發明專利說明書200423604

（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：93116837

※ 申請日期：93-06-10　　※IPC 分類：H04K1/00

壹、發明名稱：（中文/英文）

通信系統中之金鑰產生

KEY GENERATION IN A COMMUNICATION SYSTEM

貳、申 請 人：（共 1 人）

姓名或名稱：（中文/英文）

美商奎康公司

QUALCOMM INCORPORATED

代表人：（中文/英文）

喬治 A. 懷坦

GEORGE A. WHITTEN

住居所或營業所地址：（中文/英文）

美國加州聖地牙哥市摩豪斯大道 5775 號

5775 MOREHOUSE DRIVE SAN DIEGO, CA 92121-1714 U.S.A.

國　籍：（中文/英文）

美國　　U.S.A.

參、發明人：（共 1 人）

姓　名：（中文/英文）

雷蒙 T-S. 徐

RAYMOND T-S.HSU

住居所地址：（中文/英文）

美國加州聖地牙哥市派那庫克大道 17775 號

17775 PENNACOOK COURT, SAN DIEGO, CALIFORNIA 92127, U.S.A.

國　籍：（中文/英文）

美國　　U.S.A.

肆、.聲明事項：

☐ 本案係符合專利法第二十條第一項☐第一款但書或☐第二款但書規定之期間，其日期為： 年 月 日。

☑ **本案申請前已向下列國家（地區）申請專利：**

1.美國; 2002 年 06 月 20 日; 10/177,017

2.

3.

4.

5.

☑ **主張國際優先權(專利法第二十四條)：**

【格式請依：受理國家（地區）; 申請日；申請案號數 順序註記】

1.美國; 2002 年 06 月 20 日; 10/177,017

2.

3.

4.

5.

☐ **主張國內優先權(專利法第二十五條之一)：**

【格式請依：申請日；申請案號數 順序註記】

1.

2.

☐ **主張專利法第二十六條微生物：**

☐ 國內微生物 【格式請依：寄存機構；日期；號碼 順序註記】

☐ 國外微生物 【格式請依：寄存國名；機構；日期；號碼 順序註記】

☐ 熟習該項技術者易於獲得，不須寄存。

玖、發明說明：

【發明所屬之技術領域】

本發明係關於一通信系統之互通功能，尤其是關於透過無線區域網路(WLAN)中使用之一互通功能之共同鑑認與金鑰交換機制。

【先前技術】

無線區域網路(WLAN)允許使用者實質上無限制存取網際網路協定(IP)服務與資料網路。使用一WLAN並不限於膝上型電腦及其他計算裝置，而是迅速擴大包括行動電話、個人數位助理(PDA)以及由外部網路或載波所支援之其他小型無線裝置。例如，經由一行動系統載波(cellular carrier)通信之無線裝置可在網路咖啡店或工作室漫遊在WLAN之中。按此情況，無線裝置已獲得行動系統存取權，但希望進一步存取WLAN。WLAN存取需要鑑認。因為無線裝置業已獲得行動系統存取權，所以需要進一步鑑認是多餘的。因此，需要一種允許存取一行動系統且存取一WLAN之共同鑑認機制。而且，需要一種用於產生在通信期間所使用之加密金鑰的共同機制。

【發明內容】

一種產生一主控會期金鑰(MSK)之通信系統，該MSK係用於存取不提供通信流量加密之系統實體。本方伺服器和使用者兩者均產生相同MSK。該MSK係用以產生通信流量之加密金鑰。在一項實施例中，使用一雜湊函數及請求者特定之資訊來產生該MSK。本方伺服器根據一存取請求訊

息內所含之資訊來決定產生MSK之需求。一旦產生，即將該MSK提供給系統實體，使該實體能夠加密通信流量。

【實施方式】

本文中專用的術語「示範」係表示「當作範例、實例或圖例說明」。本文中當作「示範」說明的任何具體實施例不一定被視為較佳具體實施例或優於其他具體實施例。

一HDR用戶台(本文中稱為一存取終端機(AT))可為行動或固接式，且可與一個或多個HDR基地台(本文中稱為數據機集區收發機(MPT))通信。一存取終端機可透過一個或多個數據機集區收發機發送及接收資料封包至一HDR基地台控制器(本文中稱為數據機集區控制台(MPC))。數據機集區收發機和數據機集區控制器屬於稱為存取網路之網路的部件。一存取網路傳輸介於多個存取終端機之間的資料封包。存取網路可進一步被連接至存取網路外部之額外網路(諸如企業內部網路或網際網路)，並且可傳輸介於每一存取終端機與此種外部網路之間的資料封包。已建立與一個或多個數據機集區收發機連線之啟用中通信流量頻道連接之存取終端機係稱為啟用中存取終端機，且表示其係處於通信中狀態。正在建立與一個或多個數據機集區收發機連線之啟用中通信流量頻道連接過程中的存取終端機表示其係處於一連接建立狀態。存取終端機可為透過無線頻道或有線頻道(光纖或同軸纜線)通信之任一資料裝置。一存取終端機進一步可為任一眾多類型之裝置，包括但不受限於PC卡、小型快閃記憶體、外接式或內建數據機、無線或有線

電話。存取終端機發送信號至數據機集區收發機所使用之通信鏈路係稱為反向鏈路。數據機集區收發機發送信號至存取終端機所使用之通信鏈路係稱為正向鏈路。

圖1描繪一種具有一含多個存取點(AP)之無線區域網路(WLAN)104的通信系統。一AP係一集線器或橋接器，用於提供WLAN 104無線端之一星形樸拓控制，以及存取一有線網路。

每一AP 110以及圖未示之其他AP都可支援一連線至一資料服務(諸如網際網路)的連線。一MS 102(諸如一膝上型電腦或其他數位計算裝置)可經由空中介面而與AP通信，因此稱為「無線LAN」。該AP然後與一鑑認伺服器(AS)或鑑認中心(AC)通信。AC是一種針對要求進入網路之裝置執行鑑認服務之元件。實施包括遠端鑑認撥接使用者服務 (Remote Authentication Dial-in User Service；RADIUS) 伺服器(1997年4月公佈由C. Rigney 等人所著「遠端鑑認撥接使用者服務(RADIUS)」，這是在RFC 2138中所述之一網際網路使用者鑑認)，以及鑑認、授權及帳戶處理(Authentication, Authorization, and Accounting；AAA)伺服器。

無線網路正顯現為網際網路之一重要層面。一無線網路之唯一邊界是無線電信號強度之事實，使得無線網路呈現一組獨特問題。沒有任何佈線來界定一網路中的成員。沒有任何實質方法將一無線電範圍內之系統限制為一無線網路之一會員。無線網路比任何其他網路技術更需要一鑑認和存取控制機制。不同團體目前正在研發一標準鑑認機

制。目前可接受之標準是IEEE 802.11。

一RF基礎網路之性質造成處於開放藉由發射機範圍內無線電進行封包攔截之狀態。藉使用高增益天線，就可在遠離使用者"工作"範圍之外進行攔截。利用很容易獲得之工具，竊聽者並非限於僅收集封包供以後分析，而且還能夠實際知道互動會期，例如有效無線使用者所檢視之資訊網頁。一竊聽者亦能獲取低安全保護鑑認交換，像某些網站登入。竊聽者爾後可複製登入並獲得存取權。

一旦攻擊者已獲得一WLAN如何控制存取許可之知識時，就能夠自行獲得網路的存取許可權，或者竊取一有效使用者之存取權。若攻擊者能模擬該有效使用者之MAC位址，且使用其指定IP位址，就可輕而易舉地竊取一使用者之存取權。攻擊者一直等待有效系統停止使用網路，然後接管其在網路內之位置。這會允許一攻擊者直接存取在一網路內之所有裝置，或使用該網路來獲得存取較寬頻之網際網路，始終就像是受攻擊網路的一有效使用者。因此，在WLAN實施中，鑑認及加密變成主要考量點。

鑑認係證明通信中之個人或應用程式之識別身分的程序。此種鑑認允許服務業者確認定實體為一有效使用者，並且還針對特定服務要求來確認使用者。鑑認及授權實際上具有十分特定意義，雖然兩名稱常被交換使用，且實質上常難加以清楚區別。

鑑認係一種使用者證實識別身分之權利的程序一本質上，使用一名稱之權利。現有大量技術可使用來鑑認使用

者，例如，密碼、生物測定技術、智慧卡、憑證。

一名稱或識別身分具有與其關聯之屬性(attribute)。屬性可密切繫結一名稱(例如，在一憑證酬載內)，或依據一相對應於該名稱之金鑰將屬性儲存在目錄或其他資料庫內。屬性可能會隨時間改變。

授權係用於決定是否容許一識別身分(加上與該識別身分相關聯之一組屬性)執行某動作(例如，存取一資源)之程序。應注意，容許執行一動作並非保證能執行該動作。請注意，可由不同實體在不同點進行鑑認及授權。

在一行動通信網路內，鑑認特徵係一用於允許行動通信網路驗證無線裝置之識別身分的網路能力，藉以減少未經授權使用行動通信網路。此程序不會被用戶察覺到。當用戶打電話時並不需要任何動作來鑑認其電話之識別身分。

鑑認典型上包括一密碼編譯(cryptographic)機制，其中服務提供者和使用者具有一些共用資訊和一些私人資訊。共用資訊典型上稱為"共用祕密"。

A-金鑰

鑑認金鑰(A-金鑰)係對每一個人之行動電話所唯一的祕密值。A-金鑰係向行動通信服務提供者註冊且係儲存在電話及鑑認中心(AC)中。製造商將A-金鑰程式規劃在電話內。使用者也可以從無線裝置功能表手動輸入A-金鑰，，或由銷售點的特殊終端機輸入A-金鑰。

無線裝置和AC必須有相同A-金鑰才能產生相同計算結果。A-金鑰之主要功能係當做用來計算共用祕密資料(SSD)

之一參數。

共用祕密資料(SSD)

SSD係當做在無線裝置和AC內鑑認計算的一輸入，且被儲存在這兩個地點。不同於A-金鑰，可透過網路修改SSD。AC及無線裝置可共用參與SSD計算之三個要素：1)電子序號(ESN)；2)鑑認金鑰(A-金鑰)；及3)「共用祕密資料」計算(RANDSSD)之 RANDom數。

ESN和RANDSSD係透過網路和透過空中介面發送。當一裝置進行第一次系統存取時會更新SSD，且此後定期更新。當計算SSD時，其結果是兩個獨立值SSD-A和SSD-B。SSD-A係用於鑑認。SSD-B係用於加密及語音隱密。

視伺服方系統之能力而定，AC與伺服方行動交換中心(MSC)之間可以共用或不共用SSD。若要共用祕密資料，則表示AC會將祕密資料發送至伺服方MSC，並且伺服方MSC必須能夠執行CAVE。若不要共用祕密資料，AC可保持資料並執行鑑認。

共用之類型會影響如何引導一鑑認詢問(authentication challenge)。一鑑認詢問係詢問無線裝置之識別身分所發送之一訊息。基本上，鑑認詢問可發送使用者所要處理的一些資訊，典型上即亂數資料。然後，該使用者處理該資訊且發送一回應。分析該回應以確認使用者。配合共用之祕密資料，由伺服方MSC處理一詢問。配合非共用之祕密資料，由AC處理一詢問。藉由共用祕密資料，該系統可使發送之通信流量減至最少，並且允許在伺服方交換機處更快

發生詢問。

鑑認程序

在一已知系統內，藉由將一本方位置暫存器(HLR)當作介於MSC與AC間之中間裝置來控制鑑認程序。可設定伺服方MSC用行動台的HLR來支援鑑認，反之亦然。

裝置起始鑑認程序的方式為，設定添加信號訊息串(overhead message train)中的一授權欄位，藉以向伺服方MSC通知其能夠具有鑑認能力。在回應中，伺服方MSC使用一鑑認請求來開始註冊/鑑認程序。

藉由發送鑑認請求，伺服方MSC即告知HLR/AC它是否能執行CAVE計算。AC可控制可用的伺服方MSC能力與裝置能力中所要使用的能力。當伺服方MSC並未具有CAVE能力時，在AC與MSC之間不能共用SSD且因此在AC內執行所有鑑認程序。

鑑認請求(AUTHREQ)之用途為鑑認電話並所請求之SSD。AUTHREQ包含兩個鑑認參數AUTHR和RAND參數。當AC獲得AUTHREQ時，隨即使用RAND與最後獲知之SSD來計算AUTHR。若符合在AUTHREQ內所發送之AUTHR，則鑑認成功。如果可共用SSD，則AUTHREQ的傳回結果會包含SSD。

詢問

鑑認程序係由一詢問與回應對話所組成。若是共用SSD，則會在MSC與該裝置之間進行對話。若是未共用SSD，則會在HLR/AC與該裝置之間進行對話。視交換機之

類型而定，MSC可能具有唯一性詢問、全域性詢問或兩者之能力。有些MSC目前不具有全域性詢問之能力。因為唯一性詢問使用語音頻道，所以僅在呼叫嘗試期間才會發生唯一性詢問。在呼叫起始與呼叫傳遞期間，唯一性詢問將一鑑認呈遞給一單一裝置。全域性詢問係在註冊、呼叫起始及呼叫傳遞期間發生之詢問。全域性詢問將一鑑認詢問呈遞給正在使用一特殊無線電控制頻道的所有MS。因為會在無線電控制頻道上廣播全域性詢問，並且正在存取該控制頻道的所有電話都會使用該詢問，所以稱為全域性詢問。

在一詢問期間，裝置可回應由MSC或AC所提供之亂數。該裝置使用該亂數及裝置內儲存之共用祕密資料來計算對該MSC之一回應。MSC亦使用該亂數及共用祕密資料來計算所來自該裝置之回應。經由CAVE演算法即可完成此等計算。若回應並不相同，則拒絕服務。詢問程序不會增加連接呼叫所花之時間量。事實上，可在某些情況下進行此呼叫，僅當鑑認失敗時才斷線。

無線區域網路(WLAN)已獲非常普及作為提供使用者開放存取IP資料網路之一裝置。還設計出提供高速資料存取的高資料率(HDR)網路，諸如1xEV-DO網路和其他第三代(3G)網路；雖然這些網路支援之資料率典型上低於WLAN之資料率，但是3G網路提供更廣的資料涵蓋範圍。雖然WLAN及HDR網路被視為競爭對手，但是WLAN及HDR網路可互補；WLAN在公共場所(諸如機場接待室及旅館候客廳)提供高容量作用點(hot-spot)涵蓋範圍，而HDR網路可為移

動中使用者提供近乎無所不在之資料服務。因此，相同載波可依據一單一使用者訂購同時提供HDR與WLAN兩種存取服務。此表示MS可針對這兩種類型之存取鑑認使用相同鑑認方法及祕密。

HDR網路及WLAN存取鑑認兩者可使用一項協定，諸如「詢問信號交換鑑認協定」(Challenge Handshake Authentication Protocol；CHAP)，亦稱為MD5詢問。CHAP明確使用RADIUS協定來鑑認終端機，而不需要發送安全保護資料。MS係由其本方RADIUS伺服器予以鑑認，其中本方RADIUS伺服器與MS可共用一根祕密(root secret)。在經由一CHAP詢問成功地鑑認MS後，MS和本方或HDR網路可推導出相同加密金鑰，以便使用加密金鑰來保護介於MS與WLAN存取點(AP)間所交換之通信流量。

在經由一CHAP詢問成功的WLAN存取鑑認後，本方RADIUS伺服器與MS可從共用根祕密產生相同之主控會期金鑰(MSK)。使用MSK來推導出加密金鑰，以便使用加密金鑰來保護介於MS與WLAN之AP間的實際通信流量。共用根祕密係配置給MS且係靜態的。會以每封包資料會期為基礎來產生MSK，並且僅在該會期期間固定不變。若是一新的會期，則使用一不同亂數從共用根祕密產生一新MSK。

因為當MS存取HDR網路時並不需要MSK，所以一項實施例提供一種允許本方RADIUS伺服器決定MS是否正在存取WLAN或HDR網路的機制。

圖1描繪一通信系統100，包括一HDR網路106，一WLAN

104，及一MS 102。MS 102係能夠存取HDR網路106，且已漫遊至一WLAN 104之涵蓋區內。MS 102經由WLAN 104內的AP 110試圖存取WLAN 104。請注意，WLAN 104可包括任何數量之AP(圖未示)。WLAN 104亦包括一鑑認、授權及帳戶處理(AAA)實體或伺服器112。請注意，HDR網路106亦包括一AAA伺服器108。

圖2描繪當在通信系統100內使用CHAP或MD5詢問時為存取鑑認一WLAN之訊息流程圖。MS 102使用一識別用之「網路存取識別碼」(NAI)。NAI的格式為使用名稱@網域，其中網域識別MS之本方網路，在實例中，本方網路即係HDR網路106。在WLAN網路104內之AAA伺服器112可啟始一RADIUS存取請求訊息，以發送給位於MS 102本方網路之AAA伺服器108，亦即發送給HDR網路106。請注意，HDR網路106可能是支援高資料率傳輸的任一網路。然後，AAA 108經由WLAN 104將一CHAP詢問發出至MS 102。MS 102根據該詢問(例如一亂數)來計算一回應，且將該回應當做一「RADIUS存取請求」請求以經由WLAN 104載送至AAA 108。若鑑認成功，則本方AAA伺服器108用一RADIUS存取接受訊息授予MS 102存取WLAN網路104來認可鑑認成功。如以上論述，本方AAA伺服器108和MS 102都會利用一共用根祕密來產生一相同的主控會期金鑰(MSK)。

如上述，行動通信普遍使用CAVE演算法，因此，已妥善使用和分配CAVE演算法。亦可使用替代之鑑認演算法。具體而言，在資料通信中有不同複雜性和應用的各種演算

法。為協調此等機制，已發展出可擴展鑑認協定(EAP)，用以當做支援多重鑑認及金鑰分配機制之一通用協定構架。在1998年3月公佈之RFC 2284，由L. Blunk 等人所著"PPP可擴展鑑認協定(EAP)"內即說明EAP。

按照2002年2月被公佈為一網際網路草案之由J. Ackko等人所著"EAP AKA鑑認"中的定義，由EAP所支援之一項此類機為AKA演算法。因此需要擴充EAP以納入行動通信演算法CAVE。此乃期望能提供新系統及網路之回溯相容性。

EAP

可擴展鑑認協定(EAP)係一種支援多重鑑認機制的一通用鑑認協定。EAP並非在鏈路建置和控制期間選擇一特定鑑認機制，反而是延緩到鑑認程序開始。此可讓鑑認器在決定特定鑑認機制以前請求更多資訊。鑑認器被定義為需要鑑認之鏈路的末端。鑑認器指定要在鏈路建置期間使用的鑑認協定。

金鑰產生

金鑰階層架構(key hierarchy)是用於從一根金鑰來產生一組加密金鑰的步驟序列，而加密金鑰則是用來加密/解密訊息，或者鑑認訊息。一金鑰階層架構應包括某時間變化資訊，促使每次使用該階層架構時不致產生同一組加密金鑰。一金鑰階層架構還應該建置成，如果所推導出的加密金鑰已變成已知的金鑰，則不能自加密金鑰獲得根金鑰。

在一項實施例中，整個金鑰階層架構係由三個較小型之分層式金鑰階層架構所組成：主控金鑰階層架構(master

key hierarchy)；金鑰重新產生金鑰階層架構(rekeying key hierarchy)；及每封包金鑰階層架構(per-packet key hierarchy)。視該階層架構及鑑認方法而定，主控金鑰階層架構可包括EAP金鑰產生、預先共用金鑰或亂數。若EAP金鑰產生係用於主控金鑰階層架構，則主控金鑰階層架構通常係駐在RADIUS伺服器上。

金鑰重新產生階層架構具有稱為成對式(Pairwise)金鑰階層架構及群組(Group)金鑰階層架構的兩種類型。此兩種類型階層架構內之步驟類似；僅兩種類型之輸入不同。

每封包金鑰階層架構可用於TKIP(使用一RC4加密引擎)，或者用於AES。

成對式金鑰階層架構係用來推導出在一無線網路之兩個實體之間所使用的金鑰(AP與相關聯之工作站，或在一網路內的一對工作站)。

群組金鑰階層架構係用來推導出及傳送在一無線群組內所有實體所使用的金鑰(AP及一網路內與該AP相關聯之所有工作站，或在一網路內之所有實體)。

在正使用成對式金鑰的兩個實體上，以平行方式產生成對式金鑰階層架構例項(instantiation)，其中每個實體都會使用共同資訊來計算同一組加密金鑰。兩個實體之一可驅動對成位置金鑰階層架構，該實體稱為成對式金鑰擁有者。針對一已知網路，該成對式金鑰擁有者即係AP；針對其他網路，則每一可能成對的工作站將具有一成對式金鑰階層架構，且成對式金鑰擁有者係該對工作站中擁有較低

層媒體存取控制層位址之工作站。

僅會在一個實體上產生群組金鑰階層架構例項，並且會將推導出之加密金鑰公佈給所有其他實體；驅動群組金鑰階層架構之實體係群組金鑰擁有者。針對一已知網路(例如稱為一基本服務組(BSS)之網路)，群組金鑰擁有者即係AP；針對一獨立基本服務組(IBSS)網路，群組金鑰擁有者係現行信標發送機。請注意，一BSS網路係由一AP和相關聯之工作站所組成，然而一IBSS網路係由一組工作站所組成，所有工作站係相互對等體。本文所使用之用詞「工作站」包括一行動台或能夠存取一區域網路之其他無線裝置。

每個工作台都具有至少兩個金鑰階層架構例項，且十分可能有更多金鑰階層架構例項。在一BSS網路內，AP具有用於每個相關聯工作站的一成對式金鑰階層架構例項，並且具有至少一群組金鑰階層架構；AP係所有此等階層架構之金鑰擁有者。每一相關聯之工作站都具有一個成對式金鑰階層架構例項，且具有至少一群組金鑰階層架構。針對IBSS網路，每個工作站都具有一適用於網路內每個其他工作站的成對式金鑰階層架構例項，以及一單一群組金鑰階層架構。

金鑰擁有者具有用於群組金鑰的一單一群組金鑰重新產生階層架構例項，及適用於每一關聯的一成對式金鑰重新產生階層架構例項。一金鑰擁有者具有一按照群組及成對式暫時金鑰(若有)之「臨時金鑰完整性協定」(TKIP)之暫時金鑰的每封包金鑰階層架構。一非金鑰擁有者具有一依照

關聯之用於群組金鑰及成對式金鑰的金鑰重新產生階層架構例項，以及具有一依照群組及成對式的暫時金鑰(若有)之TKIP暫時金鑰的每封包金鑰階層架構。

MSK

依據示範性實施例，MSK包括「行動通信訊息加密演算法」(CMEA)金鑰(用於保護如傳送至WLAN的MS通信流量)及一密碼金鑰(CK)。

圖3描繪產生加密金鑰之金鑰階層架構以保護介於MS 102與WLAN網路104間之通信流量。程序開始於協商MS 102識別身分。然後WLAN 104發送一RADIUS存取請求訊息至AAA 108，而AAA 108會回應一RADIUS存取詢問訊息。WLAN 104將詢問傳給MS 102，而MS 102從該詢問計算出一回應。然後將MS 102的詢問回應提供給WLAN 104。在步驟4a中，在MS 102發送鑑認回應給WLAN 104後，MS 102即使用根祕密來產生主控會期金鑰(MSK)。

WLAN 104發送RADIUS存取請求訊息至AAA 108，包括詢問回應。在步驟5a中，若成功鑑認MS 102，本方AAA伺服器108可使用MS 102根祕密來產生相同於在步驟4a中由MS 102所產生的MSK。在步驟6中，本方AAA伺服器108使用一屬性(例如MS-MPPE-Recv-Key屬性)，將MSK納入RADIUS存取接受訊息內。在步驟7中，MS 102及WLAN網路104使用適用於從MSK產生加密金鑰的程序，例如，2002年3月IEEE標準802.11i/D2.0標題為「Draft Supplement to Standards for Telecommunications and Information Exchange

Between Systems – LAN/MAN Specific Requirements--Part 11: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Specifications for Enhanced Security」(本文中稱為"802.11i標準")文件中所指定的程序。

以下提供在MS 102及本方AAA伺服器108中用以產生MSK的演算法及參數之兩個範例。按第一實施例，MSK係定義為：

MSK=雜湊函數(祕密，詢問，NAI，祕密)　　(1)

其中MSK係使用以下參數應用一雜湊函數(例如，CHAP，HMAC)之結果：

- MS 102根祕密；
- 在圖3中之步驟4至步驟5中用以鑑認MS 102的詢問；
- MS 102 NAI；及
- MS 102根祕密再來

根據本實施例，MS 102和本方AAA伺服器108具有用於獨立產生相同MSK所必需之所有金鑰資料。換言之，在MS 102與本方AAA伺服器108之間不需要交換用於MSK產生的額外金鑰資料。請注意，MSK和MS 102存取從一相同詢問值所產生的鑑認回應。一替代實施例可從一不同亂數值產生MSK。

按照另一實施例，一第二範例將MSK定義為：

MSK=雜湊函數(祕密，NAI，亂數)　　(2)

其中MSK係使用以下參數應用一雜湊函數(例如，CHAP，HMAC)之結果：

- MS 102根祕密；

- MS 102 NAI；及
- 由本方AAA伺服器所產生之一亂數，

其中該亂數不同於詢問值。依據此實施例，會從一不同於在MS 102存取鑑認過程中所使用之詢問值的亂數來產生MSK。使用獨立詢問值可降低介於MSK與MS 102存取鑑認之間的關聯性，且因此可改進安全性。請注意，會將亂數發送至MS 102，並且從該亂數產生MSK。會經由一RADIUS存取接受(圖3中的步驟6)及802.11i標準(圖3中的步驟7)中定義之機制，將亂數發送至MS 102。

當MS 102正存取一WLAN 104時會使用用於產生MSK之程序，而當MS正存取1xEV-DO或其他HDR網路時則不會使用此程序。這是因為HDR系統提供了無線通信加密(over the air encryption)。當MS啟始存取WLAN網路104或存取HDR網路106時，MS 102能夠決定是否需要MSK產生。然而，本方AAA伺服器亦必須決定何時產生MSK。

在一項實施例中，實施一特定RADIUS屬性以通知AAA 108產生一MSK。在圖3之步驟2及步驟5中，WLAN網路104所發送的RADIUS存取請求訊息中包含一用於指示MS 102希望或正請求WLAN 104存取的特定或指定之屬性。此屬性狀態會觸發本方AAA伺服器108執行MSK產生(若MS 102鑑認已成功)。當RADIUS存取請求訊息中沒有指定之屬性時，本方AAA伺服器108就不會執行MSK產生。請注意，為實施與3GPP2一致之系統，該指定之屬性係3GPP2所特有且因此可被定義為具有3GPP2廠商ID的廠商特定屬性。

圖4描繪在2000年6月公佈之RFC 2865，由C. Rigney 等人所著標題為"遠端鑑認撥接使用者服務(RADIUS)"中所述之RADIUS格式。資料格式200包括：一代碼欄位202，用於識別RADIUS封包之類型(例如存取請求，存取拒絕，等等)；一ID欄位204，用於協調相符之請求及回應；及一長度欄位206，用於指示相關聯封包之長度。圖中還描繪一屬性220，其包括：一類型欄位222，用於識別該值欄位226之內容；一長度欄位224，用於提供該屬性之長度；及一值欄位226，用於提供該屬性之特定資訊。請注意，RADIUS可支援廠商特定之屬性，其中該值欄位226係用於提供廠商識別，之後接著屬性資訊。按照1999年3月公佈之RFC 2548，由G. Zorn所著標題為"微軟廠商特定RADIUS屬性"中所述，廠商特定類型可應用於CHAP訊息。

一替代實施例在RADIUS存取請求訊息中實施一稱為網路存取伺服器(NAS)網際網路協定(IP)位址的標準屬性。標準屬性識別起始RADIUS存取請求訊息之RADIUS用戶端的IP位址。本方AAA伺服器係配置有一資料庫，該資料庫中含有在WLAN網路104內所有RADIUS用戶端的IP位址。如果在NAS IP位址屬性內所指示之IP位址相符於資料庫內之一位址，則RADIUS存取請求訊息係源自於WLAN網路104，且本方AAA伺服器108即執行MSK產生(若MS鑑認已成功)。否則，本方AAA伺服器108即不會執行MSK產生。

圖5描繪標準屬性之格式，以及一疊加在值欄位上之範例。屬性格式300包括：一類型欄位302，用於識別一值欄

位306之內容；一長度欄位304，用於提供該屬性之長度；及一值欄位306，其內含屬性資訊。請注意，在修改RFC 2865內所供之說明的情況下，值欄位306可被分割成多個顯著性欄位，包括：類型322，用於指示次屬性類型，諸如一MSK產生指令；一長度欄位324，用於提供次屬性之長度；及一值欄位326，其內含次屬性資訊，諸如一MSK產生指示項。舉例而言，若要傳送一訊息至AAA 108以向AAA 108指示MSK產生，則類型欄位322可使用一相對應之預先定義代碼而將此次屬性識別為一MSK產生指令。然後，值欄位326的值為：1－指示AAA 108產生一MSK；或2－指示AAA 108不產生該MSK。

圖6描繪一無線裝置，例如MS 102。該裝置600包括分別用接收傳輸及發送傳輸的接收電路602及發送電路604。接收電路602及發送電路604都被耦合至一通信匯流排612。該裝置600亦包括一中央處理器(CPU)606，用於控制該裝置600內之操作。CPU 606回應儲存在裝置600之記憶體儲存裝置內的電腦可讀型指令。圖中將兩個此類儲存裝置描繪成用於儲存鑑認程序608及MSK產生610。請注意，替代實施例可在硬體、軟體、韌體或其組合內實施該程序。然後CPU 606回應來自鑑認程序608之鑑認處理指令。CPU 606可將該鑑認程序608訊息置入於一傳送格式內，諸如一EAP格式。一旦對WLAN鑑認時，CPU 606回應MSK產生器610以產生MSK。CPU 606進一步處理所接收到之傳送格式訊息以從該傳送格式訊息擷取鑑認訊息。

請注意，雖本文內所述實施例詳述WLAN，但本文內所述方法及裝置亦可適用於其他系統實體。本發明可提供一種促使一系統實體能夠提供通信加密之方法。藉由使用本方伺服器來產生MSK，並將MSK提供給一系統實體，即提供該實體足夠資訊，而得以保護傳輸給一使用者(諸如一MS)的安全性。

熟習此項技術者應明白，可使用各種不同術語或技術的任一種來代表資訊及信號。例如，資料、指令、命令、資訊、信號、位元、符號及晶片有利於以電壓、電流、電磁波、磁場或粒子、光場或粒子、或其任何組合來表示。

熟習此項技術者應進一步明白，配合本文所發表之具體實施例說明的各種圖解邏輯方塊、模組、電路及演算法步驟可實施為電子硬體、電腦軟體或其組合。為了清楚解說硬體與軟體的互換性，前文中已就功能而論作廣泛說明各種圖解的組件、區塊、模組、電路及步驟。視特定應用及影響整個系統的設計限制條件而定，將功能實施成硬體或軟體。熟悉本技藝者可以用每種特別應用的不同方法來實施所述的功能，但這種實施決定不能視為背離本發明之範圍

可使用一般用途處理器、數位信號處理器 (DSP)、專用積體電路 (ASIC)、場可程式規劃閘極陣列 (FPGA) 或其他可程式規劃邏輯裝置 (PLD)、離散閘極或電晶體邏輯、離散硬體組件或其任何的組合以執行本文所說明的功能，以實施或執行配合本文所發表之具體實施例說明的各種圖

解邏輯方塊、模組及電路。一般用途處理器可能是微處理器，但是在替代方案中，處理器可能是任何傳統處理器、控制器、微控制器或狀態機器。處理器可實施為電腦裝置的組合，例如 DSP 和微處理器的組合、複數個微處理器、連接 DSP 核心的一個或一個以上微處理器或任何其他此類的組態。

配合本文中揭示之具體實施例中說明的方法或演算法步驟可直接用硬體、處理器執行的軟體模組或軟硬體組合具體化。軟體模組可駐存於RAM記憶體、快閃記憶體、ROM記憶體、EPROM記憶體、EEPROM記憶體、暫存器、硬碟、可抽取磁碟、CD-ROM、或此技藝中所熟知之任何其他形式的儲存媒體中。一種示範性儲存媒體係耦合處理器，以致於處理器可自儲存媒體中讀取資訊，以及寫入資訊到儲存媒體。在替代方案中，儲存媒體可被整合至處理器中。處理器和儲存媒體可駐存在 ASIC 中。該ASIC可存在於一使用者終端機中。在替代方案中，處理器和儲存媒體可當作散離組件駐存在使用者終端機中。

前文中提供所揭示具體實施例的說明，讓熟習此項技術者可運用或利用本發明。熟習此項技術者應明白這些具體實施例的各種修改，並且本文中定義的一般原理可適用於其他具體實施例，而不會脫離本發明的精神或範疇。因此，本發明不受限於本文中提出的具體實施例，而是符合與本文中所說明的原理及新穎功能一致的最廣泛的範疇。

【圖式簡單說明】

圖1係一通信系統其包括一高資料率或HDR類型網路及一無線區域網路(WLAN)。

圖2係在一通信系統內鑑認程序之時序圖。

圖3係在一通信系統內一鑑認程序之時序圖。

圖4及5係存取請求訊息格式。

圖6係一無線裝置其包括功能性以產生一主控會期金鑰(MSK)。

【圖式代表符號說明】

102	行動台
104	無線區域網路
106	高資料率
108,112	鑑認授權說明
110	存取點
602	接收電路
604	發送電路
606	中央處理器
608	鑑認程序
610	MSK產生

伍、中文發明摘要：

一種產生一主控會期金鑰(MSK)之通信系統，該MSK係用於存取不提供通信流量加密之系統實體。本方伺服器和使用者兩者均產生相同MSK。該MSK係用以產生通信流量之加密金鑰。於一項實施例中，使用一雜湊函數及請求者特定之資訊來產生該MSK。本方伺服器根據一存取請求訊息內所含之資訊來決定產生MSK之需求。一旦產生，即將該MSK提供給系統實體，使該實體能夠加密通信流量。

陸、英文發明摘要：

A communication system generates a Master Session Key (MSK) for accesses to a system entity that does not provide encryption to traffic. Both the home server and the user generate the same MSK. The MSK is used to generate encryption keys for traffic. In one embodiment the MSK is generated using a hashing function and information specific to the requestor. The home server determines the need to generate the MSK based on information contained in an access request message. Once generated, the MSK is provided to the system entity to enable the entity to encrypt communications.

拾、申請專利範圍：

1. 一種在一通信系統內之金鑰產生方法，包括：

鑑認一無線區域網路(WLAN)之存取；

產生該存取之一主控會期金鑰(MSK)；及

發送一包含該MSK之存取接受訊息。

2. 如申請專利範圍第1項之方法，其中鑑認包括：

接收一使用者識別；

決定一詢問值；及

決定共用祕密，

以及其中產生一MSK包括：

雜湊處理該使用者識別、該詢問值及該共用祕密。

3. 如申請專利範圍第1項之方法，其中鑑認包括：

接收一使用者識別；

決定一詢問值；及

決定一亂數值，

以及其中產生一MSK包括：

雜湊處理該使用者識別、該詢問值及該亂數。

4. 如申請專利範圍第2項或第3項之方法，其中接收使用者識別包括接收一網路存取識別碼(NAI)。

5. 一種在一通信系統內之金鑰產生方法，其包括：

請求鑑認一無線區域網路(WLAN)之存取；

接收一包含該存取之一主控會期金鑰(MSK)的存取接受訊息；及

按照該MSK來產生至少一加密金鑰，其中該至少一加密金鑰係用來加密該存取之通信流量。

6. 一種在一通信系統內之金鑰產生裝置，包括：

用於鑑認一無線區域網路(WLAN)之存取之構件；

用於產生存取之一主控會期金鑰(MSK)之構件；及

用於從該MSK決定一加密金鑰之構件。

7. 一種在一通信系統內之金鑰產生裝置，包括：

用於請求鑑認存取一無線區域網路(WLAN)之存取的構件；

用於接收一包含該存取之主控會期金鑰(MSK)之存取接受訊息的構件；及

用於按照該MSK來產生至少一加密金鑰之構件，其中該至少一加密金鑰係用來加密該存取之通信流量。

8. 一種裝置，包括：

一處理單元；

一鑑認程序單元，其被耦合至該處理單元，並且被調節成請求鑑認一系統之存取，及被調節成計算一鑑認詢問之回應；及

一主控會期金鑰(MSK)產生單元，其被耦合至該處理單元，並且被調節成產生一MSK；

其中該MSK係用於產生至少一加密金鑰，以加密該存取之通信流量。

9. 如申請專利範圍第8項之裝置，其中使用一裝置識別碼、一共用祕密及該詢問來產生該MSK。

10. 如申請專利範圍第8項之裝置，其中使用一裝置識別碼、一共用祕密及一亂數來產生該MSK。

11. 如申請專利範圍第9項或第10項之裝置，其中該裝置識別

碼係一網路存取識別碼(NAI)。

12. 一種用在一通信系統內之方法，包括：

接收一存取通信系統之存取請求訊息，該存取請求訊息具有第一欄位；

決定該第一欄位之狀態；及

若該狀態係一第一值，則產生該存取的一主控會期金鑰(MSK)。

13. 如申請專利範圍第12項之方法，進一步包括：

發送一存取接受訊息，其中：

若該狀態係為該第一值，則存取接受訊息包括該MSK。

14. 如申請專利範圍第12項或第13項之方法，其中該方法進一步包括：

鑑認該存取。

15. 如申請專利範圍第14項之方法，其中鑑認該存取包括：

接收一使用者識別；

決定一詢問值；及

決定共用祕密，

以及其中產生MSK包括：

雜湊處理該使用者識別、該詢問值及該共用祕密。

16. 如申請專利範圍第14項之方法，其中鑑認該存取包括：

接收一使用者識別；

決定一詢問值；及

決定一亂數值，

以及其中產生一MSK包括：

雜湊處理該使用者識別、該詢問值及該亂數值。

17. 如申請專利範圍第12項至第16項中任一項之方法，其中該第一欄位相對應於一用於指示存取不支援加密屬性之通信系統實體的屬性，或相對應於一用於指示該存取請求訊息之起始的屬性。

18. 如申請專利範圍第17項之方法，其中該實體係一無線區域網路(WLAN)。

19. 一種在一通信系統內之基礎元件，包括：

用於接收存取該通信系統之一存取請求訊息的構件，該存取請求訊息具有一第一欄位；

用於決定該第一欄位狀態的構件；及

用於若該狀態係一第一值則產生該存取之一主控會期金鑰(MSK)的構件。

20. 一種通信系統之存取請求訊息格式，包括：

一類型欄位，用於識別存取該通信系統之一屬性資訊類型；及

該屬性資訊的一值欄位，該值欄位包括：

一第二類型欄位，用於識別該存取之一次屬性資訊類型；及

該次屬性資訊的一第二值欄位。

21. 如申請專利範圍第20項之存取請求訊息格式，其中該次屬性資訊係一主控會期金鑰(MSK)產生指令。

拾壹、圖式：

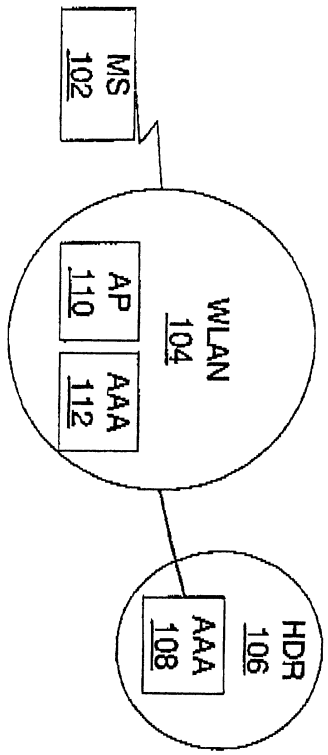
MS
102
WLAN
104
AP
110
AAA
112
HDR
106
AAA
108

圖1

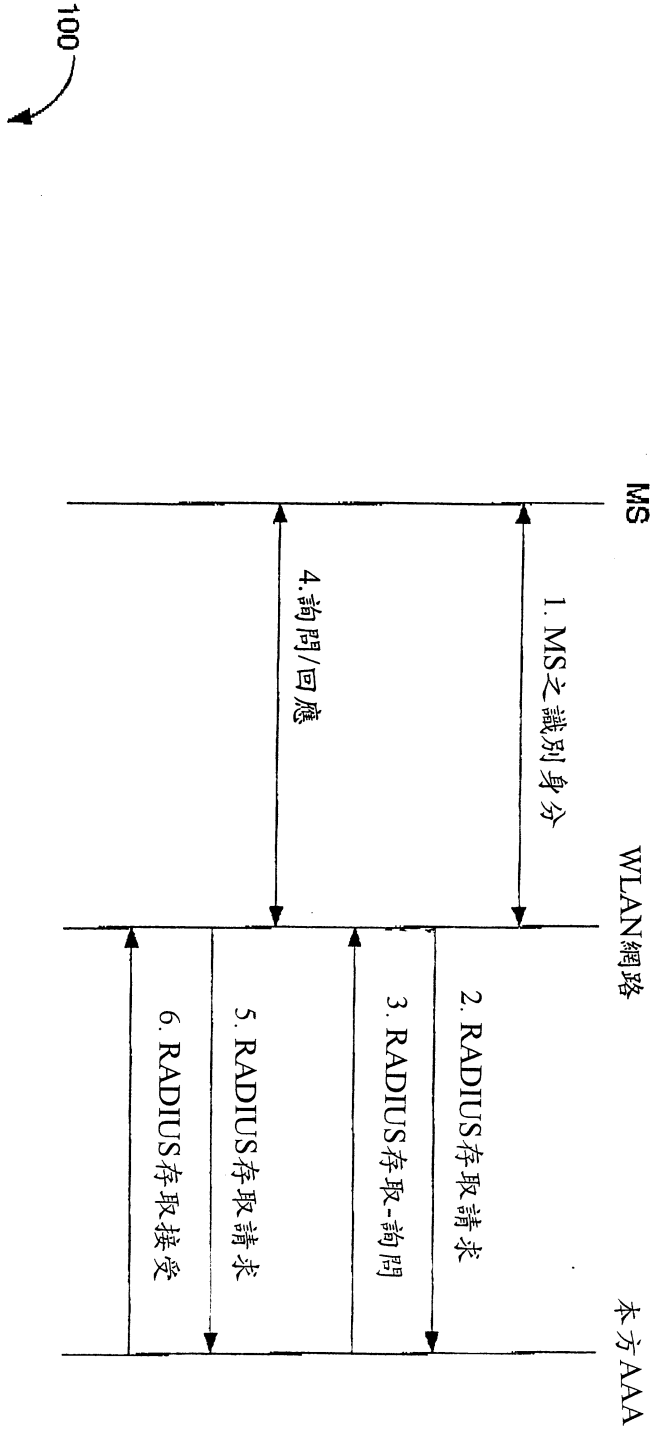
100
MS
WLAN網路
本方AAA
1. MS之識別身分
2. RADIUS存取請求
3. RADIUS存取-詢問
4.詢問/回應
5. RADIUS存取請求
6. RADIUS存取接受

圖2

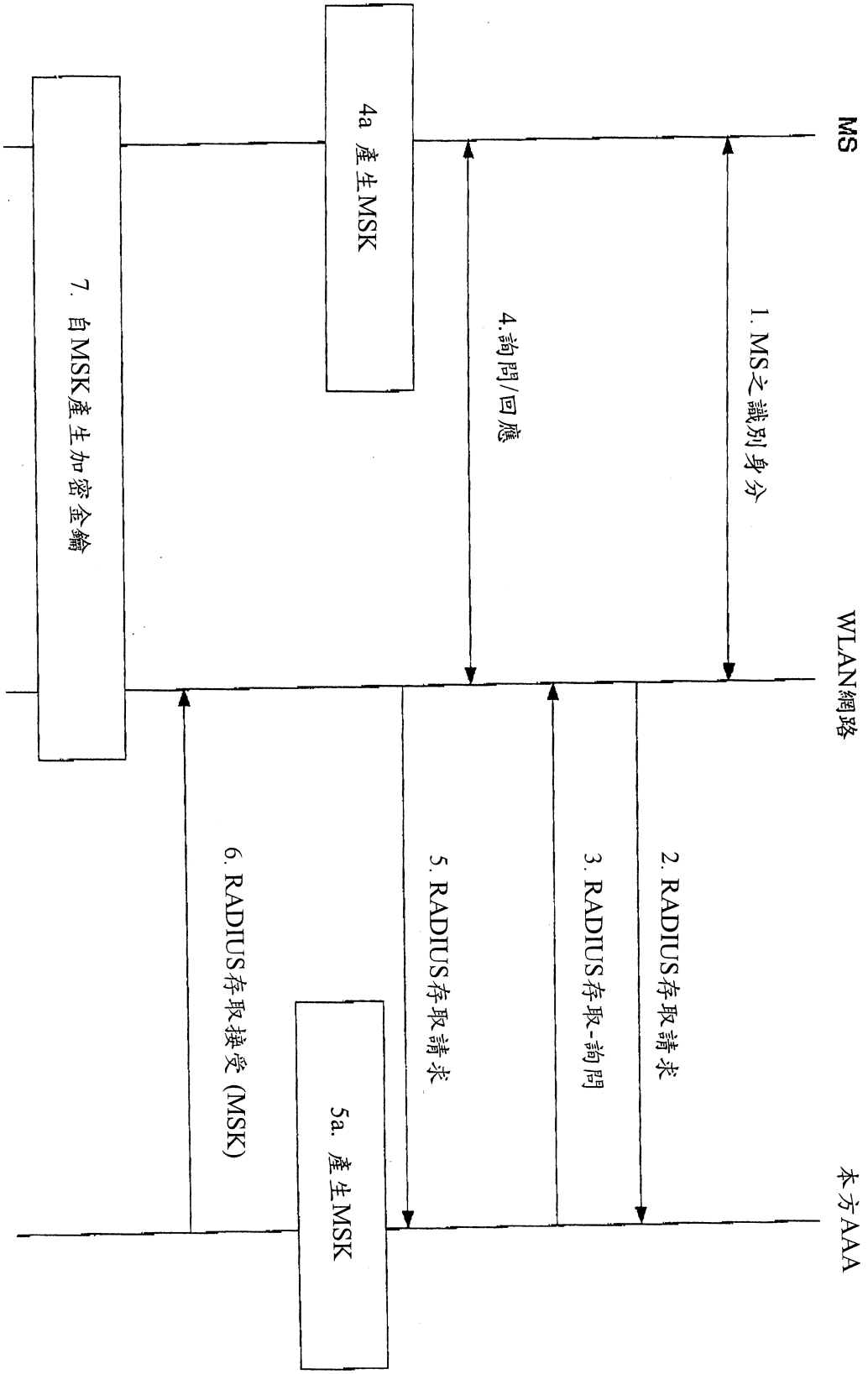
MS
WLAN網路
本方AAA
1. MS之識別身分
2. RADIUS存取請求
3. RADIUS存取-詢問
4. 詢問/回應
4a 產生MSK
5. RADIUS存取請求
5a. 產生MSK
6. RADIUS存取接受 (MSK)
7. 自MSK產生加密金鑰

圖3

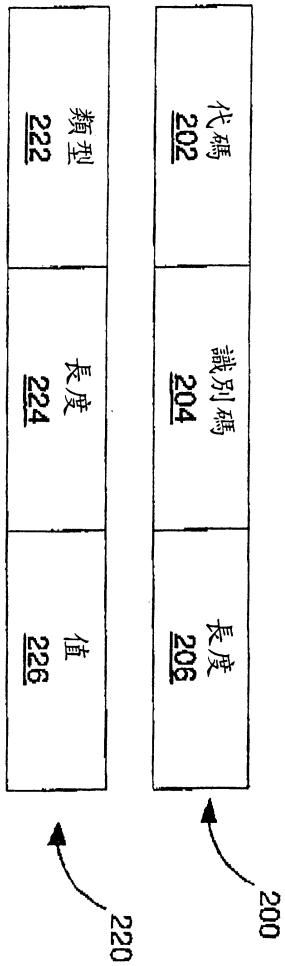
代碼
202
識別碼
204
長度
206
200
類型
222
長度
224
值
226
220

圖4

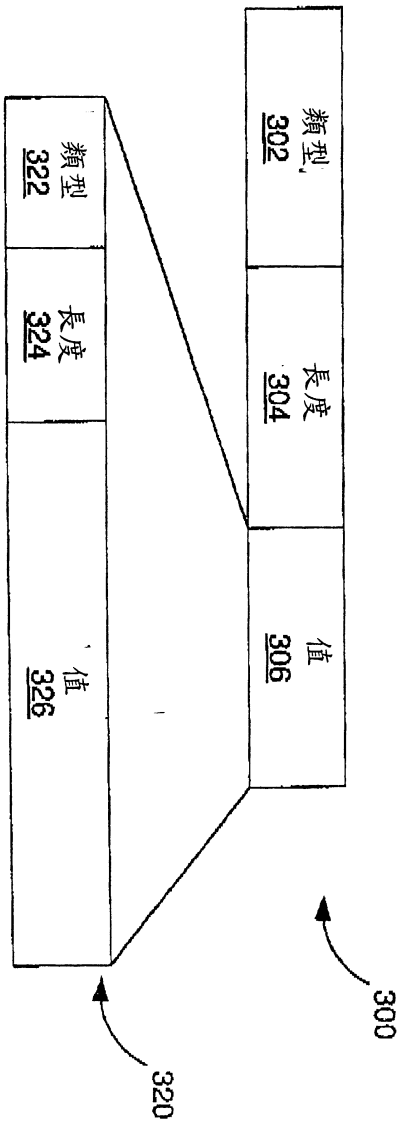
類型
302
長度
304
值
306
300
類型
322
長度
324
值
326
320

圖5

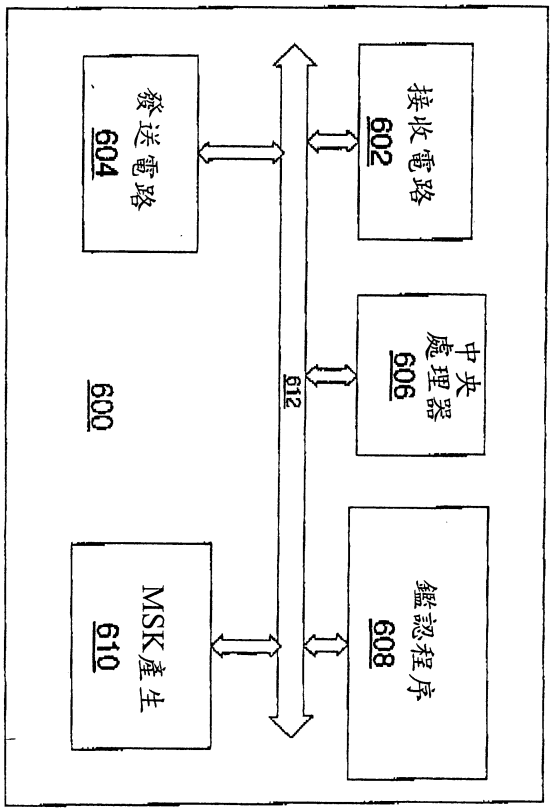

圖6

柒、指定代表圖：

(一)本案指定代表圖為：第（ 3 ）圖。

(二)本代表圖之元件代表符號簡單說明：

(無元件代表符號)

捌、本案若有化學式時，請揭示最能顯示發明特徵的化學式：