，再將 C1 送至第二金鑰回復中心(TKRC2)，同時，第二金鑰回復中心(TKRC2)產生一第二媒介數(R2)，利用其與用戶端間的共享金鑰 SK2 加密後傳送給用戶端，並計算 $C2=g^{R2} \bmod P$，再將 C2 送至第一金鑰回復中心(TKRC1)。

[d]用戶接到第一和第二金鑰回復中心所送來之上述第一和第二媒介數 R1、R2 後，藉兩者以產生一公開金鑰 $PK = g^{f(R1,R2)} \bmod P$，則使用者相對於 PK 之私密金鑰 S 為由 f(R1, R2) mod (P-1)而得，為上述第一和第二媒介數 R1、R2 之一特定運算值，可視需要，將上述 f(R1, R2)選擇為 R1+R2 或 R1×R2。

[e]用戶端將 PK 傳送給第一金鑰回復中心(TKRC1)、第二金鑰回復中心(TKRC2)，與一認證中心 CA。

[f]若 f(R1, R2)=R1×R2 則，第一金鑰回復中心(TKRC1)計算 $M1=PK^{inv(R1)} \bmod P$ 後並比較驗證 M1 是否等於 C2，同時，第二金鑰回復中心(TKRC2)計算 $M2=PK^{inv(R2)} \bmod P$ 後並比較驗證 M2 是否等於 C1，其中 inv(R1)表示 $(R1)^{-1} \bmod P-1$ 之運算。若 f(R1 , R2)=R1+R2 則第一金鑰回復中心(TKRC1)計算 $M1=PK\times g^{inv(R1)} \bmod P$ 後對比較 M1 是否等於 C2，同時 TKRC2 計算 $M2=PK\times g^{inv(R2)} \bmod P$ 後並比較 M2 是否等於 C1。

[g]若通過驗證後，第一和第二金鑰回復中心以其各自的私密金鑰對 PK 簽章後，再傳送至上述認證中心

五、發明說明（22）

CA。

[h]上述認證中心收到第一和第二金鑰回復中心對PK之簽章後，待驗證通過後即對PK作一憑證證明後，再回傳給用戶端。

[i]用戶端使用加密金鑰SK，私密資料DK及PWK，來加密私密金鑰S及用戶其它個人私密資料。

如上所述，當用戶之金鑰遺失或有爭端，而必須由第三者舉證時，即由第一和第二金鑰回復中心及認證中心呼叫出相關之資料，如R1和R2，即可藉 S=(R1×R2) mod (P-1)、或 S=(R1+R2) mod (P-1)而導出用戶端私密金鑰S。

實施例五：(回復金鑰加解密機制)

一種識別卡安全控管方法，藉此方法構成一回復金鑰加解密系統，上述回復金鑰加解密系統之控管方法包括：

資料傳送及驗證程序，係為正常情形下之資料傳送程序；以及

金鑰及密文的回復程序，藉以當發文端之金鑰或明文遺失時，能利用此一機制將之回復；

上述資料傳送及驗證程序，請參照第3A圖所示之方塊圖，其包括如下步驟：

[a]當發文端欲傳送明文資料M給收文單位時，發文單位先產生一通訊基碼SK(又稱為會談金鑰)，再由一發文端加解密器ENS，以發文端之私密金鑰KGS對上述通

五、發明說明（23）

訊基碼 SK 進行加密而得$(SK)_{KGS}$，並以收文端之公開金鑰 PKR 對上述通訊基碼 SK 進行加密而得$(SK)_{PKR}$，將上述通訊基碼 SK 與上述$(SK)_{KGS}$進行特定之運算而得一發文端密鑰，在此實施例為互斥運算，所以發文端密鑰為$SK \oplus (SK)_{KGS}$。

以上述發文端密鑰對所欲傳送之明文資料 M 進行加密而得一密文 $SM=(M)_{SK\oplus(SK)_{KGS}}$，對上述通訊基碼 SK、$(SK)_{KGS}$、$(SK)_{PKR}$及特定相關資料，(例如，發文端之機關代碼 IDS、收文端之機關代碼 IDR、及一初始向量值 IV 等)進行雜湊運算而得到一信託認證子 EA。再以一家族金鑰 FK 對上述對上述$(SK)_{KGS}$、$(SK)_{PKR}$、特定相關資料 IDR 和 IDS、以及信託認證子 EA 進行加密而得一法定存取欄位 LEAF，再將上述密文 SM、法定存取欄位 LEAF、以及初始向量值 IV 傳送至收文端。

[b]收文端接收上述資料後，利用家族金鑰 FK 解開 LEAF 而得到上述$(SK)_{KGS}$、$(SK)_{PKR}$、信託認證子 EA、以及特定相關資料 IDS、IDR、及 IV。利用收文端私密金鑰 KGR 解開$(SK)_{PKR}$而得上述通訊基碼 SK，以通訊基碼 SK 將所接收之上述$(SK)_{KGS}$還原而可得上述發文端密鑰$SK \oplus (SK)_{KGS}$，再利用發文端密鑰解開密文 $SM=(M)_{SK\oplus(SK)_{KGS}}$而得到明文資料 M；以及

[c]收文端並對所接收後解得之上述通訊基碼 SK、$(SK)_{KGS}$、$(SK)_{PKR}$、及特定相關資料 IDS、IDR、及 IV 進行雜湊運算，其運算結果用以與所接收到之信託認證子

五、發明說明（24）

EA 互相比對，若相等則表示驗證成功傳輸過程無誤。

其中上述收文端金鑰 KGR 是由一第一金鑰管理單位和第二金鑰管理單位分別提供之收文端第一金鑰因子 KGR1 與收文端第二金鑰因子 KGR2，兩者經特定運算後而得，另外上述發文端金鑰 KGS 是由一第金鑰管理單位和第二金鑰管理單位分別提供之收文端第一金鑰因子 KGS1 與收文端第二金鑰因子 KGS2，兩者經特定運算後而得。在此實施例中 KGR = KGR1 ⊕ KGR2，KGS = KGS1 ⊕ KGS2。

當發文端之金鑰或明文遺失時，請參照第 3B 圖所示之方塊圖，上述金鑰及密文的回復程序，其包括如下步驟：

發文端先要求上述第一金鑰管理單位及第二金鑰管理單位取出第一金鑰因子 KGS1 與收文端第二金鑰因子 KGS2，由 KGS1 與 KGS2 即可經互斥運算而得發文端金鑰 KGS；

利用回復之發文端金鑰 KGS，即可將 $(SK)_{KGS}$ 解開而得上述通訊基碼 SK，再利用上述通訊基碼 SK 與 $(SK)_{KGS}$ 進行互斥運算而得到上述發文端密鑰 $SK \oplus (SK)_{KGS}$，利用此一發文端私密金鑰即可以將密文解開而得到明文資料。

由上所述，利用本發明之回復金鑰加解密機制，其可在金鑰遺失之場合，輕易地將金鑰恢復，再藉以將密文解出回復，可避免因金鑰遺失而遭致漏失資料之情形

五、發明說明（25）

發生。

實施例六：(所有權驗核機制)

一般所有權驗核機制，在理論上可使用資料隱藏法技術在文件中藏入不易查覺之資訊做為所有權之證據。然而，以文件而言所加入之隱藏資訊，確可能因為使用軟體之不同，而改變了隱藏的資訊，而使所有權之歸屬有所爭議。另外，亦有藉改變文件內容之語法、語意、同義字或文句中標點等，將額外的資訊藏入原文中。然而此類方法，其實作困難且改變文件之表達方式，可能造成閱讀上的不順暢，所以並不切實際。

本發明之所有權機制，利用密碼技術實現電子文件所有權驗核之機制，其可在不修改文件原文之內容的前提下，能做到保護發文者的擁有權及文件之完整性。

擁有權機制所要處理之情形為，當一份文件被不當使用(例如有人冒用發文者發佈不實文件)時，發文者可透過公正程序證明該文件並非屬於發文者所有。

本發明所提出之一種所有權驗核機制，其透過密碼學上之技巧，建立一份與其前、後各文件間之關連性，以確保他人無法在已發出的文件間插入其他偽造之文件。此一關連性可經由一公正當局在適當時加以揭示，以確保發文者之所有權不被他人所冒用。

本發明之所有權驗核機制，可由發文端 A、收文端 B、及所有權公正機關 TKC 及公正機關 TTP 互相連動運作。而發文端 A 與所有權公正機關間之所有訊息交換均

五、發明說明（26）

經公證處理，以確保雙方文件交換之不可否認性，詳細交換過程如下：

I.初始階段：

在第一次登入時，於發文端 A 隨機選取一數字 N_0。

於發文端 A 產生所有權簽署金鑰對 A_{os}、A_{op}，以及通訊金鑰 K_{AT}。

以及，發文端 A 經由公證程序將 A_{os} 及 K_{AT} 送交上述所有權公正機關 TKC。

II.第一次文件傳輸：

a.對第一份文件 M_1 產生一第一文件表頭 $M_{T1}=ID_A+S_1+h(M_1)+A_S\{h(N_0+ID_A+S_1)\}$，其中 ID_A 為發文端 A 之身份識別碼，S_1 為第一份文件之序號，A_S 為發文端 A 之文件簽署密鑰，$h(\cdot)$表雜湊函數。

b.發文端 A 利用所有權簽署金鑰 A_{os} 對上述第一文件表頭 M_{T1} 簽章而得第一表頭簽章 $A_{os}\{M_{T1}\}$，發文端合併 ID_A、公正機關身份識別碼 ID_{TTP}、收文端身份識別碼 ID_B、文件表頭 M_{T1}、及第一表頭簽章 $A_{os}\{M_{T1}\}$後以通訊金鑰 K_{AT} 加密，再將其與第一份文件之表頭 M_{T1} 傳送至公正機關 TTP。

c.公正機關 TTP 收到後，令 T_1 等於上述第一文件表頭 M_{T1}，並將 ID_A、ID_B、$A_{os}\{T_1\}$、以及 T_1 儲存。d.發文端 A 將 $ID_A+A_{os}\{T_1\}+M_1$ 以公證程序送交收文端 B。

e.收文端 B 將 $A_{os}\{T_1\}$及文件序號、收文方等文件識別資訊以 K_{BT} 加密後，以 TTP 之公開金鑰 TTP_P 加密後，

五、發明說明（21）

送交 TTP。

f. TTP 以其私密金鑰 TTP_S 解開上述密文後比較步驟 e 中之 $A_{os}\{T_1\}$ 是否相同，並將比較結果以 K_{BT} 加密後送給 B。

g.若步驟 f 中之較結果為相同則 B 執行步驟 h，否則 B 可要求 A 動新執行步驟 d。

h.最後收文端 B 儲存 $A_{os}\{T_1\}$。

III.第 i 次文件傳輸：

a.發文端 A 對第 i 份文件產生第 i 文件表頭 $M_{Ti}=ID_A + S_i + h(M_i) + (A_{op} \oplus h(T_{i-1})$，其中 S_i 為第 i 份文件之序號。

b.發文端 A 利用所有權簽署金鑰 A_{os} 對上述第 i 文件表頭 M_{Ti} 簽章而得第一表頭簽章 $A_{os}\{M_{Ti}\}$，發文端 A 合併 ID_A、公正機關身份識別碼 ID_{TTP}、收文端身份識別碼 ID_B、文件表頭 M_{Ti}、及第 i 表頭簽章 $A_{os}\{M_{Ti}\}$ 後以通訊金鑰 K_{AT} 加密，再將其與第 i 份文件之表頭 M_{Ti} 傳送至公正機關 TTP。

c.公正機關 TTP 收到後，令 T_i 等於上述第 i 文件表頭 M_{Ti} 與第 i-1 次文件表頭 $T_{i-1}=M_{Ti-1}$ 之互斥運算值 $M_{Ti} \oplus T_{i-1}$，並將 ID_A、ID_B、$A_{os}\{M_{Ti}\}$、以及 T_i 儲存。

d.將 T1 以 Ti 取代，重覆第一次傳輸中之步驟 d～h，如此來從事正常之文件傳送。

依上述機制運作之文件系統，當收文端 B 提出 M* 及 $A_{os}\{M_{Ti}\}$，欲證明 M*為發文端 A 所送出之文件，則公正機關 TTP 可公佈 A_{op} 並解出 M_{Ti}，再根據 M_{Ti} 之內容確

五、發明說明（28）

定文件是否為發文端 A 所發出，若 M*為事後偽造之文件，則根據 T_i 及 M_{Ti} 之關連性，TTP 可證明 M*非由發文端所發出，其前後文件之關連性如下：

往前關連性為 $M_{Ti}=T_i \oplus T_{i-1}$；

往後關連性為自 M_{Ti+1} 中取出 $(A_{op} \oplus h(T_i)$ 欄位，$h(T_i)=(A_{op} \oplus h(T_i)) \oplus A_{op}$。

由上述可知，本發明之所有權核驗機制，其透過密碼學之技巧，建立各文件間之前後關連性。如此一來，縱使簽章系統被破解之情形下，仍不會有被仿冒、偽簽之危險。因為，入侵者無法得知文件間之關連性，故而無法在已發出之文件插入其他偽造之文件。而此一機制也藉由關連性而可輕易地驗證文件之所有權歸屬。

根據本發明之安全控管方法有：

一、檢驗系統檔案有無遭篡改的檢查機制。

二、植基相互認證系統的控管機制。

三、使用於簽章控管的群體導向數位簽章機制。

四、金鑰回復機制。

五、回復金鑰加解密機制。

六、所有權驗核機制。

由上述之各種控管方法，可確知本發明對於網路環境下運作之系統可提供較佳之保密及保障，尤其對於用戶端之使用者之防護能更具有可靠性和安全性，本發明所提出一套識別卡安全控管方法，其對於用戶端的軟體及存於可攜式儲存裝置的私密資料，如私密金鑰等，利

五、發明說明（29）

用密碼學加解密、電子簽章技術、以及分散機密的觀念來加以保護，以提高入侵者破解機密而危害系統的困難度。而對於使用者的私密金鑰遺失後金鑰回復之措施亦提出一可行之方案。另外，亦提出一所有權驗核機制而達到發文者擁有權及對文件完整性能有所保護之目的。

上述相關之實施例中，本發明有使用到可應用儲存裝置之系統，而儲存裝置中的內容不外乎為：

一、測試程式，用以測試欲測程式之版本，及程式之正確性。

二、個人之機密資料，包括個人私密金鑰等。

三、公開資料，如驗證碼(Certificate)、使用者 ID、用戶相關資料、磁片編號等。

四、測試資料，如程式雜湊值之簽章、程式版本及日期之簽章等。

上述各項可視所需之情形而調整。

雖然本發明已以多個較佳實施例揭露如上，然其並非用以限定本發明，任何熟悉本項技藝者，在不脫離本發明之精神和範圍內所提出之測試機制，均係涵括在本發明之保護範圍內。

四、中文發明摘要（發明之名稱：　　）

識別卡安全控管方法

在網路環境下用戶端往往是防護最少的部份，常是最容易遭受入侵者侵犯的對像。為使用戶端之防護能更具有可靠性和安全性，本發明提出一套識別卡安全控管方法，其對於用戶端的軟體及存於儲存裝置的私密資料，如私密金鑰等，利用密碼學加解密、電子簽章技術、以及分散機密的觀念來加以保護，以提高入侵者破解機密而危害系統的困難度。而對於使用者的私密金鑰遺失後金鑰回復之措施亦提出一可行之方案。另外，亦提出一所有權驗核機制而達到發文者擁有權及對文件完整性能有所保護之目的。

英文發明摘要（發明之名稱：　　）

四、中文發明摘要（發明之名稱：　　）

識別卡安全控管方法

在網路環境下用戶端往往是防護最少的部份，常是最容易遭受入侵者侵犯的對像。為使用戶端之防護能更具有可靠性和安全性，本發明提出一套識別卡安全控管方法，其對於用戶端的軟體及存於儲存裝置的私密資料，如私密金鑰等，利用密碼學加解密、電子簽章技術、以及分散機密的觀念來加以保護，以提高入侵者破解機密而危害系統的困難度。而對於使用者的私密金鑰遺失後金鑰回復之措施亦提出一可行之方案。另外，亦提出一所有權驗核機制而達到發文者擁有權及對文件完整性能有所保護之目的。

英文發明摘要（發明之名稱：　　）

修正 本98年10月6日
補充

六、申請專利範圍

1.一種識別卡安全控管方法，其包含二個程序：檢驗軟體安裝程序，以及程式偵試程序；

其中之檢驗軟體安裝程序包括如下之步驟：

將用戶端電腦系統中欲控管之軟體的根目錄下各子目錄底下之每一檔案，利用安全雜湊函數以產生相對應之第一檔案雜湊值，並儲存於該用戶端電腦系統中；

分別將上述各子目錄中之第一檔案雜湊值加以結合，再利用安全雜湊函數產生相對應之第一目錄雜湊值，並將該第一目錄雜湊值分別儲存於上述各子目錄中；

如此重覆，對該根目錄下的各層下子目錄作相同之動作，以得到各相對應之檔案雜湊值及目錄雜湊值，並分別儲存於用戶端電腦系統及各子目錄中，直到位於該根目錄下所有之子目錄均有其相對之目錄雜湊值，再於該根目錄下，將該根目錄下之目錄雜湊值加以結合，並利用安全雜湊函數產生一第一根目錄雜湊值；

利用用戶端的私密金鑰而將此第一根目錄雜湊值加以簽章，並將此簽章結果及一程式檢驗程式存在一可攜式儲存裝置(即識別卡)中；

而程式偵試程序則執行前述可攜式儲存裝置中之程式檢驗程式，以證驗該用戶端之程式有否遭篡改或是版本不符之情形；

該檢驗程式之步驟如下：

將用戶端電腦系統欲偵試之軟體的根目錄下之子目錄中每一檔案，利用安全雜湊函數產生相對應之第二檔

修正 本98年10月6日
補充

六、申請專利範圍

1.一種識別卡安全控管方法，其包含二個程序：檢驗軟體安裝程序，以及程式偵試程序；

其中之檢驗軟體安裝程序包括如下之步驟：

將用戶端電腦系統中欲控管之軟體的根目錄下各子目錄底下之每一檔案，利用安全雜湊函數以產生相對應之第一檔案雜湊值，並儲存於該用戶端電腦系統中；

分別將上述各子目錄中之第一檔案雜湊值加以結合，再利用安全雜湊函數產生相對應之第一目錄雜湊值，並將該第一目錄雜湊值分別儲存於上述各子目錄中；

如此重覆，對該根目錄下的各層下子目錄作相同之動作，以得到各相對應之檔案雜湊值及目錄雜湊值，並分別儲存於用戶端電腦系統及各子目錄中，直到位於該根目錄下所有之子目錄均有其相對之目錄雜湊值，再於該根目錄下，將該根目錄下之目錄雜湊值加以結合，並利用安全雜湊函數產生一第一根目錄雜湊值；

利用用戶端的私密金鑰而將此第一根目錄雜湊值加以簽章，並將此簽章結果及一程式檢驗程式存在一可攜式儲存裝置(即識別卡)中；

而程式偵試程序則執行前述可攜式儲存裝置中之程式檢驗程式，以證驗該用戶端之程式有否遭篡改或是版本不符之情形；

該檢驗程式之步驟如下：

將用戶端電腦系統欲偵試之軟體的根目錄下之子目錄中每一檔案，利用安全雜湊函數產生相對應之第二檔

六、申請專利範圍

案雜湊值，並檢查該第二檔案雜湊值與儲存於用戶端之第一檔案雜湊值是否相等，若不相等則停止此程序；

該檢驗程式再以如上述安裝程序之過程，而分別將各子目錄中之第二檔案雜湊值加以結合，再利用安全雜湊函數產生相對應之第二目錄雜湊值，並將其與分別儲存於各子目錄中之第一目錄雜湊值加以比較，若不相等則停止此程序；

對各層下子目錄重覆上述之檢查動作，直到位於根目錄下所有之子目錄均有其相對之目錄雜湊值且均通過驗證，再於根目錄下將根目錄下之目錄雜湊值加以結合，並再利用安全雜湊函數產生一第二根目錄雜湊值，將其與儲存於用戶端之第一根目錄雜湊值相比較，若不相等則停止此程序；

對前述第二根目錄雜湊值加以簽章，並自上述可攜式儲存裝置中讀出前述第一根目錄湊值之簽章結果，驗正兩簽章結果是否相符合，若不符合則表示該用戶端之程式有遭篡改或是版本不符之情形。

2.一種識別卡安全控管方法，此安全控管方法包含註冊程序；認證程序；以及更換密碼程序三個程序；

其中之註冊程序包括如下步驟：

[a]上述用戶端利用其識別碼(ID)、一會談金鑰(TK)、一第一驗證因子(N1)、及相關資料，合併產生一用戶端第一簽體，用戶端對該用戶端第一簽體以伺服端之公開金鑰(K_{SP})進行加密，而得用戶端第一密件(C1)，將該用戶

六、申請專利範圍

端第一密件(C1)、識別碼(ID)、一註冊請求 (Reg_req)，及相關資料傳送至伺服端；

[b]伺服端接收到上述註冊請求(Reg_req)後，以伺服端私密金鑰 K_{SS} 解開上述用戶端第一密件 C1 而獲得前述之會談金鑰(TK)、第一驗證因子(N1)、及識別碼(ID)等相關資料，伺服端並產生一加密金鑰(SK)、一第二驗證因子(N2)、及一整數 n，伺服端以上述之加密金鑰(SK)、整數 n、第一驗證因子(N1)、第二驗證因子(N2)、以及相關資料合併產生一伺服端第一簽體，以前述會談金鑰(TK)對該伺服端第一簽體加密而得一伺服端第一密件(S1)，再將其回傳給用戶端；

[c]用戶端完成接收後，以上述之會談金鑰(TK)解開該伺服端第一密件(S1)，而得上述整數 n、上述加密金鑰(SK)、上述第一驗證因子(N1)與第二驗證因子(N2)，用戶端檢查上述第一驗證因子(N1)是否為原先所送之值，驗證正確後用戶端將使者個人密碼(PWD)進行 n 次雜湊運算而得一密碼封包(OTP)；

[d]用戶端以上述密碼封包(OTP)、上述第二驗證因子(N2)、及相關之資料為用戶端第二簽體，利用上述會談金鑰(TK)對上述用戶端第二簽體進行加密而得一用戶端第二密件後，將其傳送給伺服端；

[e]伺服端接收到上述用戶端第二密件後，以上述之會談金鑰(TK)解開上述第二密件，而得上述之密碼封包(OTP)，伺服端並驗證上述第二驗證因子是否為原先所送

六、申請專利範圍

之值，若正確無誤則將上述之密碼封包(OTP)、以及整數n儲存於伺服端，並產生一註冊標記(Reg_yes)，伺服端利用上述密碼封包(OTP)、註冊標記(Reg_yes)為伺服端第二簽體，以上述會談金鑰對上述伺服端第二簽體進行加密而得一伺服端第二密件，再將其回傳給用戶端；

[f]用戶端以會談金鑰解開上述伺服端第二密件，而接收上述註冊標記(Reg_yes)確認註冊無誤後，即自行產生一用戶端金鑰(CK)並且利用使用者密碼(PWD)導出一密碼金鑰(PWK)，再使用上述加密金鑰(SK)與密碼金鑰(PWK)將上述用戶端金鑰(CK)加密成為用戶端密文(ECK)並將其結果存於用戶端上，另外亦使用上述用戶端金鑰(CK)與密碼金鑰(PWK)對使用者之私密資料(DK)加密成為一密文，並將之存於可攜式儲存裝置上，而完成註冊之程序；

其中之認證程序包括如下步驟：

[i]用戶端將其識別碼(ID)，一第三驗證因子(N3)、與此程序所要使用之會談金鑰(TK1)合併產生一用戶端第三簽體，用戶端對該用戶端第三簽體以伺服端之公開金鑰(K_{SP})進行加密，而得用戶端第三密件(C3)，並將該用戶端第三密件(C3)、上述識別碼(ID)、一確認請求(Auth_req)，及相關資料傳送至伺服端；

[ii]伺服端接收到確認請求(Auth_req)後，以伺服端私密金鑰K_{SS}解開上述用戶端第三密件C3而獲得前述之會談金鑰(TK1)、第三驗證因子(N3)、及識別碼(ID)等相

六、申請專利範圍

關資料，伺服端並找出使用者於上述註冊程序中所對應之密碼封包(OTP)、以及整數 n 等相關資料，若整數 n 小於 2 則用戶端之使用者須重新註冊，若整數 n 不小於 2，則伺服端產生一小於 n 的整數 k 及 m 而 m=n-k，再將會談金鑰 TK1、整數 m、第三驗證因子(N3)及相關資料合併為伺服端第三簽體(S3)，以會談金鑰(TK1)對其加密而得伺服端第三密件，並將伺服端第三密件回傳給用戶端；

[iii]用戶端完成接收後，以上述之會談金鑰(TK1)解開上述伺服端第三簽章(S3)，而得上述整數 m、上述第三驗證因子(N3)，用戶端檢查上述第三驗證因子(N3)是否為原先所送之值，驗證正確後用戶端將使者輸入之個人密碼(PWD)進行 m 次雜湊運算而得一第一封包(OTP1)，並產生一第四驗證因子(N4)；

[iv]用戶端以上述第一封包(OTP1)、上述第四驗證因子(N4)、及相關之資料合併為用戶端第四簽體，利用上述會談金鑰(TK1)對上述用戶端第四簽體進行加密而得一用戶端第四密件後，將其傳送給伺服端；

[v]伺服端接收到上述用戶端第四密件後，以上述之會談金鑰(TK1)解開上述第四密件，而得上述之第一封包(OTP1)，伺服端並驗證上述第四驗證因子(N4)是否為原先所送之值，若正確無誤則伺服端對上述第一封包(OTP1)進行 k 次雜湊算，其運算結果與註冊程序中儲存於伺服端之密碼封包比對是否相同，驗證正確後即儲存整數 m 於伺服端而取代原先之整數 n，同時儲存上述第一封包

六、申請專利範圍

(OTP1)取代原來的密碼封包，之後將上述註冊程序中產生之加密金鑰(SK)、第一封包(OTP1)、及驗證成功之訊息合併為伺服第四簽體，將其以會談金鑰加密後回傳給用戶端；

[vi]用戶端以會談金鑰(TK1)解開上述加密資料，分別得到加密金鑰(SK)、第一封包(OTP1)、及驗證成功之訊息，確定驗證成功後，用戶端使用上述加密金鑰(SK)與密碼金鑰(PWK)對存於存於用戶端上之密文(ECK)解密以得到上述之註冊程序中之用戶端金鑰(CK)，使用該用戶端金鑰(CK)、密碼金鑰(PWK)和加密金鑰(SK)，對存於可攜式儲存裝置中之密文加以解密而得到使用者之私密資料(DK)，完成認證；

其中之更換密碼程序包括如下步驟：

[A]用戶端將其識別碼(ID)，一第五驗證因子(N5)、與此程序所要使用之會談金鑰(TK2)合併產生一用戶端第五簽體，用戶端對上述用戶端第五簽體以伺服端之公開金鑰(K_{SP})進行加密，而得用戶端第五密件(C5)，並將上述用戶端第五密件(C5)、上述識別碼(ID)、一密碼更換請求(CP_req)，及相關資料傳送至伺服端；

[B]伺服端接收到密碼更換請求(CP_req)後，以伺服端私密金鑰 K_{SS} 解開上述用戶端第五密件 C5 而獲得上述之會談金鑰(TK2)、第五驗證因子(N5)、及識別碼(ID)等相關資料，伺服端並找出使用者於上述註冊程序中所對應之整數 n 資料，伺服端再產生一正整數 m=n-k、及整

六、申請專利範圍

數 I，其中 k 也為整數，再將整數 m、I、第五驗證因子(N5)及相關資料合併為伺服端第五簽體(S5)，以會談金鑰(TK2)對其加密而得伺服端第五密件，並將伺服端第五密件回傳給用戶端；

[C]用戶端完成接收後，以上述之會談金鑰(TK2)解開上述伺服端第五密件(S5)，而得上述整數 m、I、上述第五驗證因子(N5)，用戶端檢查上述第五驗證因子(N5)是否為原先所送之值，驗證正確後用戶端將使者輸入之個人密碼(PWD)進行 m 次雜湊運算而得一第一封包(OTP1)，並產生一第六驗證因子(N6)，同時對使用者所輸入之新密碼 NPWD 進行 I 次雜湊運算，而得一第二封包(OTP2)；

[D]用戶端以上述第一封包(OTP1)、第二封包(OTP2)上述第六驗證因子(N6)、及相關之資料合併為用戶端第六簽體，利用上述會談金鑰(TK2)對上述用戶端第六簽體進行加密而得一用戶端第六密件後，將其傳送給伺服端；

[E]伺服端接收到上述用戶端第六密件後，以上述之會談金鑰(TK2)解開上述第六密件，而得上述之第一封包(OTP1)和第二封包，伺服端並驗證上述第六驗證因子(N6)是否為原先所送之值，若正確無誤則伺服端對上述第一封包(OTP1)進行 k 次雜湊算，其運算結果與註冊程序中儲存於伺服端之密碼封包比對是否相同，驗證正確後即儲存整數 I 於伺服端而取代原先之整數 n，也將第二封包儲存於伺服端，並產生一新加密金鑰 NSK，將註冊程序

六、申請專利範圍

產生之加密金鑰 SK 和新加密金鑰(NSK)、以及第一封包(OTP1)與第二封包(OTP2)、及更換成功之訊息 CP_yes 合併為伺服第六簽體，將其以會談金鑰加密後回傳給用戶端；

[F]用戶端以會談金鑰(TK2)解開上述加密資料後，而分別得到加密金鑰(SK)、新加密金鑰 NSK，第一封包(OTP1)和第二封包(OTP2)、及更換成功之訊息 CP_yes，確定更換成功後，先以 PWK 及 SK 解出存於用戶端的 ECK，再用 CK 合併使用者的個人密碼所導出的金鑰 PWK 以及 SK 解出原先加密存於可攜式儲存裝置中的密鑰密文 EDK，之後用戶端即自行產生一用戶端新金鑰(NCK)，以先前獲得之 NSK 使用者之新密碼 NPWD 所導出的 NPWK 加密儲存於用戶端，再以 NPWK、NSK 及 NCK 加密 DK 而將結果存於可攜式儲存裝置中。

3.如申請專利範圍第 2 項所述之安全控管方法，其中在所有程序裡，伺服端產生的所有簽體中包括有系統時間，以供用戶端收到每個簽體所對應之密件時可用以驗證傳輸時間是否在合理之範圍內，而用戶端產生的所有簽體中亦包括有系統時間，以供伺服端收到簽體所對應之密件時可用以驗證傳輸時間是否在合理之範圍內，藉以防止密件於傳送途中遭人攔截篡改。

4.如申請專利範圍第 2 或 3 項所述之安全控管方法，其中在所有程序中，伺服端產生加鹽值且合併入簽體中傳送給用戶端，用戶端則對使用者密碼和加鹽值之

六、申請專利範圍

合併值進行雜湊運算而產生各個程序中之各個密碼封包。

5.一種識別卡安全控管方法，其包括如下步驟：

當要簽出文件時，以用戶端使用者之私密金鑰先行對上述文件簽章而得一第一簽章，再以伺服端之私密金鑰對上述第一簽章再行簽章而得到一第二簽章，而完成簽章之過程；以及

在驗證過程中，將上述第二簽章先以伺服端之公開金鑰解開而得一驗證簽章，再將上述驗證簽章以使用者之公開金鑰解開而得一驗證文件，比較上述第一驗證文件與上述原先送出之文件是否相同，若正確則表示簽章係為正確無誤。

6.一種識別卡安全控管方法，其包括如下步驟：

用戶端與伺服端之公開金鑰分別為 up 及 sp，其模數為 Nu 和 Ns，而其相對應之之私密金鑰分別為 us 和 ss；在簽章過程時，首先以用戶端的私密金鑰 us 對文件 M 簽章而得 $SIG1=M^{us} \bmod Nu$，再用伺服端的私密金鑰 sp 對 SIG1 簽章而得 $SIG2=SIG1^{ss} \bmod Ns$；

在驗證過程時，收文者要驗證文件 M 之簽章 SIG2 時，先用伺服端的公開金鑰 sp 計算 $SIG2^{sp} \bmod Ns$ 而解得 SIG1，再以用戶端之公開金鑰 up 計算 $SIG1^{up} \bmod Nu$ 而解得一待驗證值 M1；

檢查 M1 與文件 M 是否相等，若相等則 SIG2 才是正確的簽章，否則不是正確簽章。

六、申請專利範圍

7.一種識別卡安全控管方法，其包括下列步驟：

伺服端與用戶端使用者兩者對外只有一共通公開金鑰，伺服端與用戶端使用者各有其私密金鑰和與其私密金鑰相對應之公開金鑰，上述共通公開金鑰係由伺服端公開金鑰與使用者公開金鑰而得，而欲簽出之文件須先經使用者之私密金鑰簽過後，再由伺服端之私密金鑰簽過才可送出，當要驗證所簽出文件之簽章時則須使用上述共通公開金鑰對所簽出之文件解密後加以比對即可。

8.一種識別卡安全控管方法，其使用一生成子 g 及一大質數 P，用戶端使用者之私密金鑰 us，與其相對應之公開金鑰為 $up=g^{us} \bmod P$，以及伺服端私密金鑰 ss，其相對之公開金鑰為 $sp=g^{ss} \bmod P$，和兩者對外之共通公開金鑰為 $Y=(up\times sp) \bmod P$，此安全控管方法當用戶端之使用者欲簽出文件(M)時，用戶端與伺服端需進行簽章過程及驗證過程；

其中之簽章過程時包括如下步驟：

[a]用戶端與伺服端分別產生隨機變數 k1 及 k2；

[b]用戶端計算 $r1=g^{k1} \bmod P$，同時伺服端也計算 $r2=g^{k2} \bmod P$，之後用戶端與伺服端互相交換 r1 及 r2；

[c]用戶端與伺服端均計算 $R=(r1\times r2) \bmod P$；

[d]用戶端先驗證 sp^M 與 $(r2^R\times g^{ss}) \bmod P$ 是否相等，若兩者相等則用戶端計算 $S1=(us\times M-k1\times R) \bmod (P-1)$；以及

[e]伺服端驗證 up^M 與 $(r1^R\times g^{us}) \bmod P$ 是否相等，若兩者相等則伺服端計算 $S2=(ss\times M-k2\times R) \bmod (P-1)$，若不

六、申請專利範圍

相等則結束簽章程式重頭進行；否則

SIG=(R, S=(S1+S2) mod P-1)即作為對文件M之簽章；

而其中之驗證過程包括如下步驟：

以共通公開金鑰Y驗證Y^M mod P是否與$R^R \times G^S$ mod P相等，若相則表示SIG為文件M之正確簽章，否則不是正確的簽章。

9.一種識別卡安全控管方法，使用一金鑰交換系統、一公開值(M)，藉以回復金鑰，其包括如下步驟：

[a]用戶端與伺服端先執行一相互認證之程序，認證完成後伺服端可得一加密金鑰(SK)及一儲存裝置上之私密資料(DK)，並由自己所選之密碼而獲得PWK；

[b]用戶端產生兩大質數p和q，其中p×q=N，N為一模數；

[c]用戶端與一第一金鑰回復中心(TKRC1)利用金鑰交換系統或是執行前述相互認證之程序而獲得一第一共享金鑰(SK1)，同時亦與一第二金鑰回復中心(TKRC2)進行相同之程序而獲得一第二共享金鑰(SK2)；

[d]第一與第二金鑰回復中心(TKRC1 和 TKRC2)分別產生一第一媒介數(R1)和第二媒介數(R2)，再分別利用其與用戶端間之第一和第二共享金鑰(SK1 和 SK2)，而對上述之第一與第二媒介數加密後，傳送給用戶端；

[e]用戶端接到上述第一和第二媒介數後，藉兩者以產生一公開金鑰(PK)，若無法產生公開金鑰(PK)則重覆

六、申請專利範圍

步驟[c]、[d]、[e]直到可以得出一公開金鑰為止；

[f]用戶端計算 M^{PK} mod N 而得一生成子 C，並將上述生成子 C、公開金鑰 PK、及模數 N 傳送給上述第一金鑰回復中心(TKRC1)，及第二金鑰回復中心(TKRC2)，並將上述公開金鑰 PK、模數 N 傳送至一認證中心 CA；

[g]第一金鑰回復中心(TKRC1)計算 $M1=C^{R1}$ mod N 後，並將其傳送給第二金鑰回復中心(TKRC2)，同時，第二金鑰回復中心(TKRC2)計算 $M2=C^{R2}$ mod N，並將其傳送給第一金鑰回復中心(TKRC1)；

[h]第一金鑰回復中心(TKRC1)計算 $M1^*=C^{R1}$ mod N 或 $M1^*=(C^{R1}\times C^{R2})$mod F(N)，並驗證檢查 M1*是否等於 M，同時，第二金鑰回復中心(TKRC2)計算 $M2^*=C^{R2}$ mod N 或 $M2^*=(C^{R2}\times C^{R1})$mod F(N)，並驗證檢查 M2*是否等於 M，若通過驗證，則第其中一和第二金鑰回復中心分別利用其各自之的私密金鑰對公開金鑰 PK 及模數 N 簽章後再將其傳送至上述認證中心 CA；

[i]上述認證中心收到第一和第二金鑰回復中心對公開金鑰 PK 及模數 N 之簽章後，待驗證通過後即對 PK 及 N 作一憑證證明，再回傳給用戶端之使用者；

[j]用戶端則可使用加密金鑰 SK，私密資料 DK 及 PWK 加密用戶之私密金鑰 S 及其他個人私密金鑰。

10.如申請專利範圍第 9 項所述之安全控管方法，其中之相互認證之程序包括如下步驟：

[I]用戶端將其識別碼(ID)，一第一驗證因子(N1)、

六、申請專利範圍

與此程序所要使用之會談金鑰(TK1)合併產生一用戶端第一簽體，用戶端對該用戶端第一簽體以伺服端之公開金鑰(K_{SP})進行加密，而得用戶端第一密件(C1)，並將該用戶端第一密件(C1)、用戶端識別碼(ID)、一確認請求(Auth_req)，及相關資料傳送至伺服端；

[II]伺服端接收到確認請求(Auth_req)後，以伺服端私密金鑰K_{SS}解開上述用戶端第一密件C1而獲得前述之會談金鑰(TK1)、第一驗證因子(N1)、及用戶端識別碼(ID)等相關資料，伺服端並找出使用者於註冊程序時所對應之密碼封包(OTP)、以及整數n等相關資料，若整數n小於2則用戶端之使用者須重新註冊，若整數n不小於2，則伺服端產生一小於n的整數k及m而m=n-k，再將會談金鑰TK1、整數m、第一驗證因子(N1)及相關資料合併為伺服端第一簽體(S1)，以會談金鑰(TK1)對其加密而得伺服端第一密件，並將伺服端第一密件回傳給用戶端；

[III]用戶端完成接收後，以上述之會談金鑰(TK1)解開上述伺服端第一簽章(S1)，而得上述整數m、上述第一驗證因子(N1)，用戶端檢查上述第一驗證因子(N1)是否為原先所送之值，驗證正確後用戶端將使者輸入之個人密碼(PWD)進行m次雜湊運算而得一第一封包(OTP1)，並產生一第二驗證因子(N2)；

[IV]用戶端以上述第一封包(OTP1)、上述第二驗證因子(N2)、及相關之資料合併為用戶端第二簽體，利用上述會談金鑰(TK1)對上述用戶端第二簽體進行加密而

六、申請專利範圍

得一用戶端第二密件後，將其傳送給伺服端；

[V]伺服端接收到上述用戶端第二密件後，以上述之會談金鑰(TK1)解開上述第二密件，而得上述之第一封包(OTP1)，伺服端並驗證上述第二驗證因子(N2)是否為原先所送之值，若正確無誤則伺服端對上述第一封包(OTP1)進行 k 次雜湊算，其運算結果與註冊程序中儲存於伺服端之密碼封包比對是否相同，驗證正確後即儲存整數 m 於伺服端而取代原先之整數 n，同時儲存上述第一封包(OTP1)取代原來的密碼封包，之後將上述註冊程序中產生之加密金鑰(SK)、第一封包(OTP1)、及驗證成功之訊息合併為伺服第二簽體，將其以會談金鑰加密後回傳給用戶端；

[VI]用戶端以會談金鑰(TK1)解開上述加密資料後，而分別得到加密金鑰(SK)、第一封包(OTP1)、及驗證成功之訊息，確定驗證成功後，用戶端使用上述加密金鑰(SK)與密碼金鑰(PWK)對存於存於用戶端上之密文(ECK)解密以得到上述之註冊程序中之用戶端金鑰(CK)，使用上述用戶端金鑰(CK)、密碼金鑰(PWK)和加密金鑰(SK)對存於可攜式儲存裝置中之密鑰密文(EDK)解密而得到使用者之私密資料(DK)，如此即完成認證之過程，之後用戶端之使者即可以利用其私密資料(DK)執行欲進行之動作。

11.如申請專利範圍第 9 項所述之安全控管方法，其中之公開金鑰 PK 符合下列之式子，PK×(f(R1 , R2)) = 1

六、申請專利範圍

mod F(N)，其中 F(N)=(p-1) × (q-1)或 F(N)為(p-1)、(q-1)之最小公倍數，而用戶端相對於 PK 之私密金鑰為 S = f(R1 , R2) mod F(N)。

12.如申請專利範圍第 11 項所述之控管方法，其中之 f(R1,R2)為 R1+R2 或 R1×R2。

13.一種識別卡安全控管方法，使用一金鑰交換系統，一公開值(M)，以及第一金鑰回復中心(TKRC1)及第二金鑰回復中心(TKRC2)，並具一大質數P及產生子g，藉以回復金鑰，此安全控管方法包括如下步驟：

[a]用戶端與伺服端先執行一相互認證之程序，認證完成後伺服端可得一加密金鑰(SK)及一儲存裝置上之私密資料(DK)，並由自己所選之密碼而獲得之 PWK；

[b]用戶端與第一金鑰回復中心(TKRC1)利用上述金鑰交換系統或是執行上述相互認證之程序而獲得一第一共享金鑰(SK1)，同時亦與第二金鑰回復中心(TKRC2)進行相同之程序而獲得一第二共享金鑰(SK2)；

[c]第一金鑰回復中心(TKRC1)產生一第一媒介數(R1)，利用其與用戶端間的共享金鑰 SK1 加密後傳送給用戶端，並計算 $C1=g^{R1} \bmod P$，再將 C1 送至第二金鑰回復中心(TKRC2)，同時，第二金鑰回復中心(TKRC2)產生一第二媒介數(R2)，利用其與用戶端間的共享金鑰 SK2 加密後傳送給用戶端，並計算 $C2=g^{R2} \bmod P$，再將 C2 送至第一金鑰回復中心(TKRC1)；

[d]用戶接到第一和第二金鑰回復中心所送來之上

六、申請專利範圍

述第一和第二媒介數 R1、R2 後，藉兩者以產生一公開金鑰 PK = $g^{f(R1,R2)}$ mod P，則使用者相對於公開金鑰 PK 之私密金鑰 S 為由 f(R1 , R2) mod (P-1)而得，f(R1 , R2)為上述第一和第二媒介數 R1、R2 之一特定運算值；

[e]用戶端將公開金鑰 PK 傳送給第一金鑰回復中心(TKRC1)、第二金鑰回復中心(TKRC2)，與一認證中心 CA；

[f]若第一金鑰回復中心(TKRC1)計算 M1=$PK^{inv(R1)}$ mod P 後並比較驗證 M1 是否等於 C2，同時，第二金鑰回復中心(TKRC2)計算 M2=$PK^{inv(R2)}$ mod P 後並比較驗證 M2 是否等於 C1，其中 inv(R1)表示$(R1)^{-1}$ mod P-1 之運算；

[g]若通過驗證後，第一和第二金鑰回復中心以其各自的私密金鑰對公開金鑰 PK 簽章後，再傳送至上述認證中心 CA；

[h]上述認證中心收到第一和第二金鑰回復中心對公開金鑰 PK 之簽章後，待驗證通過後即對公開金鑰 PK 作一憑證證明後，再回傳給用戶端；以及

[i]用戶端使用加密金鑰 SK，私密資料 DK 及 PWK，來加密私密金鑰 S 及用戶其它個人私密資料。

14.如申請專利範圍第 13 項所述之安全控管方法，其中之相互認證之程序包括如下步驟：

[I]用戶端將其識別碼(ID)，一第一驗證因子(N1)、與此程序所要使用之會談金鑰(TK1)合併產生一用戶端

六、申請專利範圍

第一簽體，用戶端對該用戶端第一簽體以伺服端之公開金鑰(K_{SP})進行加密，而得用戶端第一密件(C1)，並將該用戶端第一密件(C1)、用戶端識別碼(ID)、一確認請求(Auth_req)，及相關資料傳送至伺服端；

[II]伺服端接收到確認請求(Auth_req)後，以伺服端私密金鑰 K_{SS} 解開上述用戶端第一密件 C1 而獲得前述之會談金鑰(TK1)、第一驗證因子(N1)、及用戶端識別碼(ID)等相關資料，伺服端並找出使用者於註冊程序時所對應之密碼封包(OTP)、以及整數 n 等相關資料，若整數 n 小於 2 則用戶端之使用者須重新註冊，若整數 n 不小於 2，則伺服端產生一小於 n 的整數 k 及 m 而 m=n-k，再將會談金鑰 TK1、整數 m、第一驗證因子(N1)及相關資料合併為伺服端第一簽體(S1)，以會談金鑰(TK1)對其加密而得伺服端第一密件，並將伺服端第一密件回傳給用戶端；

[III]用戶端完成接收後，以上述之會談金鑰(TK1)解開上述伺服端第一簽章(S1)，而得上述整數 m、上述第一驗證因子(N1)，用戶端檢查上述第一驗證因子(N1)是否為原先所送之值，驗證正確後用戶端將使者輸入之個人密碼(PWD)進行 m 次雜湊運算而得一第一封包(OTP1)，並產生一第二驗證因子(N2)；

[IV]用戶端以上述第一封包(OTP1)、上述第二驗證因子(N2)、及相關之資料合併為用戶端第二簽體，利用上述會談金鑰(TK1)對上述用戶端第二簽體進行加密而得一用戶端第二密件後，將其傳送給伺服端；

六、申請專利範圍

[V]伺服端接收到上述用戶端第二密件後，以上述之會談金鑰(TK1)解開上述第二密件，而得上述之第一封包(OTP1)，伺服端並驗證上述第二驗證因子(N2)是否為原先所送之值，若正確無誤則伺服端對上述第一封包(OTP1)進行 k 次雜湊算，其運算結果與註冊程序中儲存於伺服端之密碼封包比對是否相同，驗證正確後即儲存整數 m 於伺服端而取代原先之整數 n，同時儲存上述第一封包(OTP1)取代原來的密碼封包，之後將上述註冊程序中產生之加密金鑰(SK)、第一封包(OTP1)、及驗證成功之訊息合併為伺服第二簽體，將其以會談金鑰加密後回傳給用戶端；

[VI]用戶端以會談金鑰(TK1)解開上述加密資料後，而分別得到加密金鑰(SK)、第一封包(OTP1)、及驗證成功之訊息，確定驗證成功後，用戶端使用上述加密金鑰(SK)與密碼金鑰(PWK)對存於存於用戶端上之密文(ECK)解密以得到上述之註冊程序中之用戶端金鑰(CK)，使用上述用戶端金鑰(CK)、密碼金鑰(PWK)和加密金鑰(SK)對存於可攜式儲存裝置中之密鑰密文(EDK)解密而得到使用者之私密資料(DK)，如此即完成認證之過程，之後用戶端之使者即可以利用其私密資料(DK)執行欲進行之動作。

15.如申請專利範圍第 13 項所述之安全控管方法，其中之 f(R1,R2)為 R1+R2 或 R1×R2。

16.一種識別卡安全控管方法，此安全控管方法包括

六、申請專利範圍

有一資料傳送及驗證程序，其係為正常情形下之資料傳送程序；以及一金鑰及密文的回復程序，其係當發文端之金鑰或明文遺失時，能利用此一程序將之回復；

其中之資料傳送及驗證程序包括如下步驟：

[a]當發文端欲傳送明文資料 M 給收文單位時，發文單位先產生一通訊基碼 SK，再以發文端之私密金鑰 KGS 對該通訊基碼 SK 進行加密而得$(SK)_{KGS}$，並以收文端之公開金鑰 PKR 對該通訊基碼 SK 進行加密而得$(SK)_{PKR}$，將上述通訊基碼 SK 與上述$(SK)_{KGS}$進行特定之運算而得一發文端密鑰，以該發文端密鑰對所欲傳送之明文資料 M 進行加密而得一密文 SM，對上述通訊基碼 SK、$(SK)_{KGS}$、$(SK)_{PKR}$及特定相關資料進行雜湊運算而得到一信託認證子 EA，以一家族金鑰 FK 對上述$(SK)_{KGS}$、$(SK)_{PKR}$、特定相關資料、以及信託認證子 EA 進行加密而得一法定存取欄位 LEAF，再將密文 SM、法定存取欄位 LEAF、以及特定相關資料傳送至收文端；

[b]收文端接收密文 SM、法定存取欄位 LEAF、以及特定相關資料後，利用家族金鑰解開 LEAF 而得到前述$(SK)_{KGS}$、$(SK)_{PKR}$、信託認證子 EA、以及特定相關資料，利用收文端私密金鑰 KGR 解開$(SK)_{PKR}$而得上述通訊基碼 SK，以通訊基碼 SK 將所接收之上述$(SK)_{KGS}$還原而可得前述發文端密鑰，再利用該發文端密鑰解開密文 SM 而得到明文資料 M；以及

[c]收文端並對所接收之通訊基碼 SK、$(SK)_{KGS}$、

六、申請專利範圍

$(SK)_{PKR}$、及特定相關資料進行雜湊運算，其運算結果用以與所接收到之信託認證子 EA 互相比對，若相等則表示驗證成功傳輸過程無誤；

而其中上述收文端金鑰 KGR，是由一第一金鑰管理單位和第二金鑰管理單位分別提供之收文端第一金鑰因子 KGR1 與收文端第二金鑰因子 KGR2，兩者經特定運算而得，而上述發文端金鑰 KGS，是由一第金鑰管理單位和第二金鑰管理單位分別提供之收文端第一金鑰因子 KGS1 與收文端第二金鑰因子 KGS2，兩者經特定運算而得；

其中之金鑰及密文的回復程序，包括如下步驟：

發文端先要求上述第一金鑰管理單位及第二金鑰管理單位取出第一金鑰因子 KGS1 與收文端第二金鑰因子 KGS2，由 KGS1 與 KGS2 即可經運算而得發文端金鑰 KGS；

利用回復之發文端金鑰 KGS，即可將 $(SK)_{KGS}$ 解開而得上述通訊基碼 SK，再利用該通訊基碼 SK 與 $(SK)_{KGS}$ 進行特定之運算而得到上述發文端密鑰，利用此一發文端密金鑰即可以將密文解開而得到明文資料。

17.如申請專利範第 16 項所述之安全控管方法，其中之發文端私密金鑰 KGS 係由 KGS1⊕KGS2 而得，而收文端私密金鑰 KGR 係由 KGR1⊕KGR2 而得，⊕表示互斥運算。

18.如申請專利範第 16 項所述之安全控管方法，其

六、申請專利範圍

中之特定相關資料可為發文端之機關代碼 IDS、收文端之機關代碼 IDR、及任意初始向量值之組合群體。

19.一種所有權驗核機制，此所有權驗核機制包括了初始階段、第一次文件傳輸及第 i 次文件傳輸；

其中之初始階段包括如下步驟：

在第一次登入時，於發文端 A 隨機選取一數字 N_0；

然後，於發文端 A 產生所有權簽署金鑰對 A_{os} 和 A_{op}，以及通訊金鑰 K_{AT}；最後

發文端 A 經由公證程序將 A_{os} 及 K_{AT} 送交所有權公正機關 TKC；

其中之第一次文件傳輸包括如下步驟：

(a)對第一份文件 M_1 產生一第一文件表頭 M_{T1}，該表頭 M_{T1} 至少包括發文端 A 之身份識別碼 ID_A、第一份文件之序號 S_1、以及分別利用發文端 A 之文件簽署密鑰 A_S 加密之相關資料，或經雜湊函數 h(·)處理過之相關資料；

(b)發文端 A 利用所有權簽署金鑰 A_{os} 對上述第一文件表頭 M_{T1} 簽章而得第一表頭簽章 $A_{os}\{M_{T1}\}$，發文端合併 ID_A、公正機關 TTP 身份識別碼 ID_{TTP}、收文端 B 身份識別碼 ID_B、文件表頭 M_{T1}、及第一表頭簽章 $A_{os}\{M_{T1}\}$ 後以通訊金鑰 K_{AT} 加密，再將其與第一份文件之表頭 M_{T1} 傳送至公正機關 TTP；

(c)公正機關 TTP 收到後，令 T_1 等於上述第一文件表頭 M_{T1}，並將 ID_A、ID_B、$A_{os}\{T_1\}$、以及 T_1 儲存；

(d)發文端 A 將 ID_A+ $A_{os}\{T_1\}$+M_1 等相關資料以公證

六、申請專利範圍

程序送交收文端 B；

(e)收文端 B 將 $A_{os}\{T_1\}$及文件序號、收發文方等文件識別資訊以 K_{BT} 加密後，以公正機關 TTP 之公開金鑰 TTP_P 加密後，送交公正機關 TTP；

(f)公正機關 TTP 以其私密金鑰 TTP_S 解開上述密文後比較步驟(e)中之 $A_{os}\{T_1\}$是否相同，並將比較結果以 K_{BT} 加密後送給 B；

(g)若步驟(f)中之較結果為相同則 B 執行步驟(h)，否則 B 要求 A 重新執行步驟(d)；以及

(h)最後，收文端 B 儲存 $A_{os}\{T_1\}$；

其中之第 i 次文件傳輸包括如下步驟：

(I)發文端 A 對第 i 份文件產生第 i 文件表頭 $M_{Ti}=ID_A+S_i+h(M_i)+(A_{op}\oplus h(T_{i-1})$，其中 S_i 為第 i 份文件之序號；

(II)發文端 A 利用所有權簽署金鑰 A_{os} 對上述第 i 文件表頭 M_{Ti} 簽章而得第一表頭簽章 $A_{os}\{M_{Ti}\}$，發文端 A 合併 ID_A、公正機關身份識別碼 ID_{TTP}、收文端身份識別碼 ID_B、文件表頭 M_{Ti}、及第 i 表頭簽章 $A_{os}\{M_{Ti}\}$後以通訊

金鑰 K_{AT} 加密，再將其與第 i 份文件之表頭 M_{Ti} 傳送至公正機關 TTP；

(III)公正機關 TTP 收到後，令 T_i 等於上述第 i 文件表頭 M_{Ti} 與第 i-1 次文件表頭 $T_{i-1}=M_{Ti-1}$ 之互斥運算值 $M_{Ti}\oplus T_{i-1}$，並將 ID_A、ID_B、$A_{os}\{M_{Ti}\}$、以及 T_i 儲存；

六、申請專利範圍

(IV)將 T1 以 Ti 取代，重覆第一次文件傳輸中之步驟(d)~(h)，如此來從事正常之文件傳送。

20.如申請專利範第 19 項所述之所有權驗核機制，其中當收文端 B 提出 M^*及 $A_{os}\{M_{Ti}\}$，欲證明 M^*為發文端 A 所送出之文件，則公正機關 TTP 可公佈 A_{op}以解出 M_{Ti}，再根據 M_{Ti}之內容確定文件是否為發文端 A 所發出，若 M^*為事後偽造之文件，則根據 T_i及 M_{Ti}之關連性，TTP 可證明 M^*非由發文端所發出，其中前後文件之關連性之判斷如下：

往前關連性為 $M_{Ti}=T_i \oplus T_{i-1}$；

往後關連性為自 M_{Ti+1} 中取出 $(A_{op} \oplus h(T_i))$欄位，$h(T_i)= (A_{op} \oplus h(T_i)) \oplus A_{op}$。

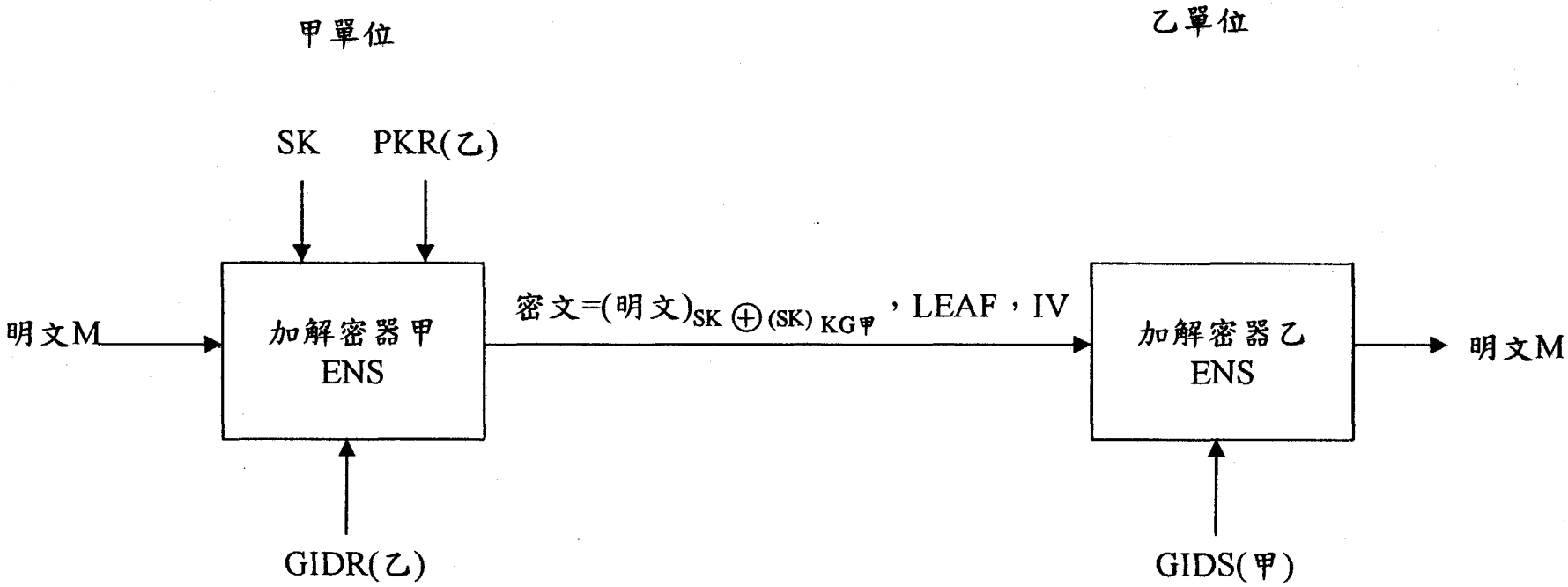
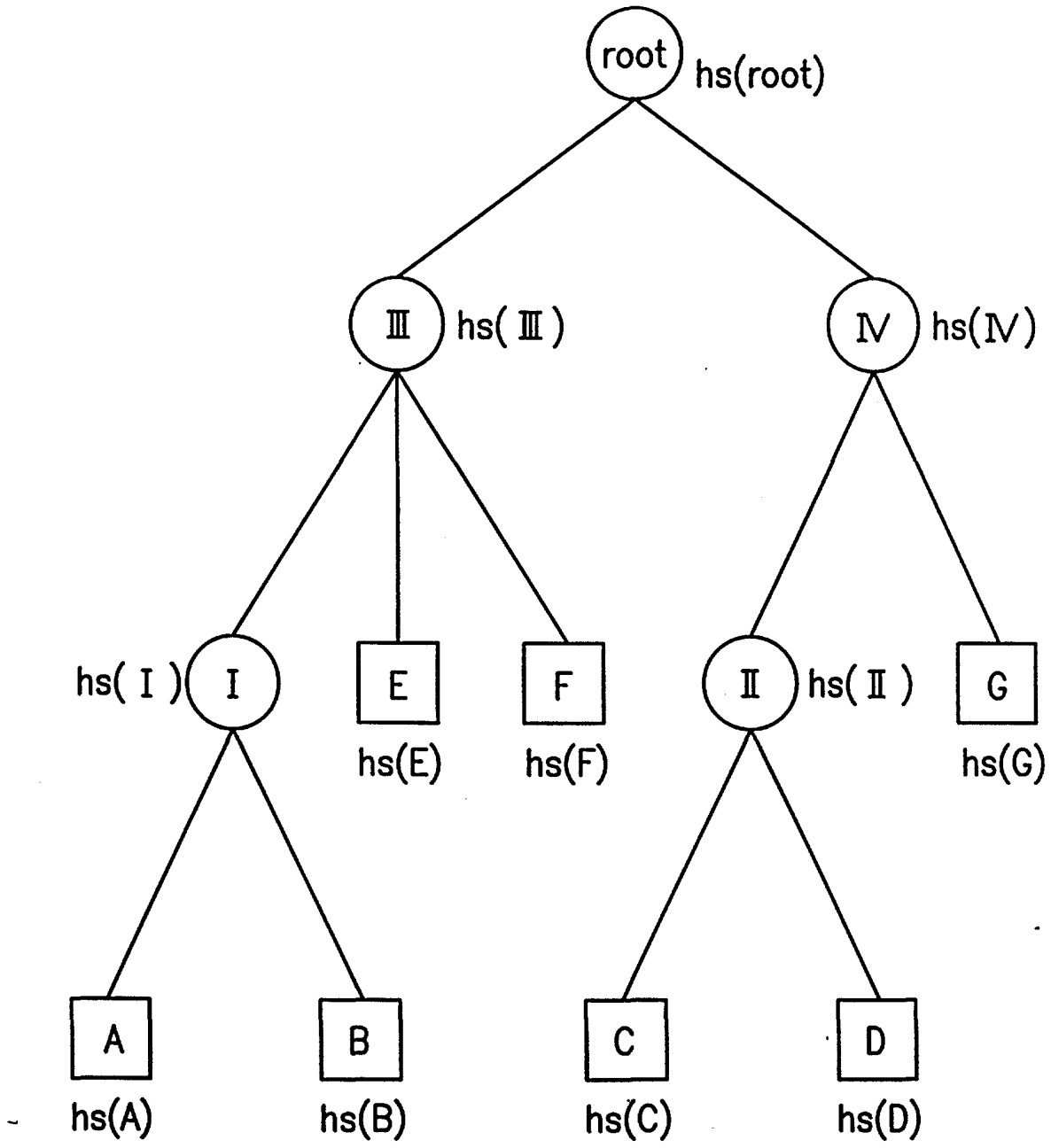
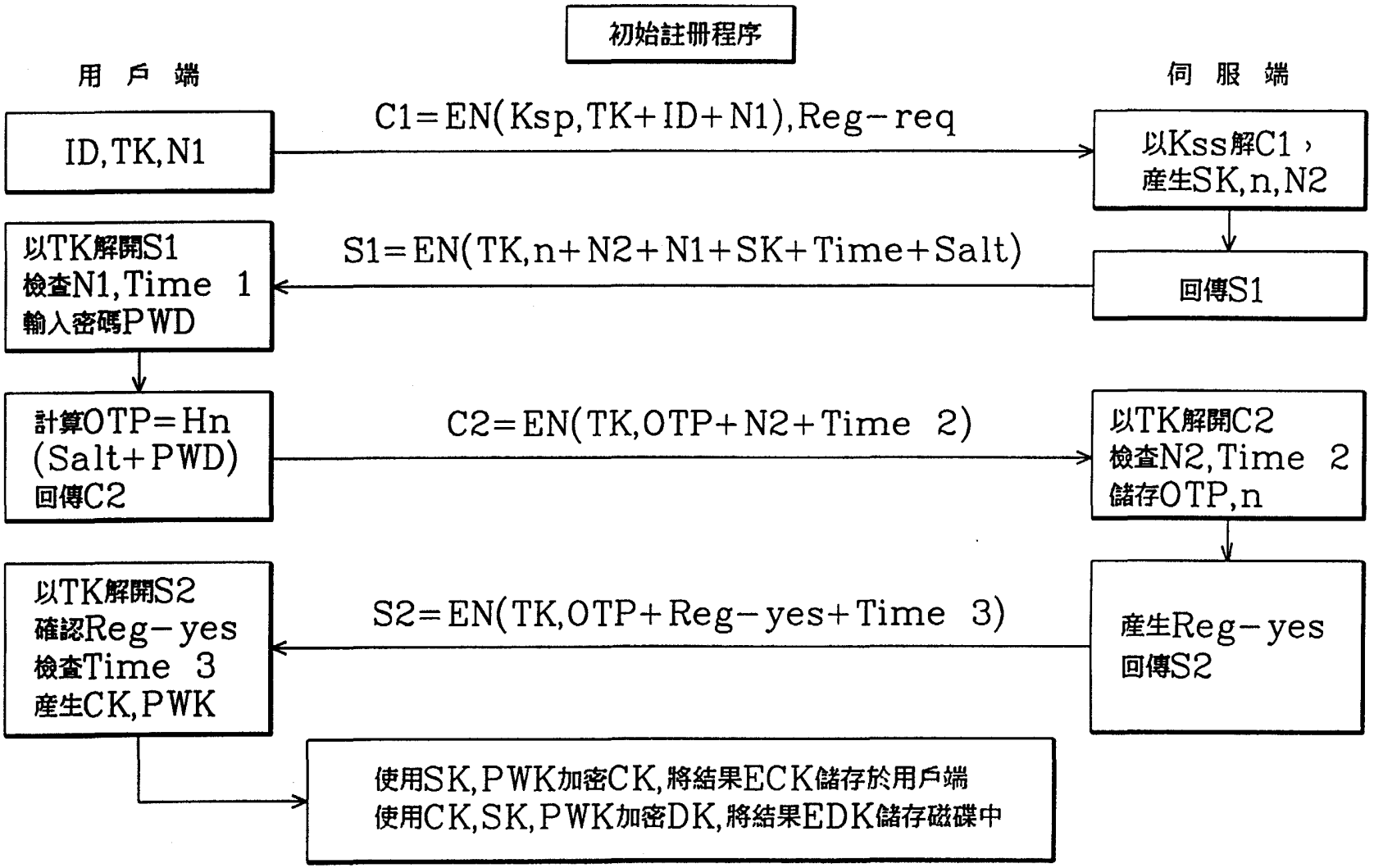


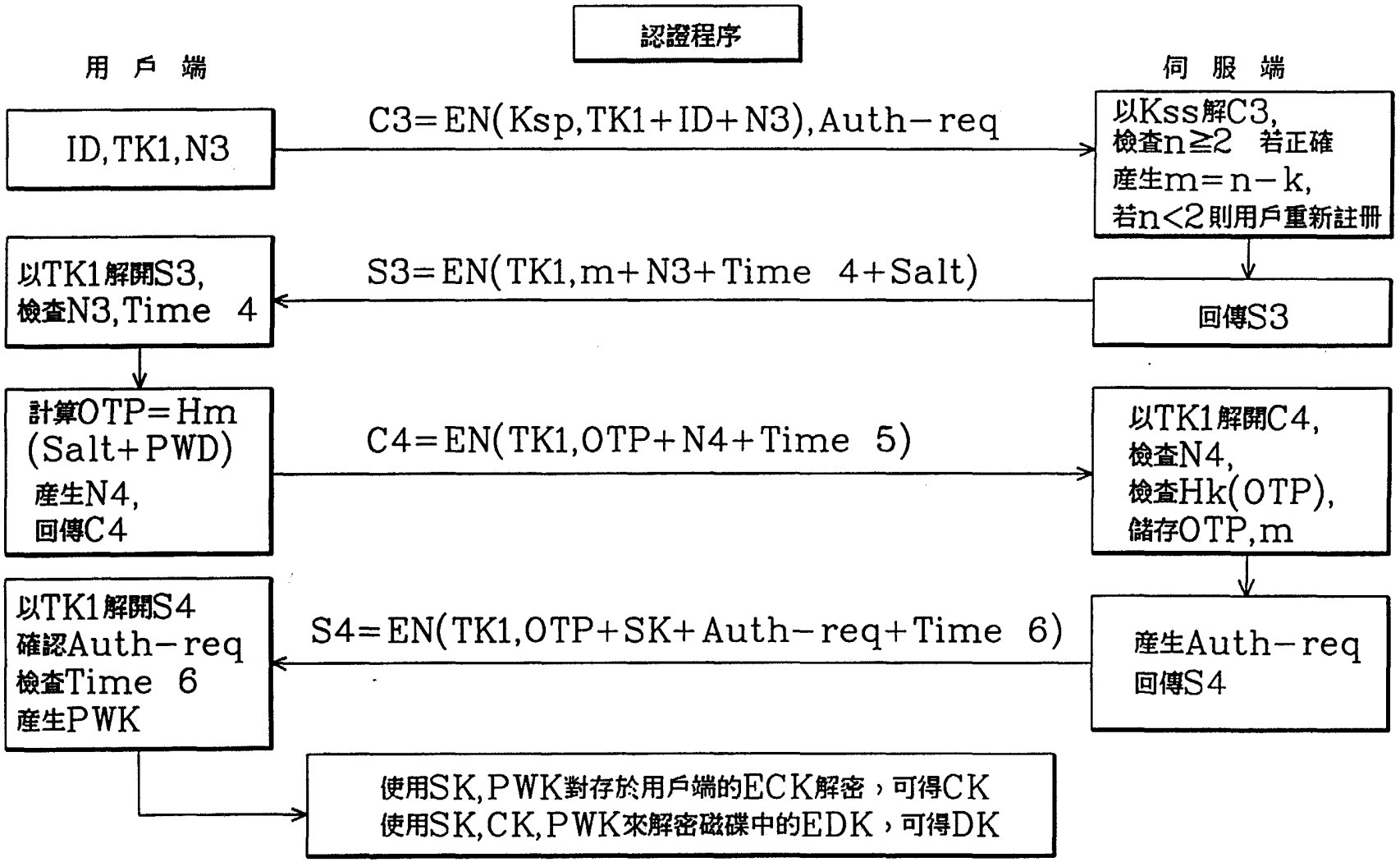
圖3A


root
hs(root)
Ⅲ
hs(Ⅲ)
Ⅳ
hs(Ⅳ)
hs(Ⅰ)
Ⅰ
E
F
Ⅱ
hs(Ⅱ)
G
hs(E)
hs(F)
hs(G)
A
B
C
D
hs(A)
hs(B)
hs(C)
hs(D)

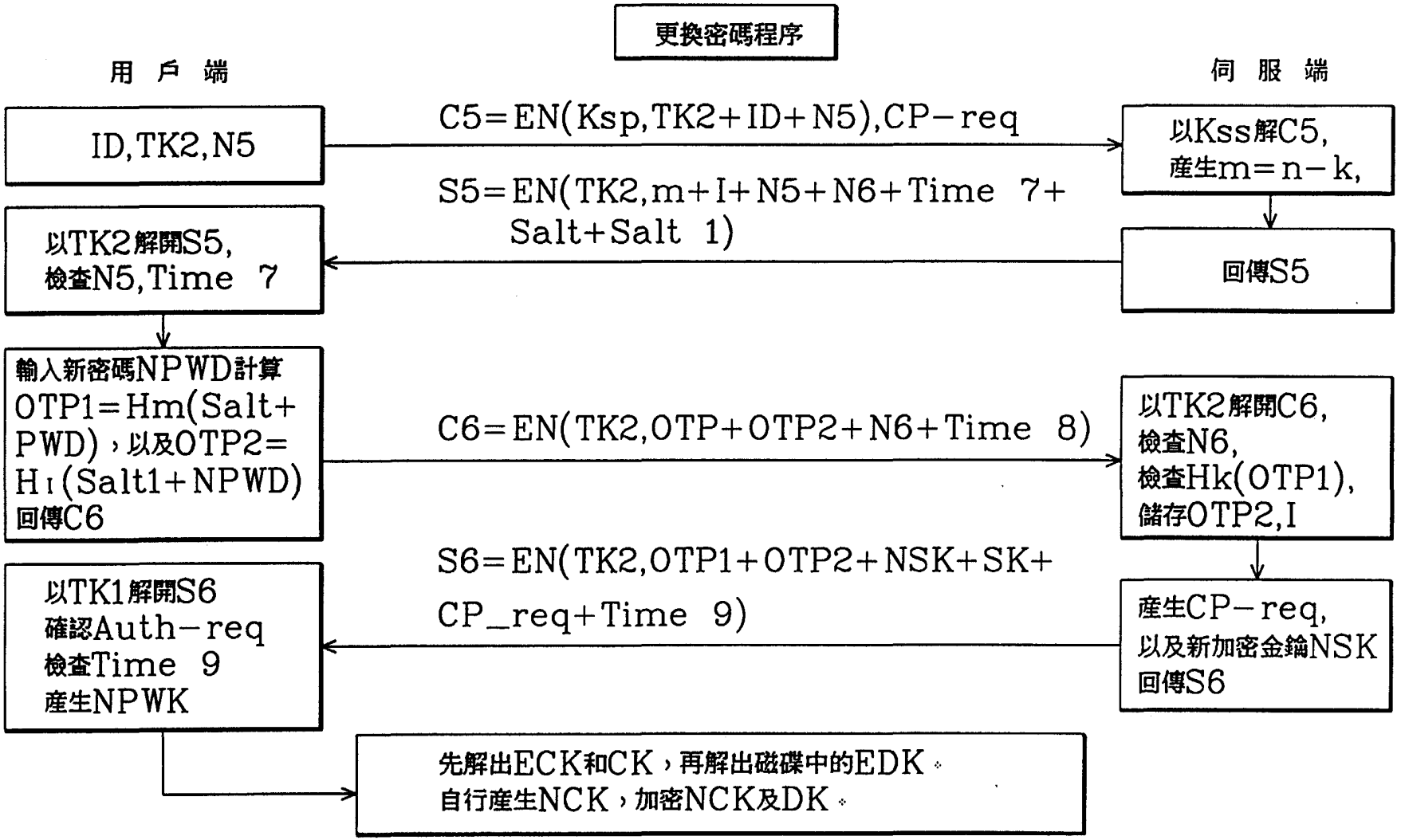
第 1 圖


初始註冊程序
用 戶 端
伺 服 端
ID,TK,N1
C1=EN(Ksp,TK+ID+N1),Reg-req
以Kss解C1，
產生SK,n,N2
以TK解開S1
檢查N1,Time 1
輸入密碼PWD
S1=EN(TK,n+N2+N1+SK+Time+Salt)
回傳S1
計算OTP=Hn
(Salt+PWD)
回傳C2
C2=EN(TK,OTP+N2+Time 2)
以TK解開C2
檢查N2,Time 2
儲存OTP,n
以TK解開S2
確認Reg-yes
檢查Time 3
產生CK,PWK
S2=EN(TK,OTP+Reg-yes+Time 3)
產生Reg-yes
回傳S2
使用SK,PWK加密CK,將結果ECK儲存於用戶端
使用CK,SK,PWK加密DK,將結果EDK儲存磁碟中

第2A圖


認證程序
用 戶 端
伺 服 端
ID,TK1,N3
C3=EN(Ksp,TK1+ID+N3),Auth-req
以Kss解C3,
檢查n≧2 若正確
產生m=n-k,
若n<2則用戶重新註冊
以TK1解開S3,
檢查N3,Time 4
S3=EN(TK1,m+N3+Time 4+Salt)
回傳S3
計算OTP=Hm
(Salt+PWD)
產生N4,
回傳C4
C4=EN(TK1,OTP+N4+Time 5)
以TK1解開C4,
檢查N4,
檢查Hk(OTP),
儲存OTP,m
以TK1解開S4
確認Auth-req
檢查Time 6
產生PWK
S4=EN(TK1,OTP+SK+Auth-req+Time 6)
產生Auth-req
回傳S4
使用SK,PWK對存於用戶端的ECK解密，可得CK
使用SK,CK,PWK來解密磁碟中的EDK，可得DK

第2B圖


更換密碼程序
用 戶 端
伺 服 端
ID,TK2,N5
C5=EN(Ksp,TK2+ID+N5),CP−req
以Kss解C5,
產生m=n−k,
S5=EN(TK2,m+I+N5+N6+Time 7+
Salt+Salt 1)
以TK2解開S5,
檢查N5,Time 7
回傳S5
輸入新密碼NPWD計算
OTP1=Hm(Salt+
PWD)，以及OTP2=
H1(Salt1+NPWD)
回傳C6
C6=EN(TK2,OTP+OTP2+N6+Time 8)
以TK2解開C6,
檢查N6,
檢查Hk(OTP1),
儲存OTP2,I
S6=EN(TK2,OTP1+OTP2+NSK+SK+
CP_req+Time 9)
以TK1解開S6
確認Auth−req
檢查Time 9
產生NPWK
產生CP−req,
以及新加密金鑰NSK
回傳S6
先解出ECK和CK，再解出磁碟中的EDK。
自行產生NCK，加密NCK及DK。

第2C圖

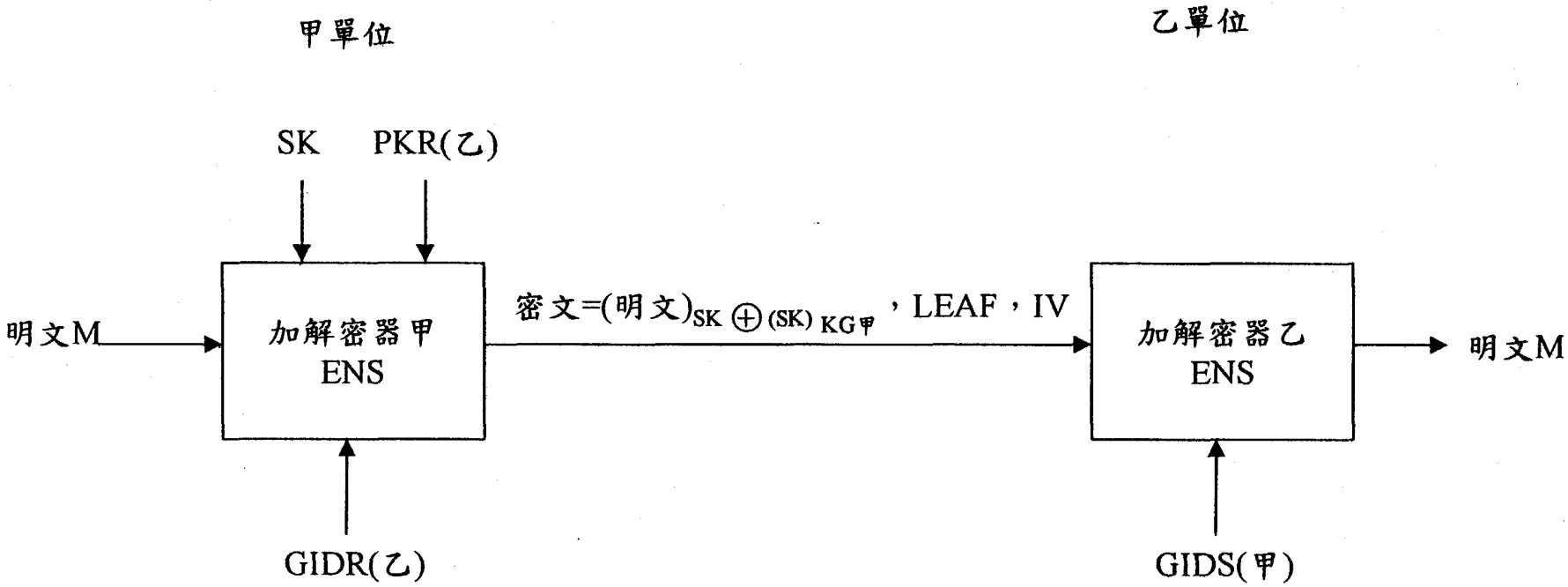


圖3A

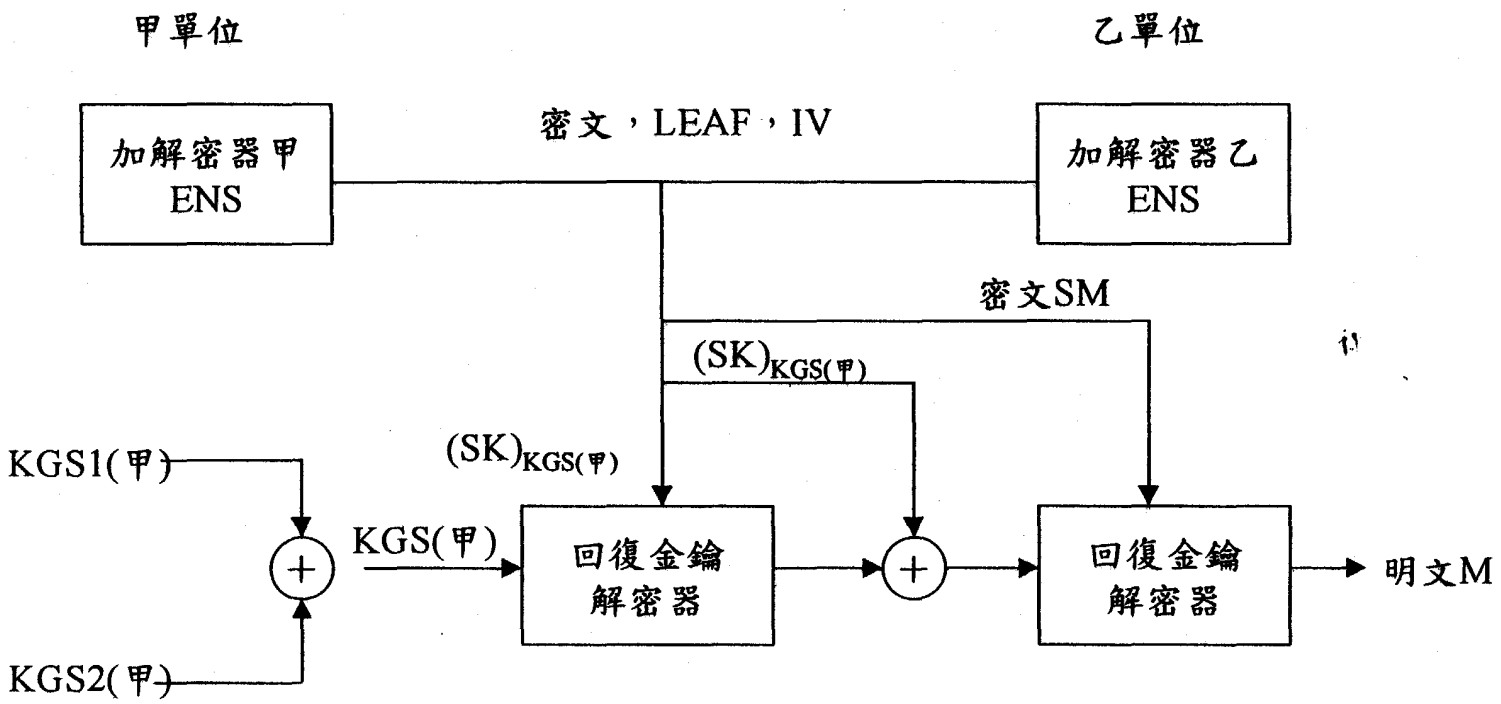

甲單位
乙單位
加解密器甲
ENS
密文，LEAF，IV
加解密器乙
ENS
密文SM
(SK)KGS(甲)
KGS1(甲)
(SK)KGS(甲)
KGS(甲)
回復金鑰
解密器
回復金鑰
解密器
明文M
KGS2(甲)

圖3B