

申請日期

類別

公告本

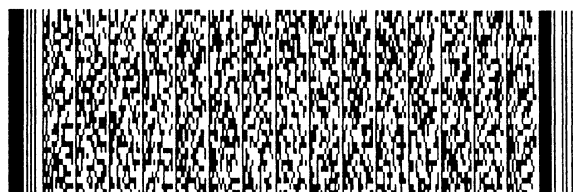
案號：89123855

(以上各欄由本局填註)

發明專利說明書

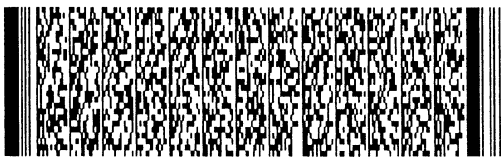
543313

一、 發明名稱	中文	鑰匙和鎖裝置
	英文	KEY AND LOCK DEVICE
二、 發明人	姓名 (中文)	1. 漢努 希佛尼恩 2. 畢裘 馬格努森 3. 因吉 里登 4. 拉福 諾伯格
	姓名 (英文)	1. HANNU SIVONEN 2. BJORN MAGNUSSON 3. INGE LIDEN 4. ROLF NORBERG
	國籍	1. 芬蘭 2. 瑞典 3. 瑞典 4. 瑞典
	住、居所	1. 芬蘭馬喬發拉市馬喬發拉路40號 2. 瑞典艾斯克土那市德裘加路18AII號 3. 瑞典艾斯克土那市福里魯路13號 4. 瑞典塔比市伊勒路29A號
三、 申請人	姓名 (名稱) (中文)	1. 瑞典商ASSA亞伯洛伊公司
	姓名 (名稱) (英文)	1. ASSA ABLOY AB
	國籍	1. 瑞典
	住、居所 (事務所)	1. 瑞典史塔克荷姆市70340郵政
	代表人 姓名 (中文)	1. 卡爾-漢瑞克 思凡伯格
	代表人 姓名 (英文)	1. CARL-HENRIC SVANBERG



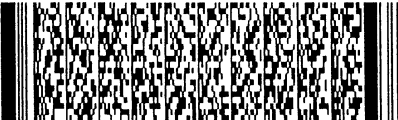
申請日期：	案號：
類別：	

(以上各欄由本局填註)

發明專利說明書		
一、 發明名稱	中 文	
	英 文	
二、 發明人	姓 名 (中文)	5. 古德倫 伯里奈克 6. 克里斯多夫 查奈 7. 喬根 克魯 8. 亞努 里福
	姓 名 (英文)	5. GUDRUN BRENNECKE 6. CHRISTOPHE CHANEL 7. JURGEN KRUHN 8. ARNAUD LEFEBVRE
	國 籍	5. 德國 6. 法國 7. 德國 8. 法國
	住、居所	5. 德國柏林市哈林格街1號 6. 德國柏林市威莫斯多夫街125號 7. 德國柏林市貝斯勒街162A號 8. 法國卓易斯市帕斯特道92號
三、 申請人	姓 名 (名稱) (中文)	
	姓 名 (名稱) (英文)	
	國 籍	
	住、居所 (事務所)	
	代表人 姓 名 (中文)	
	代表人 姓 名 (英文)	
		

申請日期：	案號：
類別：	

(以上各欄由本局填註)

發明專利說明書		
一、 發明名稱	中 文	
	英 文	
二、 發明人	姓 名 (中文)	9. 伯恩 凱克布希
	姓 名 (英文)	9. BERND KIKEBUSCH
	國 籍	9. 德國
	住、居所	9. 德國柏林市云斯坦那路53A號
三、 申請人	姓 名 (名稱) (中文)	
	姓 名 (名稱) (英文)	
	國 籍	
	住、居所 (事務所)	
	代表人 姓 名 (中文)	
	代表人 姓 名 (英文)	
		

本案已向

國(地區)申請專利

瑞典 SE

申請日期

2000/03/10 0000795-5

案號

主張優先權

無

有關微生物已寄存於

寄存日期

寄存號碼

無



五、發明說明 (1)

發明領域

本發明一般與鑰匙和鎖裝置相關，且更特定地與一種適合用於鎖系統的電子機械鎖裝置相關，其中可變的電子編碼鍵用於增加安全性。本發明也與一種使用可變的編碼鍵的一種方法和系統相關。

發明背景

先前已知的電子機械鎖系統，其中鑰匙以傳統方式相似於鑰匙在機械鎖系統散佈的方式，指派給不同的使用者。然而，這樣的散佈難以達成且散佈新鑰匙也是麻煩的程序。並且，總是存在未經授權的人士取得系統鑰匙的危險，導致安全性的風險等等。

另一個問題是電子密碼可以被複製，例如，藉由讀取機"錄製"密碼，其中拷貝可以存在鑰匙系統而不需系統擁有者的知識。

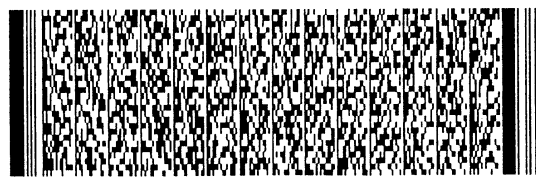
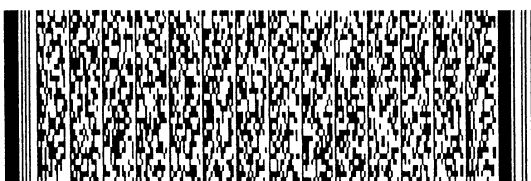
之前技藝的另一個問題是鑰匙空白可以被任何人使用，產生安全性風險。

發明目的

本發明的目的之一是提供一種先前提到的電子機械鑰匙和鎖裝置且使用在系統，其中鑰匙和鎖裝置在製造商，通路商，和消費者之間的散佈和授權具有高安全性。

本發明的另一目的是提供電子機械裝置，其中鑰匙的散佈和授權是方便的。

本發明的另一目的是提供鑰匙裝置，其如果沒有系統擁有者的知識是很難複製的。



五、發明說明 (2)

另一目的是提供鑰匙空白，其視使用而限制於限制數目的通路商。

另一目的是提供於容易和安全的加入鑰匙和鎖到鎖系統。

另一目的是提供一種用以安全方式儲存和顯示有關主鑰匙資訊的方法和系統。

另一目的是提供用以在鑰匙和鎖裝置的製造商，通路商，和終端使用者之間交換訊息之方法和系統。

發明摘要

本發明以下面的了解為基礎：之前提及先前技藝的問題可以藉由提供和改變鑰匙和鎖裡的電子密碼而解決，其中該密碼係用於在鑰匙和鎖之間，和牽涉鎖系統之建造和維護的不同團體之間編碼過的通訊。

根據本發明提供了一種如申請專利範圍第1項之方法。

根據本發明也提供如申請專利範圍第8項之鑰匙和鎖裝置，和如申請專利範圍第11項之鑰匙和鎖系統。

進一步的較偏好具體實施例定義在相關的申請專利範圍裡。

有了此方法，與本發明相符的鑰匙和鎖裝置和系統，至少一些上面討論的先前技藝問題獲得解決。

圖式簡述

現在描述本發明，藉由舉例，和參考隨附的圖式，其中：

圖1是與本發明相符具有鎖和鑰匙的階層鎖系統之全部



五、發明說明 (4)

體和軟體工具之散佈，那就是，消費者100，通路商200和製造商300。

使用者鑰匙

在消費者系統100，有許多使用者鑰匙101適合與一些鎖20使用。使用者鑰匙和鎖一起構成了主鑰匙系統(master key system(MKS))。每個鑰匙都有唯一個別的電子密碼控制它的功能。電子密碼分成不同區段給製造商，通路商和消費者使用。公共區段提供給公開資訊，而私密區段提供給私密資訊。區段進一步分成不同電子密碼元件或是項目。電子鑰匙密碼進一步一起與保護模式之描述在底下討論。

程式化和授權鑰匙

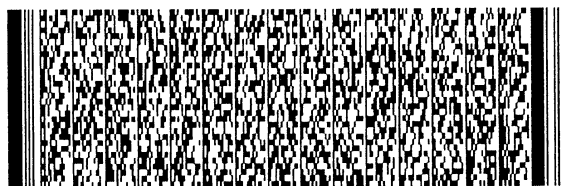
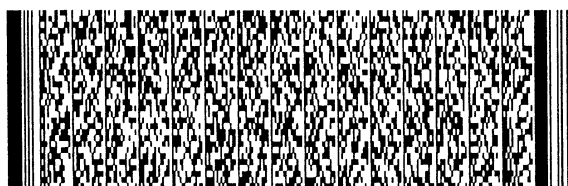
對於消費者系統100至少有一個消費者程式化和授權碼鑰匙(C-鑰匙)102。C-鑰匙，一起和D-鑰匙和M-鑰匙參閱下面，在本文件中也將稱為系統鑰匙(SYS-keys)。

消費者程式化方塊(programming box)

在消費者端，有適合用於經由如序列介面連接到電腦(個人電腦)104的程式化方塊。此程式化方塊包含靜態讀取機107且它是用於在消費者系統中程式化。靜態讀取機是鑰匙讀取機而沒有阻礙的機制，因此包含電子電路等等，用以讀取和程式化鑰匙。

雖然消費者程式化方塊顯示在圖中，但是此方塊在非常小的鎖系統中可以省略。

消費者軟體



五、發明說明 (5)

消費者具有存取個人電腦104的權利，只以開放系統資訊執行消費者管理軟體(C-軟體)。因此，C-軟體把哪個鑰匙授權給在討論的主鑰匙系統中的哪個鎖，紀錄在稱為鎖圖表裡。然而，所有鑰匙的秘密識別(參照下面)以編碼的形式儲存，其只能藉由系統鑰匙讀取。

於通路商的授權鑰匙

通路商授權鑰匙(D-鑰匙)202是給鎖系統的通路商，其可以是，例如，鎖匠。

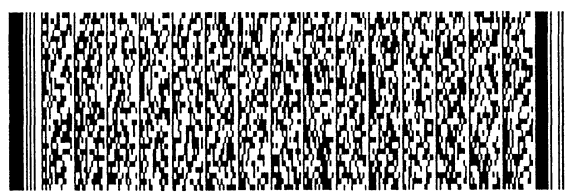
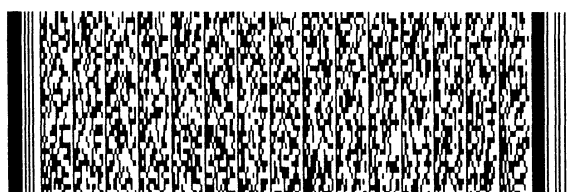
通路商程式化方塊

在通路商端，也有一程式化方塊206適合用於經由例如序列介面連接到電腦(個人電腦)204。此程式化方塊係與消費者系統100裡相關描述的程式化方塊是相同的或是相似的。

通路商軟體

通路商具有特殊電腦軟體(D-軟體)給個人電腦204。D-軟體包括開放部分用以開放系統資訊之顯示和用以改變的設計等等。它也包括秘密部分包括在系統中使用的授權碼和秘密關鍵字。D-軟體也支援經由，例如，數據機連線208到製造商鎖系統304的編碼通訊，將會進一步在下文討論。

通路商軟體用為模組，鑰匙/鎖暫存器，其描述消費者系統。以此種方式，通路商可以透明地工作就猶如通路商和消費者軟體是同一個系統。假若通路商要緊密地涉及服務消費者系統的話，對於通路商是必須的。



五、發明說明 (6)

於製造商的授權鑰匙

有一製造商授權鑰匙(M-鑰匙)302是給鎖系統的通路商製造商程式化方塊

在製造商端，也有相似於通路商程式化方塊206的程式化方塊306且適合於連接到電腦(個人電腦)304。

製造商軟體

製造商具有存取個人電腦304的權利，執行軟體(M-軟體)且對關於鑰匙和鎖的增加或刪除之操作有完全的權利。

資訊元件

所有的鑰匙和鎖都具有唯一的電子識別或是密碼，包括許多資訊元件控制鑰匙和鎖的功能。鑰匙或鎖的資訊元件現在會個別參照圖2a和2b加以描述。

電子密碼分成不同的區段給製造商，通路商，和消費者使用。一些公用元件對於主鑰匙系統的裝置是常見的，然而秘密區段提供給秘密資訊且總是群組中的個人。

每個電子鑰匙密碼包括下列部分：

- 公用鑰匙識別(PKID)包括
 - 製造商識別(M)
 - 主鑰匙系統識別。(MKS)
 - 功能識別(F)
 - 群組識別(GR)
 - 唯一識別(UID)
- 編碼鍵(K_{DES})



五、發明說明 (7)

- 秘密鑰匙識別(SKID)包括

- 秘密群組識別(SGR)

相同地，每個電子鎖密碼包括下列部分

- 公用鎖識別(PKID)包括

- 製造商識別(M)

- 主鑰匙系統識別。(MKS)

- 功能識別(F)

- 群組識別(GR)

- 唯一識別(UID)

- 編碼鍵(K_{DES})

- 秘密鎖識別(SLID)包括

- 秘密群組識別(SGR)

基本元件現在將會更詳細地描述。

M-製造商

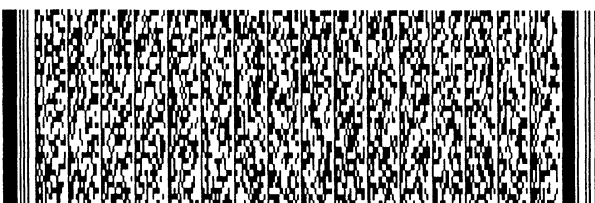
M識別主鑰匙系統的製造商。因此，使用本發明的每個製造商都指派一個唯一的M密碼識別源於製造商的鑰匙和鎖。

MKS-主鑰匙系統

MKS識別不同主鑰匙系統100。鎖將接受使用者鑰匙或是C-鑰匙只有在他們有相同的MKS密碼。

F-功能

F識別裝置的角色；它是否是鎖，使用者鑰匙，C-鑰匙，D-鑰匙，M-鑰匙等等。

GR-功能

五、發明說明 (8)

GR 是識別一群組裝置的整數。GR 在每個主鑰匙系統是唯一的且以1開始，一次加1。

UID-唯一識別

UID 識別在群組中不同的使用者。UID 在每個群組中是唯一的，且以1開始，一次加1。因此群組識別字和唯一識別的組合獨特地識別在主鑰匙系統中的裝置。

K_{DES}-編碼鍵

K_{DES} 包含隨機產生的編碼鍵。在較偏好的具體實施例中，會使用DES編碼演算法，部分是因為它的速度，且較偏好三倍DES(3DES)。DES編碼的運作有許多的模式且兩個模式是本發明較偏好的:ECB(電子密碼簿(Electronic Code Book))和CBC(密碼區塊鏈(Cipher Block Chaining))。

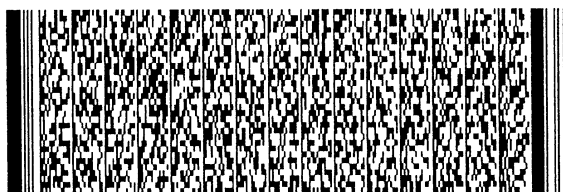
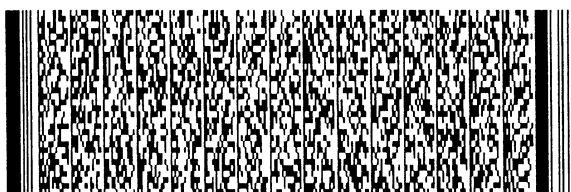
K_{DES} 在主鑰匙系統中的所有裝置是相同的。

K_{DES} 沒有辦法從外面讀取且只能在鑰匙和鎖裝置內部執行的演算法使用。這是非常重要的特點因為它減少了只藉由讀取記憶體的內容而複製鑰匙的可能性。並且，K_{DES} 只在功能模式在鑰匙中存在，請參閱下面討論的保護模式。

K_{DES} 使用在發生於不同裝置的授權過程。因此，要使鑰匙能夠操作鎖，鑰匙和鎖兩者必須有相同的K_{DES}。否則，授權過程將會失敗。

SGR-秘密群組

SGR係隨機產生的號碼且對於一個群組是相同的。上述的資訊元件和其他使用於與本發明相符的鑰匙和鎖系統中



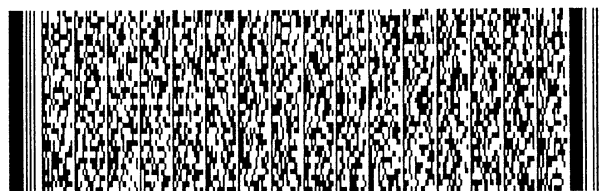
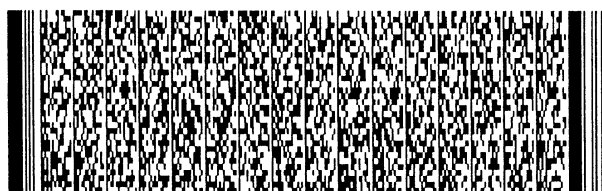
五、發明說明 (9)

的其他電子資料是對系統功能的當然重要資料。所以，為了確保資料的整合性，MAC(訊息授權碼(Message Authentication Code))用於某些資料。在鑰匙或是鎖裝置中，它用於使用 K_{DES} 的晶片中的每個授權清單。它也用於某些資料元件在裝置進入功能模式(參閱下面)之前和某些其它的資料元件。在C-，D-，或是M-軟體，訊息授權碼用於某些未編碼的資料檔案。

與本發明相符的鑰匙和鎖系統顯示非常高安全的層級。安全構造係以下列事實為基礎，系統鑰匙，換言之，C-，D-，或是M-鑰匙，可以跟許多不同的軟體一起運作。因此，要根據每個執行的授權改變授權編碼鍵並不容易。在圖1中所示的階層式系統的通常資訊流顯示於圖3。此圖為例子顯示系統和在不同層級，換言之，製造商，流通商，和消費者之間資訊交換的複雜性。

在此例子中，消費者想要加入使用者鑰匙至他的主鑰匙系統(步驟401)。因此，使用平面(planar)軟體(步驟402)，關於請求改變的資訊經由如數據機連線108-308，轉移到製造商，參閱圖1。在製造商300，使用M-軟體304(步驟403)，M-軟體資料庫304藉由M-鑰匙(步驟405)而存取(步驟404)。M-軟體資料庫之後更新且相關的資訊經由如數據機連線308-208送到D-軟體(步驟406)。

在通路商200，D-軟體資料庫204藉由D-鑰匙202(步驟408)存取(步驟407)和更新。藉由D-鑰匙202和程式化方塊206取得和程式化屬於在討論中的主鑰匙系統在保護模式



五、發明說明 (10)

之裝置。

在消費者100，C-軟體104從通路商(步驟409)，例如經由數據機連線，接收資訊。C-軟體資料庫於是被存取(步驟410)而更新且由流通商(步驟411)傳遞的新裝置經由程式化方塊106和C-鑰匙102(步驟412)程式化。當被保護的裝置進入功能模式時(步驟413)，M-軟體304被通知此事實而M-軟體資料庫就照著更新。

讀取機了解所有運作的複雜性和簡單但是安全移轉電子資訊和鑰匙或鎖裝置本身方法之需要。

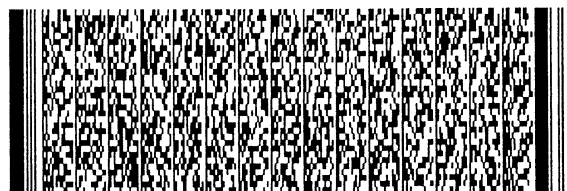
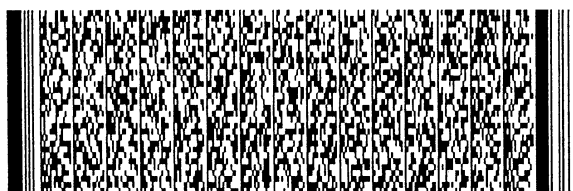
保護模式

為了對付安全傳輸裝置到消費者或是通路商的問題，例如，一個與本發明相符的鎖和鑰匙裝置的特點就稱為保護模式。此基本上表示不同階層層級的使用者，換言之，製造商，通路商，和終端使用者對屬於此系統裝置的授權具有完全控制。

此藉由使用儲存於裝置的電子鑰匙密碼中可變的編碼鍵而達成。這可變的編碼鍵之功能將會參照圖4a-e而在下文加以描述，其中儲存於裝置中的電子記憶體的電子密碼內容會顯示。

剛開始，製造商製造空白裝置，換言之，一個沒有機械或是電子編碼的裝置。因此，電子密碼記憶體是空的，參閱圖4a。

在製造商的下一步驟是加入特定於在討論中的製造商之密碼元件，參閱圖4b。此第二個元件，標示"M"，指示特



五、發明說明 (11)

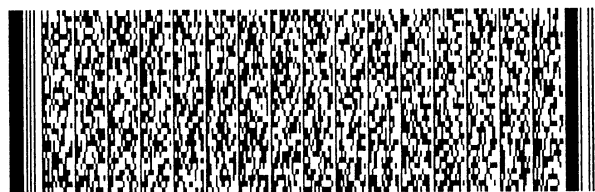
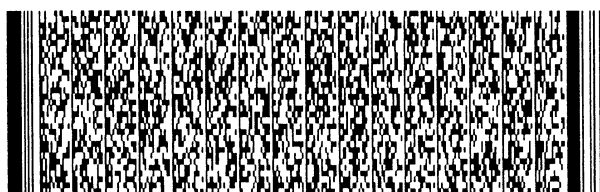
定的製造商和對於每個製造商來說都是唯一的。因此，可能藉由只讀取M元件以發現鑰匙源始於哪個製造商。

標示" K_{DES-M} "的元件係為製造商M使用為傳輸或是儲存密碼之DES編碼鍵。就如已經陳述，運作裝置所需的編碼鍵 K_{DES} 只存在功能模式下的裝置中，換言之，可操作於消費者主鑰匙系統100中的啟動鑰匙和鎖。 K_{DES-M} 鑰匙由製造商軟體(M-軟體)提供且對於除了具有M-軟體製造商之外的任何人是不可能提供鑰匙空白和於特定製造商是唯一的 K_{DES-M} 鑰匙。在那方面，鑰匙在製造商儲存期間是被保護的，因為他們對於除了正確的製造商之外的任何人是無用的。

當製造商將要傳送裝置給通路商，特定於討論中的通路商的電子密碼元件加入，參閱圖4c。此元件，標示"D"，表明特定的通路商且對每個通路商都是唯一的。其通常儲存於主鑰匙系統密碼通常使用的位置。

同時，在製造商，編碼鍵 K_{DES-M} 以 K_{DES-D} 取代，對於討論中的通路商都是唯一的編碼鍵。然而，為了能夠實現這個改變，在製造商保護鑰匙和M-鑰匙之間的授權過程必須執行。此授權過程只有當製造商保護裝置的編碼鍵和M-鑰匙，換言之， K_{DES-M} 是相同的時候才會成功。編碼鍵 K_{DES-M} 儲存於M-軟體，在成功的授權過程之後，它可以從其中擷取出來。提供 K_{DES-D} 編碼鍵，此裝置在通路商保護模式。

當消費者下了訂單，不論是給製造商或是通路商，會啟動放置鑰匙在消費者保護模式的過程，如參照圖3所描述。此過程所需的資訊之後以電子方式從製造商軟體傳送



五、發明說明 (12)

到通路商，但不是以完全文字。而是，以通路商編碼鍵所編碼而傳送。例如，在消費者保護模式下裝置的消費者編碼鍵 K_{DES-C} 以下列格式傳送：

$eK_{DES-D}(K_{DES-C})$

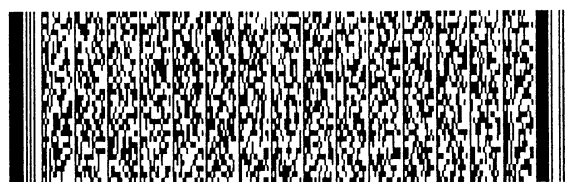
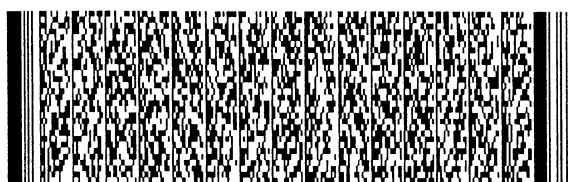
其他相關的資訊元件，如主鑰匙系統，群組，唯一識別， K_{DES} 和假如沒有使用消費者保護模式， K_{DES-C} ，是以同樣的方式編碼傳送。此資訊之後下載至通路商的保護鑰匙。

為了解碼編碼的資訊，授權的過程必須發生在通路商。此過程發生在保護裝置和D-鑰匙之間，其為 K_{DES-D} 編碼鍵所儲存的地方。密碼元件因此被解碼，藉由其顯示在圖4c的通路商保護裝置轉變成圖4d所示的消費者保護裝置。在同時，正確的功能密碼元件"F"儲存，其指示元件的功能，例如，使用者鑰匙。

然而，離開通路商的裝置尚不能用於消費者的最後主鑰匙系統，換言之，它並不是處於功能模式。藉由C-軟體和C-鑰匙，消費者接受消費者保護裝置且以 K_{DES} 取代 K_{DES-C} 編碼鍵，參閱圖4e。只有在那之後裝置可以用於主鑰匙系統。

C-鑰匙通常從製造商直接供應給消費者。詞"消費者保護模式"指下列正確的事實，被授權的消費者可以使用通路商傳遞的鑰匙，因為鎖系統鑰匙必須經由C-鑰匙由系統接受。

物理上的鑰匙，換言之，系統鑰匙用於改變另一裝置密



五、發明說明 (13)

碼的特點有許多的優點。第一，物理上的鑰匙容易處理。第二，它提供給安全系統。沒有人可以把裝置置於功能模式而不需正確的系統鑰匙(如C-鑰匙)。

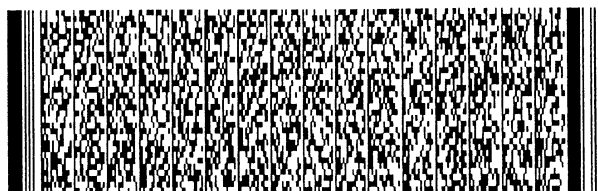
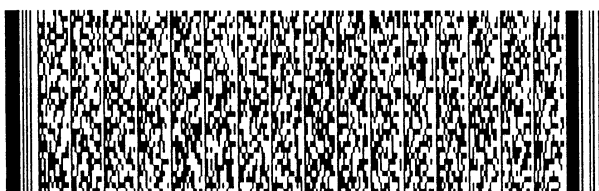
在本發明的另一具體實施例中，通路商步驟省略掉。因此，製造商負責參照圖4a-c所描述的步驟且傳遞裝置和系統鑰匙兩者給消費者。此並不影響系統的安全性只要裝置和系統鑰匙分開的傳送。

或者，假如消費者如此的請求，鑰匙可以在功能模式傳送給消費者，換言之， K_{DES} 已經儲存了。那會是較少安全性的系統但是省略一個或多個步驟的可能性顯示保護模式觀念的彈性。

如同已經陳述的，電子密碼的F資訊元件-功能元件-決定裝置的角色。此元件是"0"，換言之，在製造商或通路商儲存期間是未定義的而當鑰匙置於功能模式時，就給定預先決定的值。此值取決於鑰匙的角色；它是否是鎖或是使用者，C-，D-或是M-鑰匙。識別的正確方式對於本發明並不重要。

資料交換安全

在下面，在不同階層層級上的軟體之間的資料交換之安全性方面將會參照圖5討論。每一對製造商-通路商，製造商-消費者，和通路商-消費者有他們自己的編碼鍵，以確保足夠的安全性。然而，相同的編碼鍵會用在兩個方向，如從通路商到消費者和反之亦然，兩者。所有需要的編碼鍵儲存在討論中的軟體。編碼鍵一起與軟體傳送，但是假



五、發明說明 (14)

如編碼鍵必須更新時，新的編碼鍵以從製造商現有的通訊編碼鍵編碼而傳送。

使用者和系統鑰匙

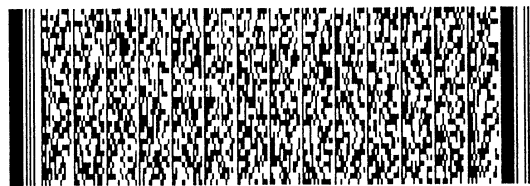
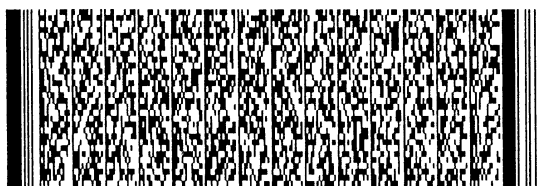
顯示於圖1系統的每個使用者必須由在使用的軟體識別。為了這個目的，每個使用者有他/她自己的唯一使用者名稱且屬於三個使用者範疇之一：超級使用者(superuser)，讀/寫，或是唯讀。不同的範疇有不同的權利和存取限制，其將會在下面簡短地討論。

超級使用者可以改變使用者的權利和系統鑰匙的擁有權。它也可以改變所有系統鑰匙和使用者的密碼(password)和PIN密碼且改變在軟體中的C-鑰匙授權。並且，他可以執行所有讀/寫使用者所允許的操作。為了得到對軟體的存取，超級使用者需要特別的系統鑰匙，一個稱為主系統鑰匙和輸入PIN密碼。每個軟體只有一個主系統鑰匙。

讀/寫使用者可以改變在主鑰匙系統的鎖圖表中的授權。他也可以解碼或是編碼轉移到系統其他軟體的檔案。為了得到對軟體的存取，讀/取使用者需要授權的系統鑰匙且輸入PIN密碼。

為了取得對軟體的存取，唯讀使用者需要屬於主鑰匙系統的鑰匙和輸入密碼。唯讀使用者只可以讀取鎖系統的組成設定，換言之，檢視鎖圖表且不能造成任何授權改變等等。

在使用者，系統鑰匙和使用的不同軟體之間也有授權協



五、發明說明 (15)

定。軟體識別編碼鍵 K_{SWIDj} 以編碼的檔案儲存在軟體中。編碼鍵 K_{SWIDj} 於每個系統鑰匙都是唯一的且整個授權過程遵循下列步驟：首先，公共識別在軟體和系統鑰匙之間交換。之後，使用者輸入使用者名稱和PIN密碼。之後軟體以相似於在下面標題"資料庫安全"使用上述唯一軟體識別編碼鍵，而確認系統鑰匙的可靠性。

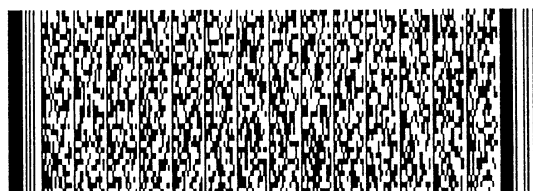
資料庫安全

在下面，資料庫安全的各方面將會參照圖6和7而討論，其顯示一起用於圖1系統的資料庫編碼。在主鑰匙系統，不同的資訊項目儲存在不同的檔案。這表示假若某編碼鍵被破解，只有部分資料庫已經被破解。不同資訊元件的例子為：

- 檔案1-鎖圖表
- 檔案2-鑰匙和鎖和他們的公共識別(PID)清單
- 檔案i

每個這些檔案都以不同編碼鍵編碼，在此例中為 K_{DB-F1} ， K_{DB-F2} ，... K_{DB-Fi} ，參閱圖6。

存取軟體的使用者將會給他/她的使用者名稱和PIN密碼(除非是唯讀使用者的情況下，其中是以輸入密碼代替)。使用者也使用系統鑰匙j而授權過程啟動。假設授權過程成功，儲存在系統鑰匙j的編碼鍵 K_{SYSj} 用於存取軟體使用在下列的解碼過程。如圖6所見， K_{SYSj} 使用在存取一組編碼過



五、發明說明 (16)

的編碼鍵 K_{DB-F1} ， K_{DB-F2} ，... K_{DB-Fi} ，等等的時候，用於資料庫檔案1，2，3等等編碼。因此，編碼鍵 K_{DB-F1} ， K_{DB-F2} ，... K_{DB-Fi} 等等他們自己本身是以編碼鍵 K_{SYSj} 編碼而儲存且經由儲存在授權的物理上的系統鑰匙的編碼鍵而解碼。

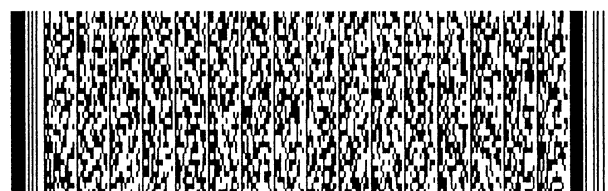
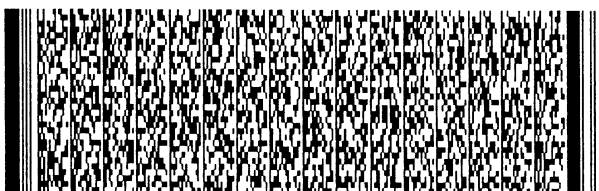
為了讀取檔案1，例如，解碼鑰匙 K_{DB-F1} 用於解碼儲存在資料庫的資訊。然而，為了進一步增加安全性，檔案的編碼鍵每次檔案存取時都會修改。此藉由在圖6和7的修改子 R_{DB-i} 而實現。實際用於解碼特別檔案的編碼鍵稱為 $K_{DB-Fi-mod} = K_{DB-Fi} \oplus R_{DB-i}$ 。每次檔案 i 儲存時，新的 R_{DB-i} 就計算，檔案 i 以新的 $K_{DB-Fi-mod}$ 編碼且新的 R_{DB-i} 清楚地儲存。

使用的編碼鍵不要於不必要長時間的儲存是重要的。所以，參閱圖6，圍在方塊A四周的資料元件只儲存在主記憶體而不在磁片上。圖6圍在標示B的方塊的資料元件和資訊儲存在磁片上。此解決方法是提供於鑰匙資料庫安全的儲存，因為編碼鍵只存在於電腦僅止於開機那段時間。因此，舉例來說，假如具有資料庫的電腦被偷了，解碼過的編碼鍵將會存在電腦系統中是沒有危險的。

識別程序

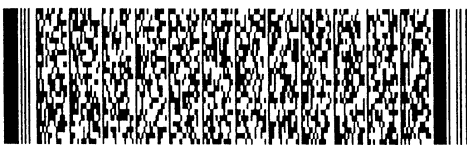
鑰匙插入鎖時，啟動識別程序。此識別程序是以編碼鍵的使用為基礎，且進一步在我們的一起等待的申請SE-9901643-8中描述，其可以參照。然而，重要的特點是為了成功地執行程序，例如授權過程，互相通訊的兩個裝置必須具有相同的編碼鍵。

本發明較偏好的具體實施例已經在上面描述。熟悉此技



五、發明說明 (17)

藝的人士了解根據本發明的鎖裝置可以變化而不需背離定義在申請專利範圍之發明範圍。因此，雖然DES編碼已經與較偏好的具體實施例一起描述，但是其它編碼的方法也是可以使用。



四、中文發明摘要 (發明之名稱：鑰匙和鎖裝置)

一種遵循下列步驟授權一鑰匙或鎖裝置的方法。首先，鑰匙或鎖備有一具有相關記憶體的電子電路。然後，第一編碼鍵(K_{DES-M} ， K_{DES-D} ， K_{DES-C} ， K_{DES})儲存在該記憶體中。藉由軟體運作，儲存在該電子記憶體的第一編碼鍵被第二編碼鍵取代。此第二編碼鍵與儲存在一第二使用者裝置的編碼鍵是相同的，因此，讓該第一和第二使用者裝置彼此互相工作。這樣提供一種散佈鑰匙或是鎖的安全方式。

英文發明摘要 (發明之名稱：KEY AND LOCK DEVICE)

A method of authorising a key or lock device follows the following steps. First, a key or lock is provided with an electronic circuitry with an associated memory. Then, a first encryption key (K_{DES-M} ， K_{DES-D} ， K_{DES-C} ， K_{DES}) is stored in the memory. By means of a software operation, the first encryption key stored in said electronic memory is replaced by a second encryption key. This second encryption key is identical to an encryption key stored in a second user device, thereby making



四、中文發明摘要 (發明之名稱：鑰匙和鎖裝置)

英文發明摘要 (發明之名稱：KEY AND LOCK DEVICE)

said first and second user devices work with each other. This provides for a secure way of distributing keys or locks.



六、申請專利範圍

1. 一種授權鑰匙或鎖裝置(20, 101)的方法, 其包括下列步驟:

- 產生第一使用者裝置(20, 101), 其包括具有適於儲存電子密碼的電子記憶體(101a)之電子電路,

- 儲存第一編碼鍵(K_{DES-M} , K_{DES-D} , K_{DES-C} , K_{DES})在該電子記憶體中(101a),

其特徵為下列步驟:

- 藉由具有該第一編碼鍵(K_{DES-M} , K_{DES-D} , K_{DES-C})的第一系統裝置(102, 202, 302)執行軟體運作, 其中儲存在該電子記憶體的軟體運作該第一編碼鍵被第二編碼鍵取代, 且

- 其中該第二編碼鍵與儲存在第二使用者裝置(20, 101)的編碼鍵相同, 因此使該第一和第二使用者裝置可互相運作。

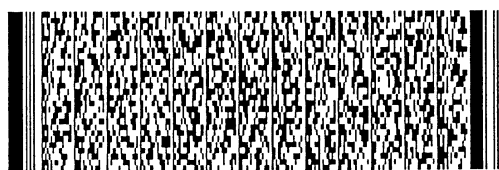
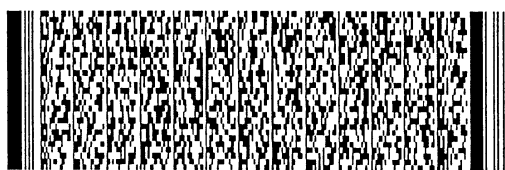
2. 如申請專利範圍第1項之方法, 其中該第一系統裝置係為主鑰匙系統的系統鑰匙。

3. 如申請專利範圍第1項之方法, 其中該第一使用者裝置係為主鑰匙系統(100)的使用者鑰匙(101)。

4. 如申請專利範圍第1項之方法, 其中第一使用者裝置係為主鑰匙系統(100)的鎖(20)。

5. 如申請專利範圍第1項之方法, 其中該電子編碼鍵(K_{DES-M} , K_{DES-D} , K_{DES-C} , K_{DES})不能從該電子電路之外讀取。

6. 如申請專利範圍第1項之方法, 其中該編碼鍵(K_{DES-M} , K_{DES-D} , K_{DES-C} , K_{DES})係為DES編碼鍵, 較佳為三倍DES編碼鍵。



六、申請專利範圍

7. 如申請專利範圍第6項之方法，其中DES編碼的運作模式是在下列運作模式之中選擇的：電子密碼本和密碼區塊鏈接。

8. 一種電子機械鑰匙和鎖裝置，包括

- 一電子電路，具有適合儲存電子密碼的電子記憶體(101a)，該電子密碼唯一地識別裝置且包括第一電子編碼鍵(K_{DES-M} ， K_{DES-D} ， K_{DES-C} ， K_{DES})，

其特徵為：

該第一編碼鍵，適合藉由由具有該第一編碼鍵(K_{DES-M} ， K_{DES-D} ， K_{DES-C})的系統裝置(102，202，302)所執行的授權之軟體操作，以第二編碼鍵取代。

9. 如申請專利範圍第8項之裝置，其中該系統裝置(102，202，302)係為一具有可程式化電子電路的鑰匙。

10. 如申請專利範圍第8項之裝置，其中該電子編碼鍵(K_{DES})不能從該電子電路之外讀取。

11. 一種鑰匙和鎖系統，包括：

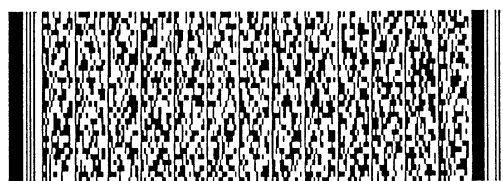
- 複數個使用者裝置(20，101)，包括：

- 複數個使用者鑰匙(101)，具有電子電路，該電路包括：適合儲存可變的電子編碼鍵的電子記憶體，以及

- 複數個鎖(20)具有電子電路，包括適合儲存可變電子編碼鍵的電子記憶體，

- 其中使用者鑰匙和鎖只在假如使用者鑰匙和鎖中儲存相同編碼鍵時候才可運作，

其特徵為：



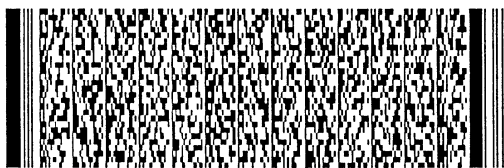
六、申請專利範圍

-至少一個系統裝置(102, 202, 302)，具有一電子電路，該電路包括適合儲存永久電子編碼鍵的電子記憶體和

-電腦程式軟體適合改變使用者裝置的可變電子編碼鍵從第一到第二編碼鍵，其為在下面之間執行的成功授權過程之結果

-具有儲存的可變電子編碼鍵的鎖或使用者鑰匙，和

-具有相同的編碼鍵如該鎖或是使用者鑰匙的系統裝置。



圖式

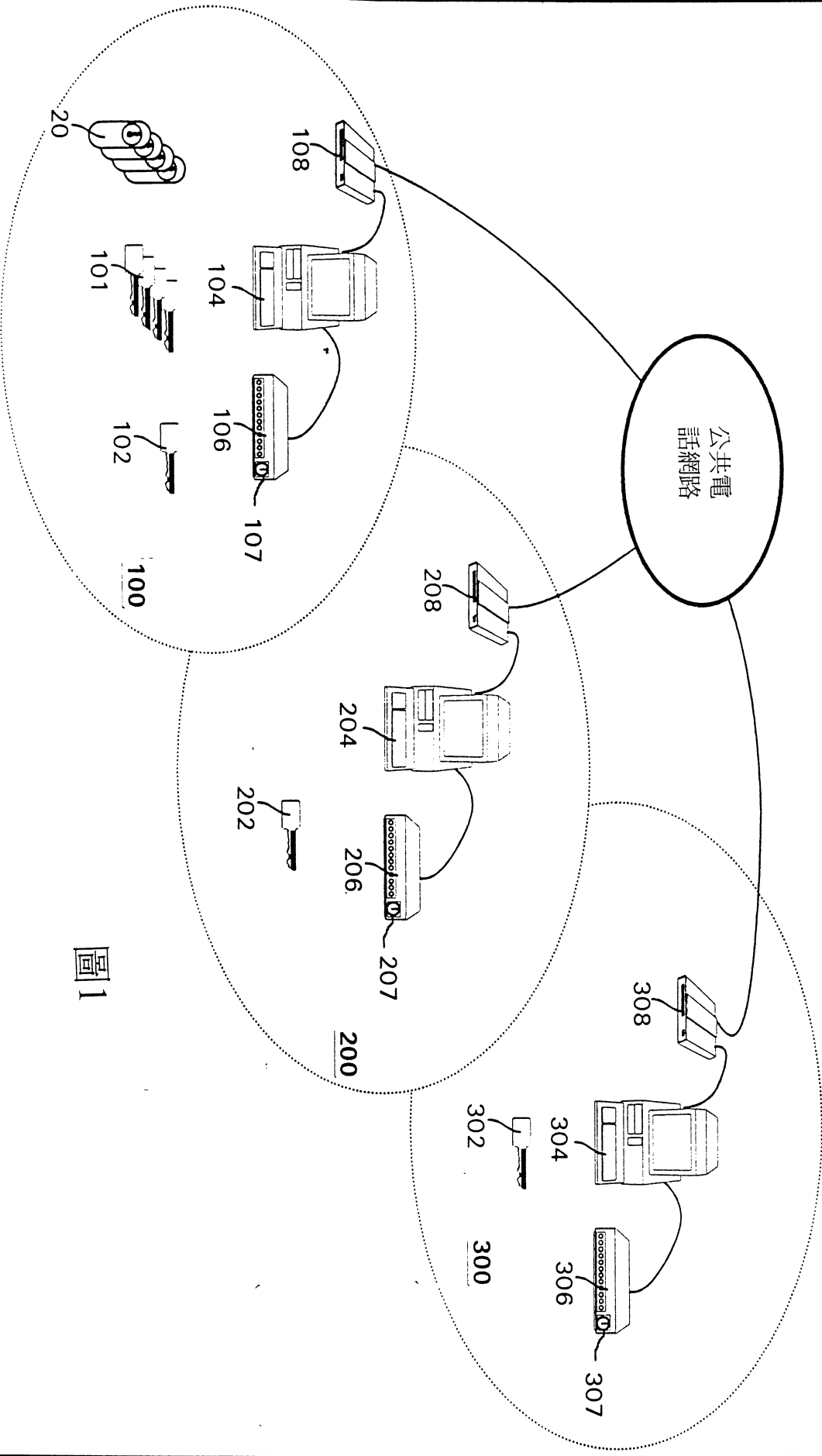


圖 1

圖式



PKID K_{DES} SKID

圖2a



PLID K_{DES} SLID

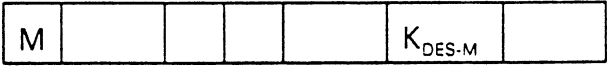
圖2b

圖4a



M-軟體

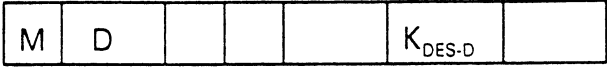
圖4b



M-軟體

M-鑰匙

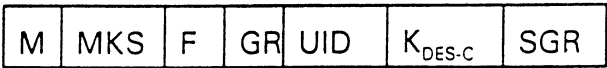
圖4c



D-軟體

D-鑰匙

圖4d



C-軟體

C-鑰匙

圖4e



圖式

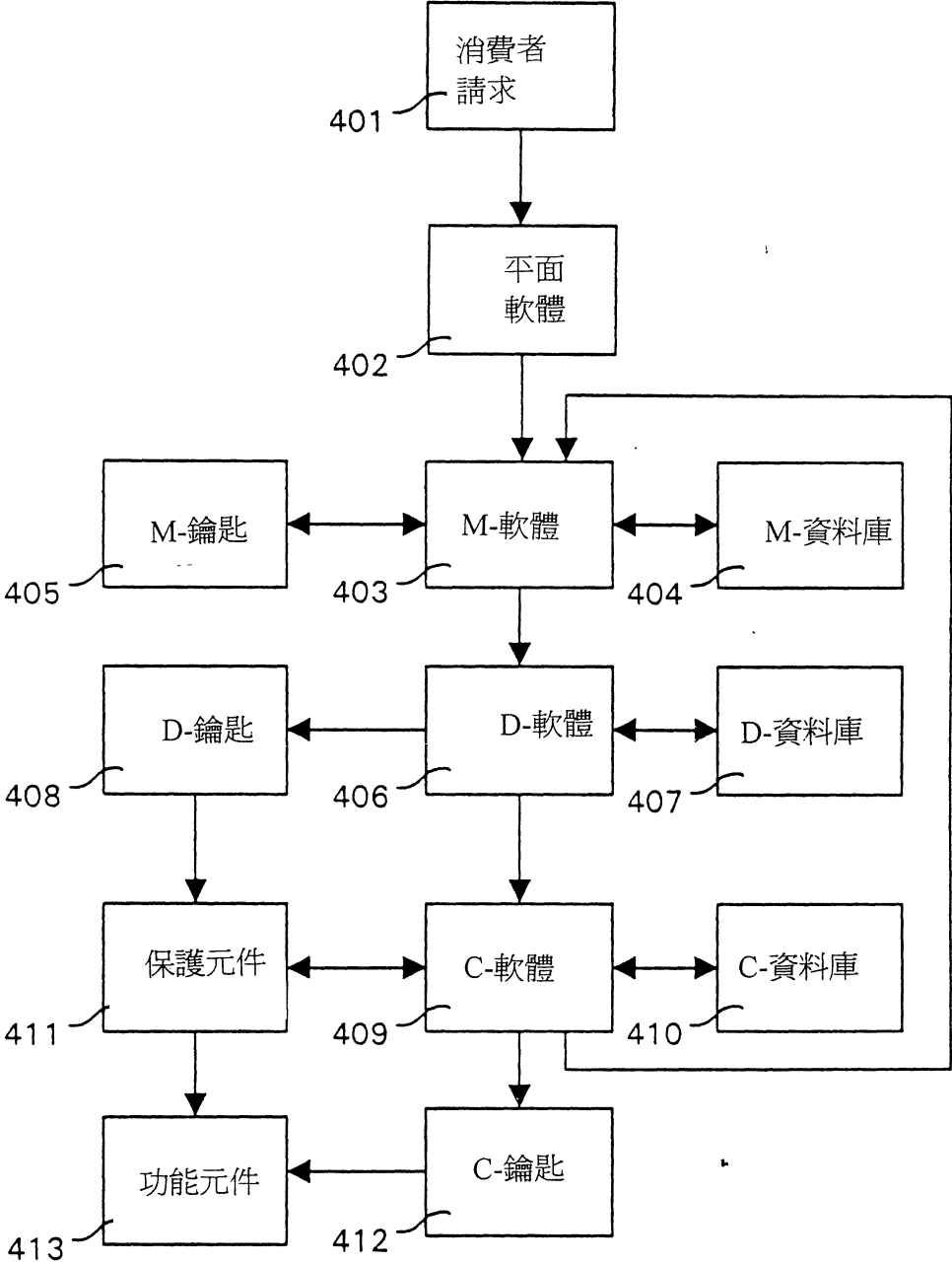


圖3

圖式

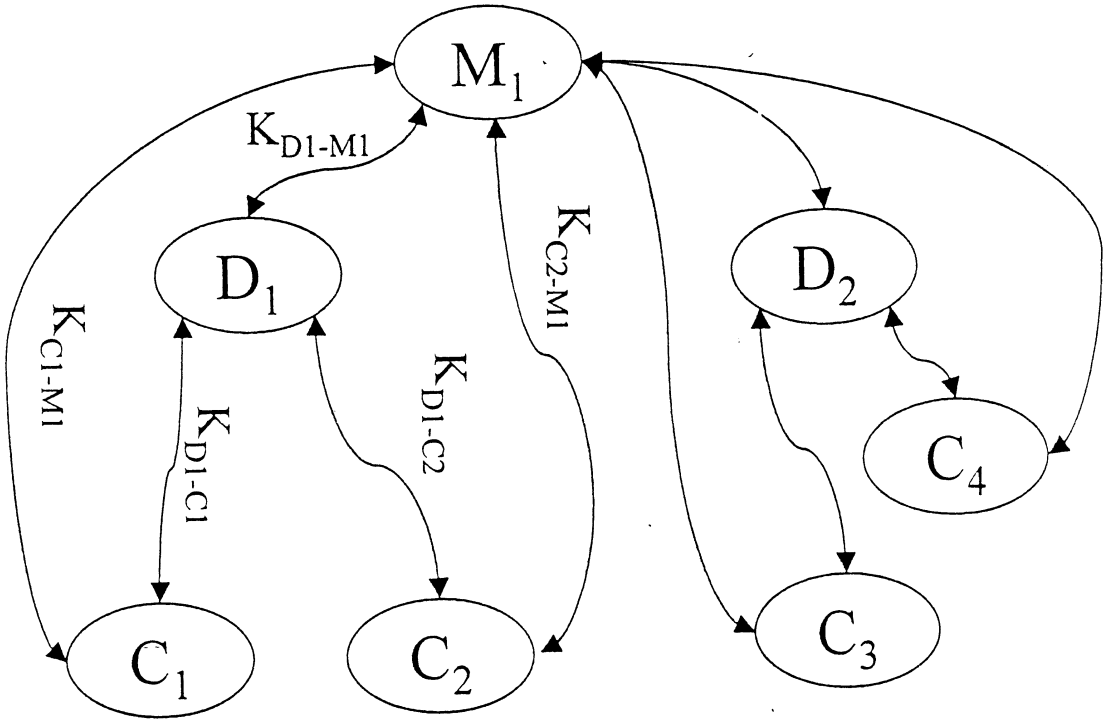
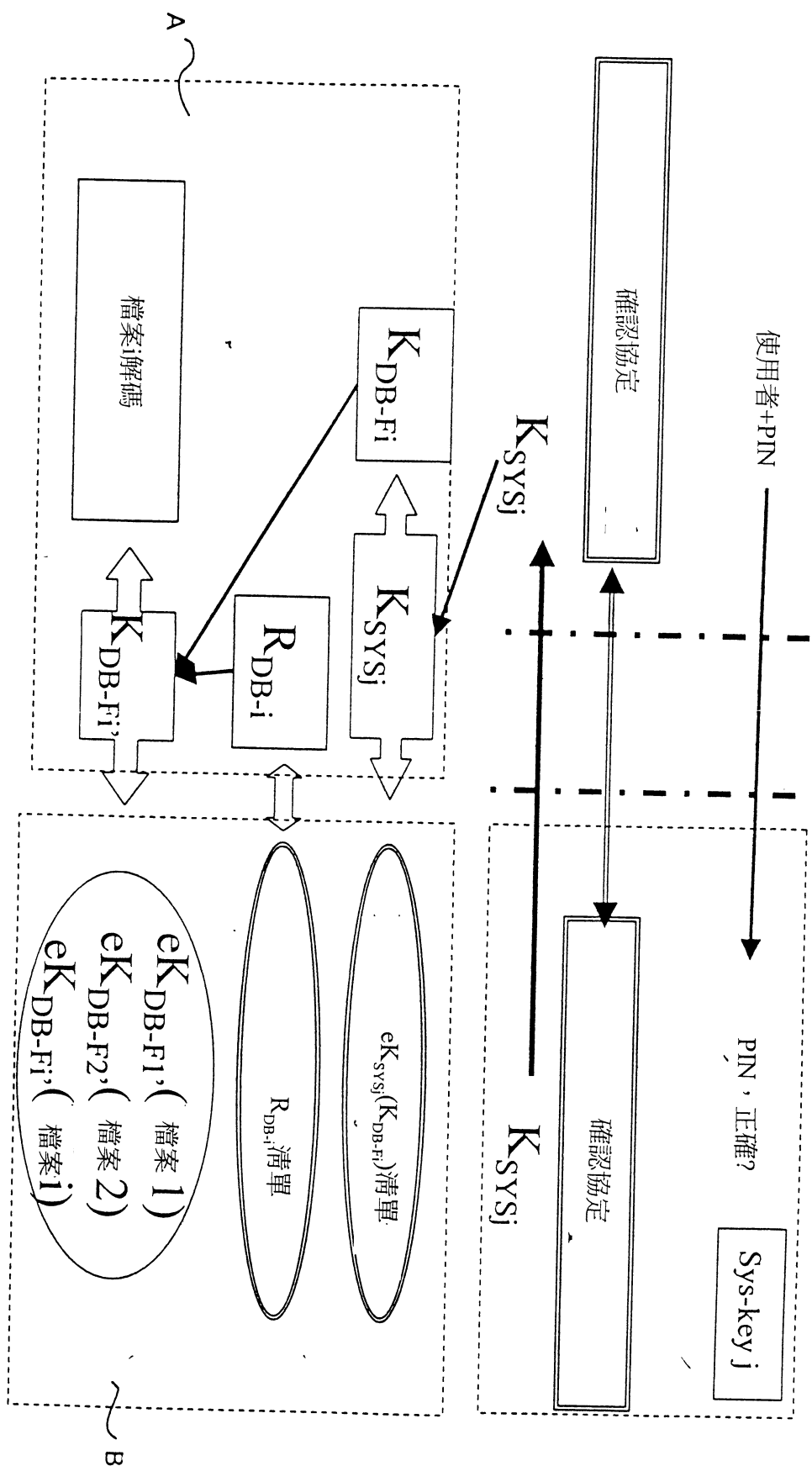


圖5



回
6

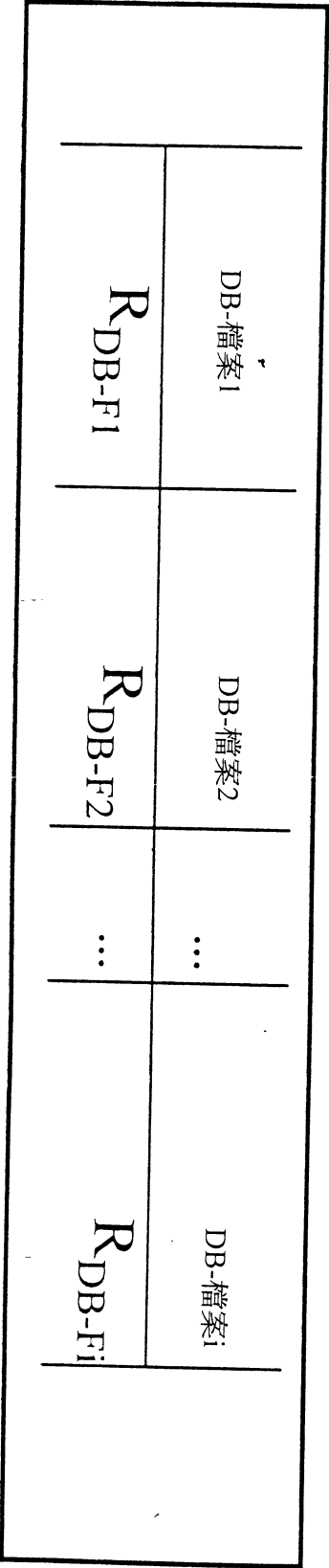
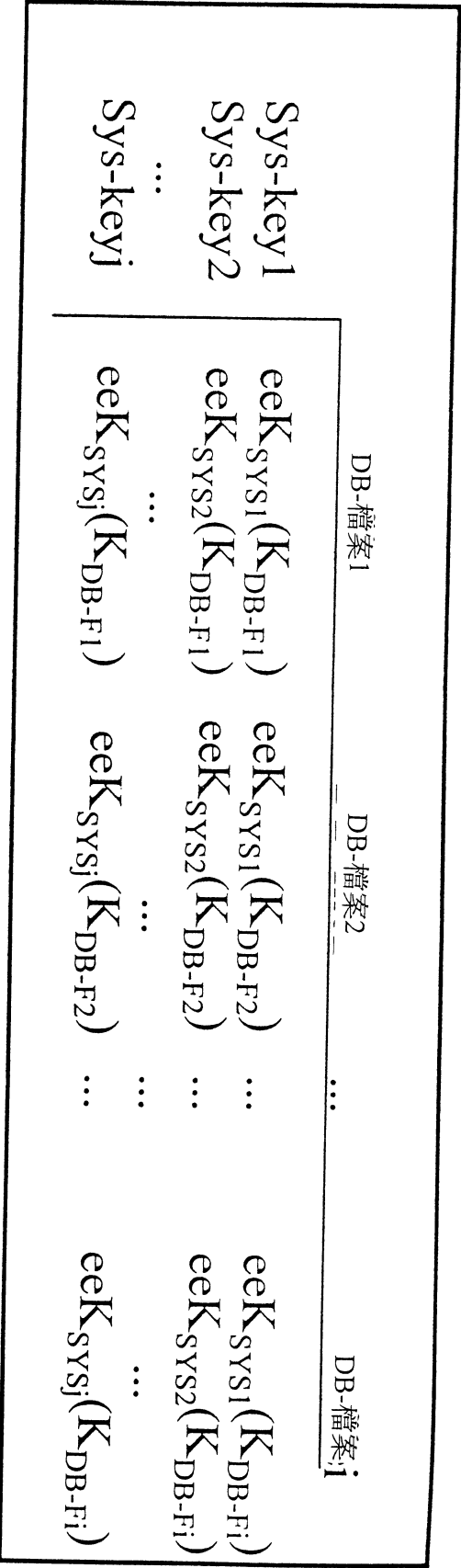


圖7

圖式

五、發明說明 (3)

檢視。

圖2a和2b分別是鑰匙和鎖裝置的資訊元件之展示，其與本發明相符。

圖3係顯示在圖1中的系統之資訊流的一個例子。

圖4a-4e係與本發明相符之鑰匙和鎖裝置中所提供電子鑰匙密碼元件之概觀。

圖5係以在製造商，通路商，和消費者之間資料交換安全性為例子的示圖。

圖6係為與本發明一起使用之資料庫編碼之概觀。

圖7顯示作為例子之資料庫檔案編碼表。

發明詳細描述

現在將描述本發明較偏好的具體實施例。為了提供清楚的描述，假設鑰匙是指物理上的鑰匙，詞"鑰匙"將會藉由加上"物理上的"而清楚明白，換言之，即適合與鎖一起使用的機械鑰匙。假如鑰匙是指電子鑰匙，會加上"電子"或是"編碼"，例如編碼鍵。

除此之外，字首"e"用於表示編碼的資訊和字首"d"表示解碼的資訊。使用的編碼鍵隨著字首之後。因此，例如eKx(檔案1)表示檔案1是以編碼鍵"Kx"所編碼。

在本描述中，有時要參考"裝置"。在本發明上下文中的裝置解譯為鑰匙或是鎖裝置。

剛開始，包含與本發明相符之鑰匙和鎖裝置的鎖系統將會參照圖1而描述，其顯示在不同階層層級之中，典型硬



圖式簡單說明

元 件 符 號 對 照 表

20	鎖	
100	消 費 者	
101 , 102	鑰 匙	
104	個 人 電 腦	
106 , 206 , 306	程 式 化 方 塊	
107 , 207 , 307	靜 態 讀 取 機	
108 , 208 , 308	數 據 機 連 線	
200	通 路 商	
202	鑰 匙	
204	個 人 電 腦	
300	製 造 商	
302	鑰 匙	
304	製 造 商 鎖 系 統	

