

# 發明專利說明書

(本說明書格式、順序及粗體字，請勿任意更動，※記號部分請勿填寫)

※申請案號：95111525

※申請日期：95.3.31

※IPC 分類：H04L 9/32 (2006.01)

## 一、發明名稱：(中文/英文)

用於鑑別與一驗證系統電氣通信之物品之身份的方法

METHODS FOR AUTHENTICATING AN IDENTITY OF AN ARTICLE  
IN ELECTRICAL COMMUNICATION WITH A VERIFIER SYSTEM

## 二、申請人：(共 1 人)

姓名或名稱：(中文/英文)

美商利盟國際股份有限公司

LEXMARK INTERNATIONAL, INC.

代表人：(中文/英文)

D 布蘭特 蘭伯特

LAMBERT, D. BRENT

住居所或營業所地址：(中文/英文)

美國肯他基州萊英頓市西新圓環路740號

740 WEST NEW CIRCLE ROAD, LEXINGTON, KY 40550, U. S. A.

國籍：(中文/英文)

美國 U.S.A.

三、發明人：(共 2 人)

姓 名：(中文/英文)

1. 克里斯多福 A 艾肯  
ADKINS, CHRISTOPHER A.
2. 提摩西 L 史壯克  
STRUNK, TIMOTHY L.

國 籍：(中文/英文)

1. 美國 U.S.A.
2. 美國 U.S.A.

#### 四、聲明事項：

☐ 主張專利法第二十二條第二項 ☐ 第一款或 ☐ 第二款規定之事實，其事實發生日期為： 年 月 日。

☒ 申請前已向下列國家（地區）申請專利：

【格式請依：受理國家（地區）、申請日、申請案號 順序註記】

☒ 有主張專利法第二十七條第一項國際優先權：

1. 美國；2005年04月01日；11/096,600

2.

☐ 無主張專利法第二十七條第一項國際優先權：

1.

2.

☐ 主張專利法第二十九條第一項國內優先權：

【格式請依：申請日、申請案號 順序註記】

☐ 主張專利法第三十條生物材料：

☐ 須寄存生物材料者：

國內生物材料 【格式請依：寄存機構、日期、號碼 順序註記】

國外生物材料 【格式請依：寄存國家、機構、日期、號碼 順序註記】

☐ 不須寄存生物材料者：

所屬技術領域中具有通常知識者易於獲得時，不須寄存。

## 五、中文發明摘要：

用於鑑別與一驗證系統電氣通信之物品之性質的方法包括，例如自該物品讀取一識別碼；自一驗證系統上產生一詢問用語；將一詢問用語寫入該物品上一第一記憶體位置；自該物品上之第二記憶體位置讀取一回應用語，其中該第二記憶體位置經組態以該第二記憶體位置與該第一記憶體位置之一組合邏輯閘輸出來做出回應；藉由使用一預定演算法加密該識別碼來產生一訊息鑑別碼；產生一比較碼，其中該比較碼係該訊息鑑別碼與該詢問用語之一組合邏輯閘輸出；及確定該比較碼是否等效於該回應用語。經組態用於該等方法之物品。

## 六、英文發明摘要：

七、指定代表圖：

(一)本案指定代表圖為：第(1A)圖。

(二)本代表圖之元件符號簡單說明：

(無元件符號說明)

八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

(無)

## 九、發明說明：

### 【發明所屬之技術領域】

本發明係關於多種用於鑑別一請求者之方法，其中藉助利用該請求者上之最小計算能力來實施該鑑別。

### 【先前技術】

對於諸多行業一愈來愈重要之領域係比對一電子系統之另一組件(驗證者)鑑別該系統之一組件(請求者)，例如該組件之身份。鑑別可用於諸多不同目的，該等目的之具體細節留給個別技術人員。於一實施例中，鑑別可用於向驗證者確認一特定請求者係既定之請求者或係驗證者期望之物品。顯而易見，在諸如此類之驗證過程中信任驗證者可能較佳。一確保該驗證者可信之通常手段係將該驗證者託管於一實體上安全之伺服器或電腦中。在鑑別之前通常不信任該請求者，此乃因其非實體上安全且因此可被複製或改變。

鑑別系統之一實例係用於智慧卡中之系統。智慧卡本身不可信任，因此對於每一商業交易，其必須係一請求者。於初始交易中其與之通信之伺服器/電腦通常位於一實體上安全之位置並因此可信任。由於該伺服器係可信任，因而其可對每一商業交易執行驗證任務。此一系統中通常用於執行鑑別之常用手段被稱作「詢問-回應協定」。在商業交易期間當一請求者需要被鑑別時，該詢問-回應協定具有三個主要步驟：

A. 該驗證者給該請求者發出一隨機詢問(發送一其中

具有一隨機數之訊息至該請求者)

B. 該請求者以針對該詢問之正確應答回應該驗證者  
(一藉由密碼術與該詢問相關之唯一數字)

C. 驗證者確認該請求者之應答正確。

若該回應正確，則該請求者被鑑別，且該商業交易可繼續。假設該密碼系統未妥協(compromise)，則該請求者須係合法以便以一正確應答做出回應。兩種確保僅合法請求者方可正確回應一隨機詢問之常用方法係對稱式及不對稱式密碼術。對稱式密碼術方法及不對稱式密碼術方法兩者皆使用在公開領域中公佈之演算法，但藉由使用僅有系統設計者知曉之密鑰保持安全。舉例而言，在對稱密碼術之情況下，驗證者及請求者兩者皆使用相同之密鑰。由此，請求者中之逆向工程設計將顯露該驗證者用來獲得對該隨機數詢問之正確應答之密鑰。兩個廣泛使用之對稱式密碼演算法係DES及IDEA。DES(資料加密標準)使用一56位元密鑰並將一64位元明文輸入塊映射成一64位元密文輸出塊。IDEA(國際資料加密演算法)使用一128位元密鑰將一64位元明文塊加密成一64位元密文塊。

另一方面，對於對稱式密碼術，請求者使用一與該驗證者用來使應答與隨機詢問相關之密鑰(私鑰)不同之密鑰(公鑰)來產生應答。與對稱式密碼術之實質區別係不對稱式演算法使用兩個不同之密鑰進行加密及相應之解密。每一參與者均擁有唯一一對密鑰(一秘密密鑰與一公鑰)。秘密密鑰與公鑰在算術上彼此相依，其中易於根據該秘密密鑰

計算出公鑰，但難以根據公鑰計算出密鑰。

然而，該兩種方法之缺陷皆係大量計算能力通常必須駐存於該等請求者中。雖然該計算能力可小於該驗證者所需，但對於一請求者(其可能係一簡單之行動裝置)而言，此仍係一需克服之重大障礙。先前技術中所論述之典型實施方案已嘗試最大程度地減小該請求者所需之計算能力。然而，對於習用對稱式與不對稱式詢問-回應協定，微處理器樣(或連續)計算能力係請求者中之根本要求，此乃因必須執行諸如乘法及調變等高級數學功能方能產生對該詢問之正確回應。該所需計算能力對大多數應用而言皆係成本過高。由此需要一種鑑別一請求者之方法，其中該請求者具有一相當低之計算能力臨限值。

### 【發明內容】

本發明係關於一種用於鑑別一具有最小計算能力之請求者之方法。本發明之例示性實施例提供請求者之安全鑑別同時明顯降低請求者之計算能力，從而允許諸多對鑑別之新應用(其中先前之鑑別過程需要明顯更大之計算能力)。於本發明之一例示性實施例中，請求者所需之唯一計算能力係組合邏輯。換言之，所需之一切係AND、OR及類似邏輯，而非當前驗證方法中通常所需之乘法運算。由此，請求者可獲益於一相當低成本之電子裝置。

本發明之一態樣係一種用於將一鑑別回應自一物品發送至一驗證系統之方法。該方法包括：將一詢問用語儲存於該物品上一第一記憶體位置中，其中該詢問用語係自該驗

證系統中接收；自該物品上一第二記憶體位置擷取一訊息鑑別碼(MAC)，其中該MAC係在該物品之製造時儲存於該第二記憶體位置中；因應自該驗證系統中接收到對該第二記憶體位置之一讀取請求，發送該詢問用語與該MAC之一組合邏輯閘輸出；擷取一儲存於該物品上之序號識別符，其中該序號識別符在該物品之製造時儲存於該物品上；及因應來自該驗證系統之對該序號識別符之一請求，將該序列識別符發送至該驗證系統。

本發明之另一態樣係一種用於鑑別與一驗證系統電氣通信之物品之性質之方法。該方法包括：自該物品讀取一識別碼；自該驗證系統產生一詢問用語；將該詢問用語寫入該物品上一第一記憶體位置；自該物品上一第二記憶體位置讀取一回應用語，其中該第二記憶體位置經組態以該第二記憶體位置與該第一記憶體位置之一組合邏輯閘輸出來做出回應；藉由使用一預定密碼術演算法加密該識別碼來產生一訊息鑑別碼(MAC)；產生一比較碼，其中該比較碼係該MAC與該詢問用語之一組合之邏輯閘輸出；及確定該比較碼是否等同於該回應用語。

本發明之例示性方法可有利地用於向一驗證系統提供請求者鑑別同時最大程度地減小請求者所需之計算能力。根據詳細闡述將顯見該等及其他優點。

### 【實施方式】

現在將詳細參考顯示於隨附圖式中之各種實施例，其中在該等圖式中，相同之編號指示類似之元件。

本發明之一實施例係一用於將一驗證回應自一請求者發送至一驗證系統之方法。該方法包括：在該物品上一第一記憶體位置中儲存一詢問用語，其中該詢問用語係接收自該驗證系統；自該物品上一第二記憶體位置擷取一訊息鑑別碼(MAC)，其中該MAC係在該物品之製造時儲存於該第二記憶體位置中；因應自該驗證系統中接收到對該第二記憶體位置之一讀取請求，發送該詢問用語及該MAC之一組合邏輯閘輸出；擷取一儲存於該物品上之序號識別符，其中該序號識別符係在製造該物品時儲存於該物品上；及因應一來自該驗證系統之對該序號識別符之請求，將該序列識別符發送至該驗證系統。

於另一例示性實施例中，該詢問用語包括一隨機產生之數字。如熟習此項技術者所瞭解，該詢問用語可包括任何數量之位元或資料。於另一例示性實施例中，該詢問用語包括50%的1及50%的0。

於再一例示性實施例中，若該詢問用語之位元長度小於該MAC之位元長度，則將重複該詢問用語直至該詢問用語等於該MAC之位元長度。以一相同方式，若該詢問用語之位元長度大於該MAC之位元長度，則可重複該MAC直至該MAC等於該詢問用語之位元長度。另一選擇係，在當前鑑別方法中僅可應用較小之位元長度。

如熟習此項技術者所瞭解，該組合邏輯閘可包括一AND閘或一OR閘。當記憶體之未程式化狀態係邏輯0時，可使用AND運算。另一選擇係，若未程式化狀態係邏輯1時，

可利用 OR 運算。

於本發明之一例示性實施例中，該方法進一步包括該請求者驗證自該驗證系統接收之詢問用語。如熟習此項技術者所瞭解，可利用任何用於熟習此項技術者習知之詢問用語之驗證技術。例示性驗證技術包括但不限於核對和及其他類似之資料技術。一例示性驗證過程係確定該詢問用語是否包括一預定數量之「1」及「0」。舉例而言，於一例示性實施例中，該詢問用語需恰好具有50%的1及50%的0才係一有效之詢問用語。

於再一例示性實施例中，一其性質欲被鑑別之物品係一噴墨印表機頭。於一替代例示性實施例中，此一物品可包括一供墨盒或儲墨盒。其他例示性物品可包括作為一系統之一部分之任何其他組件(其中期望鑑別該組件之性質(例如身份))。於一例示性實施例中，該驗證系統包括一與該列印頭或供墨盒電氣通信之印表機。於其他例示性實施例中，該驗證系統可係一與該請求者電氣通信之電腦或遠程伺服器。此一通信可包括一藉由網際網路或其他網路連接至該請求者裝置之遠程電腦伺服器。

舉例而言，該請求者可包括一噴墨列印頭或供墨盒且該驗證系統包括一遠程鑑別伺服器。為鑑別該噴墨列印頭或供墨盒之性質，該印表機連接至該遠程鑑別伺服器。於一實施例中，該連接係經由一連接至該印表機及網際網路之本地電腦。於一替代實施例中，該印表機直接連接至網路(例如網際網路)並與遠程鑑別伺服器電氣通信。

本發明之另一例示性實施例包括一噴墨列印頭。該列印頭包括數個連接至一設置於一基板上之墨排放口之墨通道。該列印頭進一步包括第一及第二記憶體位置，其中該第一及第二記憶體位置經組態以使其僅可被寫入一次。該第二記憶體位置經進一步組態以便因應對該第二記憶體位置之讀取請求來傳輸該第一記憶體位置與該第二記憶體位置之組合邏輯閘。

本發明之另一例示性實施例包括一用於鑑別一與一驗證系統電氣通信之物品之性質之方法。該方法包括：自該物品讀取一識別碼；在該驗證系統上產生一詢問用語；將該詢問用語寫入該物品上一第一記憶體位置；自該物品上一第二記憶體位置讀取一回應用語，其中該第二記憶體位置經組態以該第二記憶體位置與該第一記憶體位置之一組合邏輯閘輸出來做出回應；藉由使用一預定密碼術演算法加密該識別碼來產生一訊息鑑別碼(MAC)；產生一比較碼，其中該比較碼係該MAC與該詢問用語之一組合邏輯閘輸出；及確定該比較碼是否等同於該回應用語。

例示性密碼術演算法包括但不限於：MD5(訊息摘要鑑別5)、SHA-1(安全雜湊演算法)、CMEA、DES及IDEA。熟習此項技術者將瞭解，可使用任何密碼術演算法產生該MAC。

於本發明之一例示性實施例中，僅可使用諸如EPROM等技術寫入該第一記憶體位置一次。可經程式化及通常擦除EPROM(可擦除可程式化唯讀記憶體)以允許重新使用。

通常使用一穿過 EPROM 中石英擦除窗口發光之紫外 (UV) 光源來實現擦除。於一例示性實施例中，該 EPROM 晶片覆蓋有一不允許紫外 (UV) 光穿過並擦除記憶體內容之遮罩。另一選擇係，可使用一次性可程式化 (OTP) EPROM (其有時被稱作一次性可程式化唯讀記憶體 (OTPRAM))。OTP EPROM 無擦除窗口，此乃因該類記憶體僅可被程式化一次。該第二記憶體位置組態為一正常記憶體位置並可像正常記憶體一樣寫入，然而，當該第二記憶體位置被讀取時，返回彼位置與一姐妹記憶體位置 (例如第一記憶體位置) 之 AND。該組合邏輯被硬編碼進請求者之讀取定址方案中。

圖 1 之流程圖繪示本發明之一例示性實施例。圖 1 繪示根據本發明一實施例由一驗證系統鑑別一請求者之性質之例示性方法。該方法包括一製造伺服器在製造時將一序號識別符寫入一請求者之記憶體中 (100)。該製造伺服器使用一密碼術演算法及該請求者之序號產生一訊息鑑別碼 (MAC) (110)。該製造伺服器將該訊息鑑別碼寫入至該請求者上之該第二記憶體位置 (120)。

在稍後某時刻，該驗證系統確定需要鑑別該請求者之性質 (125)。舉例而言，於一列印頭實施例中，可能已安裝一新墨筒，且該印表機 / 電腦請求鑑別該列印頭之預期身份。該驗證系統產生一隨機詢問用語並將該隨機詢問用語寫入該請求者上一第一記憶體中 (130)。該驗證系統與該請求者彼此電氣通信且可直接連接或藉由諸如網際網路等資

料通信鏈路遠程連接。於一進一步實施例中，該請求者確保該詢問用語滿足任何預定之詢問用語要求(140)。舉例而言，該請求者可確保在將該詢問用語寫入該第一記憶體位置之前該詢問用語由50%的1構成。因應該驗證系統對該請求者之該第二記憶體位置之一讀取請求，該請求者以一回應用語(其包括儲存於該第一記憶體位置中之詢問用語與儲存於該第二記憶體位置中之MAC之一AND)做出回應(150)。

在鑑別過程中之某一時刻，驗證系統自該請求者之記憶體中讀取序號識別符(160)。該驗證者使用在製造時用於產生該MAC之相同密碼術演算法依據該序號識別符產生一比較訊息鑑別碼(170)。

該驗證系統自該請求者接收回應用語(180)。該驗證者執行該詢問用語與一比較訊息鑑別碼之AND來產生一比較碼(190)。然後該驗證系統比較該回應用語與該比較碼(200)。於一例示性實施例中，該比較查看該回應用語是否與該比較碼匹配(210)。若該回應用語不匹配該比較碼，則不鑑別該請求者之性質(220)。反之，若該回應用語匹配該比較碼，則鑑別該請求者之性質(240)。

於一例示性實施例中，當至少95%之比較碼匹配該回應用語時，該驗證系統將鑑別該請求者之性質。於某些情況下，該請求者之性質僅可鑑別一次。於此一例示性實施例中，該比較步驟可進一步包括確定該序號是否先前已被鑑別過。若該序號先前被已鑑別過，則不重新鑑別該請求

者。

於又一例示性實施例中，該請求者經組態以允許多次鑑別。於該實施例中，可提供多對隱藏記憶體(即MAC)及姐妹(即詢問用語)記憶體位置。由於該第一記憶體位置僅可寫入一次，因而該第一記憶體位置在已被寫入後將不接受另一詢問用語。因此，該驗證系統可包括用於確定該請求者中哪一記憶體位置係用於當前鑑別之邏輯。舉例而言，該驗證器可讀取該第一記憶體位置以查看其內容是否為空。若是，則該驗證系統會將一詢問用語寫入用於彼當前鑑別位置之第一記憶體位置。若否，則該驗證系統然後將移至下一預定記憶體位置以查看其是否為空等等。於另一例示性實施例中，該驗證者可鑑別每一先前使用之隱藏式記憶體位置與含有50%的1之姐妹位置。於再一例示性實施例中，可使用不同之密鑰或密碼術演算法在每一記憶體位置中產生該MAC。於該實施例中，該等製造及驗證伺服器將需要處於同步狀態以瞭解哪一密鑰將用於每一記憶體位置。

雖然已顯示並闡述本發明之特定實施例，但彼等熟習此項技術者將明顯看出可在不背離本發明精神及範疇之前提下進行其他各種改變及修改。因此本發明意欲在該隨附申請專利範圍中囊括所有此等屬於本發明範疇內之修改及改變。

### 【圖式簡單說明】

雖然該說明書以特別指出並明確主張本發明之申請專利

範圍結束，但咸信結合隨附圖式閱讀上文說明將更易理解本發明。

圖 1A 及 1B 繪示一根據本發明一第一實施例用於將一鑑別回應自一物品發送至一驗證系統之例示性方法之流程圖。

該等圖式中所陳述之實施例係舉例說明性質而非意欲限制由該申請專利範圍所界定之本發明。而且，根據詳細說明將更完全地明瞭及理解該等圖式及本發明之個別特徵。

## 十、申請專利範圍：

101年11月24日修正對照本

1. 一種用於自一物品發送一鑑別回應至一驗證系統之方法，其包括：

在該物品上一第一記憶體位置中儲存一詢問用語，其中該詢問用語係接收自該驗證系統；

自該物品上一第二記憶體位置擷取一訊息鑑別碼，其中該訊息鑑別碼係在該物品之製造時儲存於該第二記憶體位置中；

因應自該驗證系統中接收到對該第二記憶體位置之一讀取請求，發送該詢問用語與該訊息鑑別碼之一組合邏輯閘輸出；

擷取一儲存於該物品上之序號識別符，其中該序號識別符係在該物品之製造時儲存於該物品上；

因應一來自該驗證系統對該序號識別符之請求，將該序列識別符發送至該驗證系統；

將一第二詢問用語儲存至該物品上一第三記憶體位置內，其中該第二詢問用語係接收自該驗證系統；

自該物品上一第四記憶體位置擷取一第二訊息鑑別碼，其中該第二訊息鑑別碼係在該物品之製造時儲存於該第四記憶體中；以及

因應自該驗證系統接收到對該第四記憶體位置之一讀取請求，發送該第二詢問用語與該第二訊息鑑別碼之一第二組合邏輯閘輸出。

2. 如請求項1之方法，其進一步包括驗證自該驗證系統接

101年1月3日修正對策

收之該詢問用語。

3. 一種經組態以與請求項1之方法一起使用之物品。
4. 如請求項3之物品，其中該物品包括一列印頭及一供墨盒中之一者。
5. 如請求項3之物品，其中該驗證系統包括一與該列印頭電氣通信之印表機。
6. 如請求項1之方法，其中該驗證系統包括一與該物品電氣通信之遠端伺服器。
7. 如請求項3之物品，其中該驗證系統包括一與該列印頭電氣通信之電腦。
8. 如請求項1之方法，其中該詢問用語包括50%的1及50%的0。
9. 如請求項1之方法，其中該訊息鑑別碼包括一已加密序號識別符。
10. 如請求項1之方法，其中該組合邏輯閘包括一AND閘。
11. 如請求項1之方法，其中該組合邏輯閘包括一OR閘。

十一、圖式：

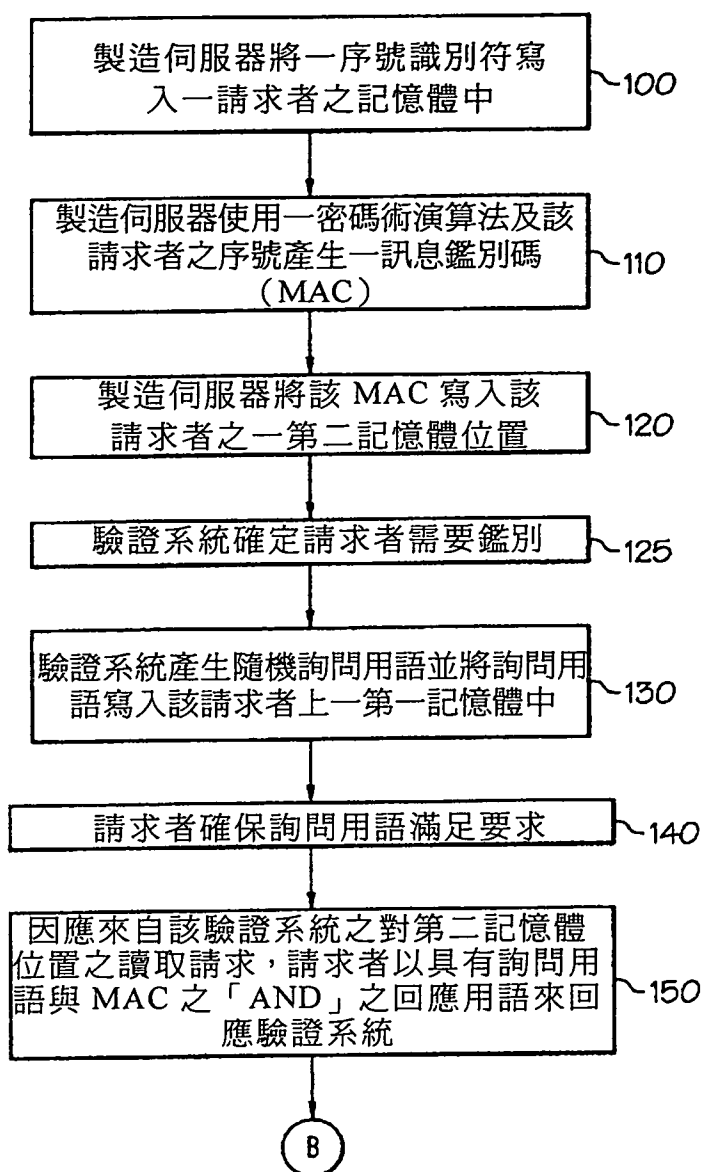


圖 1A

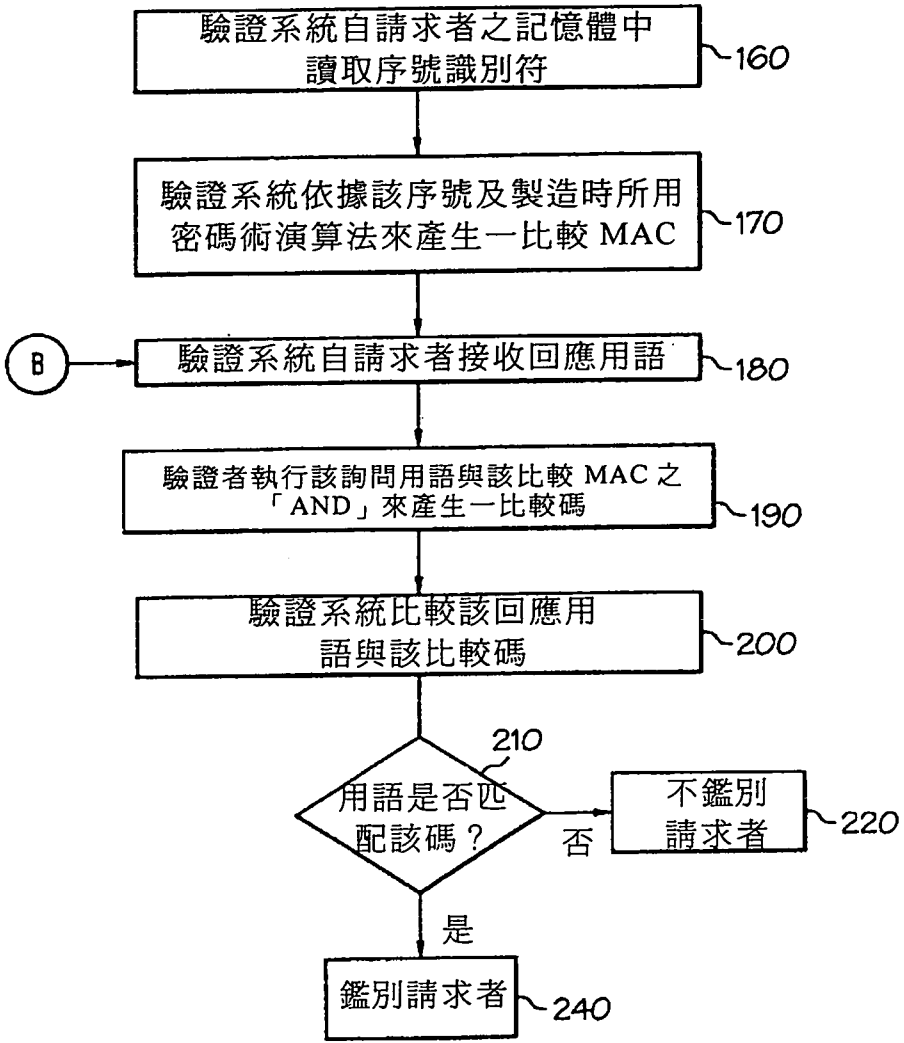


圖 1B

