(19)中華民國智慧財產局
(12)發明說明書公開本 (11)公開編號：TW 201135508 A1
(43)公開日： 中華民國 100 (2011) 年 10 月 16 日

(21)申請案號：099114865 (22)申請日： 中華民國 99 (2010) 年 05 月 10 日
(51)Int. Cl.： *G06F21/00 (2006.01)* *H04L9/00 (2006.01)*
(30)優先權：2009/06/11 美國 12/483,095
(71)申請人：微軟公司 (美國) MICROSOFT CORPORATION (US)
美國
(72)發明人：賽門丹尼爾 R SIMON, DANIEL R. (CA) ；斯溫德布萊恩 D SWANDER, BRIAN D. (US) ；梅尼斯帕斯寇 MENEZES, PASCAL (CA) ；蒙特內格諾蓋貝瑞兒 E MONTENEGRO, GABRIEL E. (US)
(74)代理人：蔡坤財；李世章
申請實體審查：無 申請專利範圍項數：20 項 圖式數：9 共 93 頁

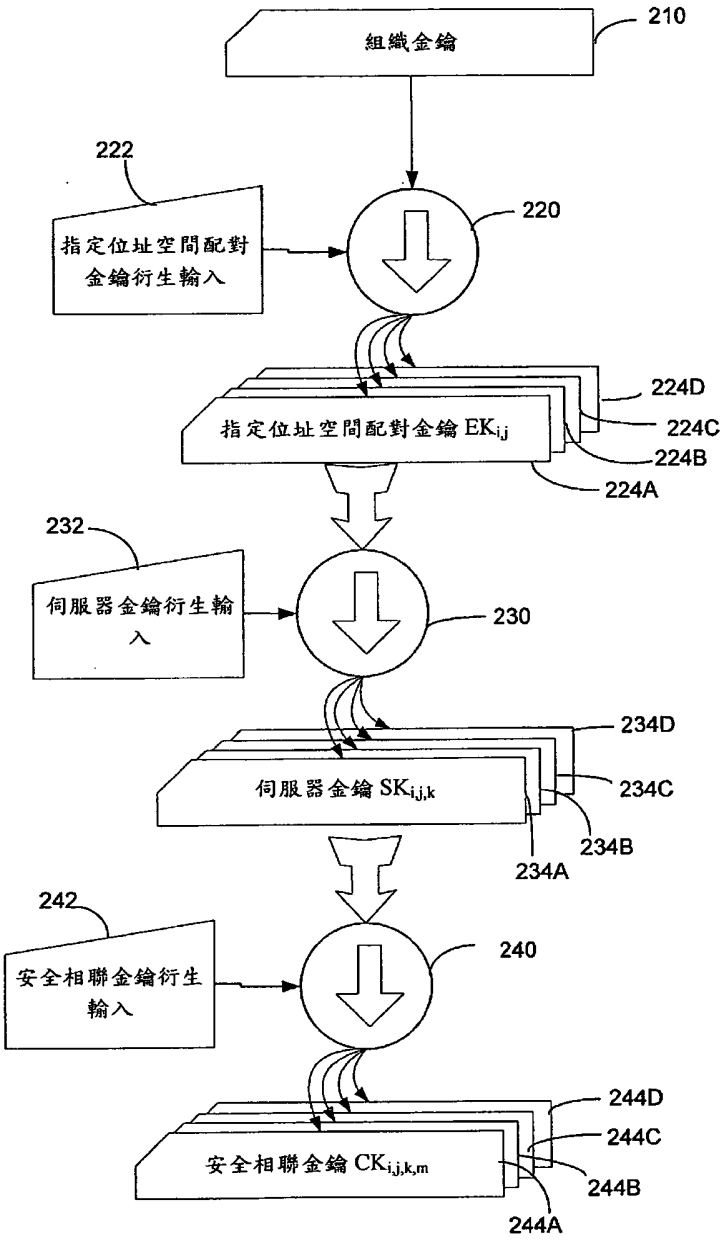
(54)名稱

在安全網路指定位址空間中的鑰管理

KEY MANAGEMENT IN SECURE NETWORK ENCLAVES

(57)摘要

本發明揭示一種用於電腦系統內的階層金鑰產生與散佈機制，其中裝置被組織成為安全指定位址空間。該機制可讓網路存取為了每一裝置而被裁剪，以逼近最小權限需求。在階層的最低等級上，使用金鑰形成裝置之間的安全相聯。每一階層等級上的金鑰都從較高階層等級上的金鑰以及金鑰衍生資訊來產生。金鑰衍生資訊可迅速從裝置識別碼或內含訊息來確定，支援密碼函數的硬體卸載。因為可根據參與安全相聯的主機所在之指定位址空間來產生金鑰，該系統包含一機制，讓裝置可發現其所在的指定位址空間。



210：組織金鑰

220：擬亂函數

222：指定位址空間配對衍生輸入

224A：配對金鑰

224B：配對金鑰

224C：配對金鑰

224D：配對金鑰

230：擬亂密碼函數

232：伺服器金鑰衍生輸入

234A：伺服器金鑰

234B：伺服器金鑰

234C：伺服器金鑰

234D：伺服器金鑰

240：擬亂密碼函數

242：安全相聯金鑰衍生輸入

244A：金鑰

244B：金鑰

244C：金鑰

244D：金鑰

(19)中華民國智慧財產局
(12)發明說明書公開本 (11)公開編號：TW 201135508 A1
(43)公開日： 中華民國 100 (2011) 年 10 月 16 日

(21)申請案號：099114865 (22)申請日： 中華民國 99 (2010) 年 05 月 10 日
(51)Int. Cl.： *G06F21/00 (2006.01)* *H04L9/00 (2006.01)*
(30)優先權：2009/06/11 美國 12/483,095
(71)申請人：微軟公司 (美國) MICROSOFT CORPORATION (US)
美國
(72)發明人：賽門丹尼爾 R SIMON, DANIEL R. (CA) ；斯溫德布萊恩 D SWANDER, BRIAN D. (US) ；梅尼斯帕斯寇 MENEZES, PASCAL (CA) ；蒙特內格諾蓋貝瑞兒 E MONTENEGRO, GABRIEL E. (US)
(74)代理人：蔡坤財；李世章
申請實體審查：無 申請專利範圍項數：20 項 圖式數：9 共 93 頁

(54)名稱

在安全網路指定位址空間中的鑰管理

KEY MANAGEMENT IN SECURE NETWORK ENCLAVES

(57)摘要

本發明揭示一種用於電腦系統內的階層金鑰產生與散佈機制，其中裝置被組織成為安全指定位址空間。該機制可讓網路存取為了每一裝置而被裁剪，以逼近最小權限需求。在階層的最低等級上，使用金鑰形成裝置之間的安全相聯。每一階層等級上的金鑰都從較高階層等級上的金鑰以及金鑰衍生資訊來產生。金鑰衍生資訊可迅速從裝置識別碼或內含訊息來確定，支援密碼函數的硬體卸載。因為可根據參與安全相聯的主機所在之指定位址空間來產生金鑰，該系統包含一機制，讓裝置可發現其所在的指定位址空間。

六、發明說明：

【發明所屬之技術領域】

本發明係關於安全網路指定位址空間中的金鑰管理。

【先前技術】

對於電腦系統來說，安全越來越重要。企業通常會保存許多種資訊，像是財務資訊、機密商業資訊或有關客戶與員工的個人資訊。由於許多重要的業務因素，一般至少某些個人可透過企業電腦系統取得此資訊。不過這些資訊若遭到未獲授權者存取並誤用，可能對企業、員工或客戶造成嚴重傷害。

為了保護企業電腦系統內的資訊，已經提出許多種安全技術，其中一種方式就是稱為 IPsec 的安全網路通訊協定。在 IPsec 內，兩個即將彼此通訊的主機裝置會形成「安全相聯」，此安全相聯係基於主機之間使用金鑰交換協定所交換的一或多個金鑰，然後兩部主機使用該金鑰加密或驗證在其間傳遞的訊息，此係依所需要的安全等級而定。

在網路環境中使用 IPsec 的缺點在於，用於加密與解密或簽署與驗證訊息的加密處理，會不被情願地增加主機裝置中央處理器的負載。為了減少處理器的負擔，已

[S]

經研發出網路界面晶片組來卸除這些密碼函數。這種晶片組可替每一主動安全相聯來儲存金鑰，為此內含網路界面的一部電腦作為主機。當運用特定安全相聯將資訊傳遞至網路界面進行通訊時，該晶片組可運用適當金鑰加密或簽署該資訊。同樣，當接收關聯於一安全相聯的封包時，該晶片組可驗證或解密封包內的資訊，並且將這種處理之結果傳遞至一網路堆疊，進行進一步處理。

雖然這種處理在某些案例中有用，不過現有晶片組受到可同時維持的主動安全相聯數量之限制。例如：大型企業內的伺服器可以維護 10,000 筆層級的安全相聯，但是晶片組能維持的資訊只能支援 1,000 筆層級的安全相聯。

為了擴充網路界面晶片組所能支援的安全相聯數量，目前已經提議形成網路「指定位址空間」。根據此提議，每一指定位址空間都可擁有自己的金鑰，其用於以可預期的方式而為牽涉該指定位址空間內的裝置的「安全相聯」產生金鑰。該指定位址空間金鑰用來以可預期的方式產生金鑰給該指定位址空間內之伺服器，然後伺服器從這些金鑰當中產生用於它們所形成之安全相聯的金鑰。在裝置傳送運用安全相聯金鑰簽署或加密的封包時，該裝置會在該封包內附加識別該金鑰如何衍生的資訊。存取該封包的其他裝置可即時產生適當金鑰，用於

該封包的加密處理。因為可從該指定位址空間金鑰產生對應任何數量之安全相聯的安全相聯金鑰，所以晶片組可存取大量安全相聯，並不需要大量儲存空間。作為該安全相聯之主機的裝置，或用於處理在兩主機之間傳遞之封包的中間裝置，只要該中間裝置存取適當的指定位址空間金鑰，都可使用此自動金鑰產生方式。

【發明內容】

為了提供用於安全網路指定位址空間內之適當金鑰，所以用階層方式產生金鑰。在此定義用於建立指定位址空間的安全相聯跨越配對之配對指定位址空間金鑰，該配對指定位址空間金鑰可用來產生該配對內指定位址空間中伺服器的金鑰，這些伺服器金鑰接著可基於伺服器與用戶端裝置所在指定位址空間，用於建立與用戶端裝置相關聯的安全相聯。藉由將識別主機指定位址空間的資訊，以及用來基於配對指定位址空間金鑰產生安全相聯參數的其他資訊，併入封包內，則存取封包並且存取適當金鑰的裝置，可產生用於處理該封包的安全相聯參數。

該金鑰的階層性質可用來為裝置裁剪存取等級，利用提供較高階層等級上的金鑰，可將較高權限賦予具有較高信賴等級的裝置。相較之下，其他裝置只能存取用於[S]

在其自身指定位址空間內的通訊之金鑰，或存取用於在其自身指定位址空間與特定數量其他指定位置空間之間的通訊之金鑰。

該階層金鑰產生方式允許受信賴的中間裝置存取訊息流量，而存取限制則可根據中間裝置的角色與信賴程度來設定。連接在連接兩指定位址空間或少量指定位址空間的網路路徑內之受信賴中間裝置，可具備只存取這些指定位址空間的配對指定位址空間金鑰之權限，允許該中間裝置監控或控制出入這些指定位址空間之網路流量。具備所有網路流量存取權限的其他中間裝置，可被賦予所有指定位址空間的金鑰，或產生該等指定位址空間金鑰的較高等級金鑰，像是組織金鑰。

根據該等金鑰與其他資訊，中間裝置可使用該等這些金鑰來產生安全相聯的參數。這種其他資訊可包含於在安全相聯端點之間通訊的封包內。在某些具體實施例內，中間裝置可監控形成一安全相聯時所交換的封包，並採取行動，像是動態獲得產生安全相聯金鑰的一金鑰。若中間裝置不支援在此金鑰階層下的金鑰衍生，因而無法產生安全相聯金鑰，它可向形成該安全相聯的伺服器發出缺乏能力的信號，然後該伺服器可進行直接金鑰交換來提供安全相聯金鑰給中間裝置。

在使用安全相聯傳送的訊息首先繞送通過不支援安全

指定位址空間處理的中間裝置(在形成安全相聯之後)之案例中，該中間裝置可通知端點重新建立安全相聯，讓中間裝置有機會直接存取用來處理使用安全相聯所傳送封包之資訊。

上述為本發明非用於限制的總結，本發明由申請專利範圍所界定。

【實施方式】

本發明者已經清楚並瞭解，透過改良的金鑰管理方法可改善安全指定位址空間以及卸除密碼函數來支援安全指定位址空間之硬體。這些金鑰可被產生並分散，以允許簡易網路存取。另外，金鑰管理系統應該可限制每一裝置接收的存取。階層金鑰管理法可用來支援產生金鑰，提供不同的存取等級給不同裝置群組之間的通訊。階層金鑰管理法也可簡化將金鑰散佈至企業電腦系統的機制，如此安全指定位址空間內的裝置可適當處理網路流量。

在某些具體實施例內，整體組織金鑰形成金鑰階層的最頂級。從此組織金鑰中，產生配對指定位址空間金鑰給組織所操作的網路電腦系統內每對指定位址空間(包含與自身配對的每一指定位址空間)。每一配對指定位址空間金鑰可用來產生下一較低階層上的金鑰。 [S]

在此處描述的示範具體實施例中，位於安全相聯相對末端上的主機裝置可稱為「伺服器」和「用戶端」。伺服器產生安全相聯金鑰給形成為用戶端每一安全相聯。為了產生安全相聯金鑰，伺服器可具有伺服器金鑰，此金鑰可從用於其指定位址空間以及用戶端所在指定位址空間的配對金鑰當中取得。

在描述的具體實施例內，不論階層的等級，都將金鑰看待成安全資訊。而用來從較高階層等級金鑰中產生較低階層等級金鑰的金鑰衍生資訊，則不需看待成安全資訊。該金鑰衍生資訊可在傳送通過網路的訊息內，以不安全或相對不安全的方式來通訊。因此，許多網路裝置具備金鑰衍生資訊的存取權限。在任何等級上，具有階層內用來產生一特定安全相聯金鑰之金鑰的存取權限的裝置，因此可存取金鑰衍生資訊並產生安全相聯金鑰。

為了減少每一裝置必須保有的安全相聯金鑰數量，使用較高等級金鑰與金鑰衍生資訊來動態產生該階層內較低階層等級上的金鑰。例如：指定位址空間內的伺服器可被提供所有配對伺服器金鑰，為此該指定位址空間為相關配對內一個指定位址空間。在辨別要形成安全相聯的用戶端之指定位址空間時，可從這些金鑰之一產生特定安全相聯金鑰。

金鑰提供也可動態發生，例如：裝置可從金鑰伺服器

下載金鑰。動態提供可即時發生，回應使用金鑰執行封包上密碼函數之需求。另外，需要時可事先提供某些或全部金鑰。事先提供時，可偶爾重新提供或重新產生金鑰。重新提供可定期執行，像是每天，或可回應事件而執行，像是裝置進入或離開指定位址空間。

不論何時提供金鑰，金鑰可從頂端等級組織金鑰開始散佈到整個組織。不論業界內已知或稍後研發，合適的安全措施可用來限制該階層內不同等級的金鑰分佈，只給那些獲得授權而能存取資訊的裝置，其中該資訊使用直接或間接從該金鑰衍生的金鑰來加密。

可使用任何合適的方式決定授權裝置。在某些具體實施例內，網路管理員利用產生存取控制清單來建立授權的裝置，以證書或其他授權訊標提供給特定裝置。在某些具體實施例內，可使用企業電腦系統內已經有的安全系統來建立授權的裝置，例如：許多企業電腦系統運用Active Directory™網路管理系統來驗證裝置。這種系統可用來控制哪個裝置可存取哪個金鑰，並且提供安全機制來將金鑰通訊給這些裝置。

不論如何限制金鑰的散佈，利用適當限制不同階層等級上金鑰的散佈，可設定存取等級讓每一裝置只具備需要的存取等級，例如：某些裝置只能存取特定伺服器與特定用戶端之間的封包，其他裝置可存取特定伺服器與

任何指定位址空間內任何裝置之間的通訊。還有其他裝置可存取一個指定位址空間內任何裝置與任何指定位址空間內任何裝置之間的封包。還有其他裝置可存取送過電腦系統的任何封包。

不過，吾人應該瞭解，並非所有具體實施例內都需要呈現所有階層等級，例如：在某些具體實施例內，並非提供單一頂級組織金鑰，而是一開始就提供指定位址空間金鑰給每一指定位址空間，如此可產生配對的指定位址空間金鑰。另外，管理員可直接提供配對的指定位址空間金鑰給裝置。作為另一範例，雖然已經描述伺服器金鑰，可將配對指定位址空間金鑰的存取權限提供給伺服器，此權限可用來直接產生安全相聯金鑰，而不需要產生伺服器金鑰這個中間步驟。某些具體實施例內同樣可運用階層金鑰的額外等級。例如電腦系統可分成任何數量的次指定位址空間等級，其中每一次指定位址空間都擁有自己的金鑰，以及與其他次指定位址空間的配對金鑰。

階層金鑰管理法的用途之一為允許中間裝置存取即時產生安全相聯金鑰時所需之指定位置空間金鑰。藉由將與這些指定位址空間相關聯的配對指定位置空間金鑰提供給中間裝置，位於兩指定位置空間之間網路內的該中間裝置可獲授權來監控這兩指定位置空間之間的網路流 [S]

量。

針對任何原因，中間裝置可被提供來存取這種訊息，例如：中間裝置可執行防毒軟體，一旦訊息內容的存取被提供時，確保訊息未受病毒感染。中間裝置可根據訊息內容執行任何其他合適的監控功能。中間裝置也可執行其他功能，像是操縱訊息，或採取本文所述的控制動作。

不論中間裝置的特定功能為何，其可擷取傳送過網路的訊息內之金鑰衍生資訊。該金鑰衍生資訊結合提供給中間裝置的金鑰，可用來衍生通過中間裝置的網路流量之安全相聯金鑰。

階層金鑰也幫助硬體卸除網路封包的加密處理來支援這些功能。不論是位於安全相聯內的主機內或位於監控以安全相聯傳送的網路流量的中間裝置內，網路界面硬體都可動態產生安全相聯金鑰作為卸載處理的一部分。因此，甚至對具有較高等級存取權限的裝置而言，硬體內必須維持的金鑰數量仍為可管理的。

不過在某些案例中，電腦系統可包含支援或不支援這種金鑰衍生的中間裝置。該金鑰管理系統可提供一項機制給中間裝置，在其無法根據可用資訊產生金鑰時，獲得存取安全相聯金鑰所需的資訊。例如：可執行直接金鑰交換。中間裝置可通知當成伺服器的主機，告知其不

支援安全指定位址空間，而可觸發伺服器與中間裝置進行直接金鑰交換。若參與安全相聯的主機之一不支援在安全相聯下傳送的封包內包含金鑰衍生資訊，則可執行類似的金鑰交換。

如上述，金鑰管理係建基於與指定位置空間相關聯的裝置。在某些具體實施例內，指定位置空間為靜態並且事先定義。在這種具體實施例內，裝置可根據網路拓撲或其他因素指派至指定位置空間。裝置然後可獲得其屬於該指定位置空間的指示。

不過在其他實例中，網路可經重新組態或可支援行動裝置。在這種具體實施例內，可能無法事先指派特定裝置至指定位址空間。另外，在某些實例中，指派所有裝置至指定位址空間可能有困難或負擔太大。因此在某些具體實施例內，金鑰管理系統可包含一種指定位址空間發現協定，其允許裝置發現其指定位址空間。

可使用任何合適的指定位址空間發現協定。舉例來說，可指派網路裝置子集至指定位址空間，並可將其指定位址空間狀態通訊至其他裝置，如此其他裝置可基於對已經被指派給指定位址空間的裝置之連接，來推論自己的指定位址空間成員資格。

在某些具體實施例內，可能成為中間裝置並且牽涉到在其他網路裝置之間繞送封包的裝置，可指派給指定位[S]

址空間。這種裝置的子集足夠小，並且這些裝置的位置變動不會太頻繁，所以只需要相當小的負擔就可將該裝置所在指定位址空間的指示提供給每一這種裝置。

封包通過形成安全相聯的兩部主機時，每一這種中間裝置都可新增標記至該封包，指示一個指定位址空間。接收這種封包的主機可使用該標記來決定自己的指定位址空間。在某些具體實施例內，該標記可指示兩主機或之一的指定位址空間。中間裝置可獲得這種資訊，例如從內含系統內主機的指定位址空間指派的中間裝置可存取之資料庫。

在其他具體實施例內，該標記可包含允許主機推論其指定位址空間的資訊，例如：每一中間裝置都可附加識別所擁有指定位址空間的資訊。該中間裝置可接著新增標記，建立有順序的標記鍊。接收這種封包的任何主機都可分析標記鍊，決定標記鍊開頭與結尾上的指定位址空間，這可指示形成安全相聯的主機之指定位址空間。

主機可從此資訊決定自己的指定位址空間。單一封包就足夠讓主機決定自己的指定位址空間，雖然在某些實例中，網路內封包繞送的變化可在相同兩主機之間通訊的不同封包內產生不同的標記鍊。若有不一致，裝置可從多個封包獲得資訊，並且基於最常指示的指定位址空間識別自己的指定位址空間，或使用任何合適的方式來 S1

解決歧義。

伺服器可類似地使用指定位址空間標記鍊來決定其中用戶端所在的指定位址空間，例如，此資訊可用於選擇適當的配對金鑰，來產生伺服器金鑰，接著將用於產生安全相聯金鑰。

任何合適的裝置可都放置標記，識別封包上的指定位址空間。在某些具體實施例內，像是路由器與閘道器這類中間裝置可經組態來放置這種標記，雖然任何合適的裝置都可用來放置指定位址空間標記。

根據本發明具體實施例的金鑰管理系統可運用在任何合適的電腦系統內，舉例來說，金鑰管理系統可併入企業電腦系統 100 (第 1A 圖)，像是大公司內可發現的系統。電腦系統 100 包含多個電腦裝置，分割至指定位址空間 110A、110B、110C 和 110D 內。網路裝置可用任何合適方式分組至指定位址空間。在例示的具體實施例內，一般基於網路拓撲形成指定位址空間，以使可透過一路由器或其他閘道裝置存取的裝置，一般分組在相同的指定位址空間內。然而，任何用於將裝置分割至指定位址空間的合適準則皆可使用。

第 1A 圖為電腦系統的簡單例示。其中顯示三種裝置：伺服器、用戶端與多埠裝置。其中例示像是伺服器 120A、120B 和 120C 這些伺服器。伺服器可為具有相當[S]

大量電腦資源(像是處理功率或電腦儲存媒體)的計算裝置。這些裝置可相對固定，安裝在機架或其他靜止結構上。這種裝置可作為檔案伺服器、列印伺服器、資料庫伺服器、網路伺服器或執行企業內其他功能。不過，伺服器可為供應資訊給其他裝置的任何計算裝置。因此，本發明並不受限於伺服器處理能力的性質。有時桌上型電腦、膝上型電腦和小型電子裝置都可作為伺服器。

第 1A 圖也例示電腦系統 100 內多個用戶端裝置。為了簡化，例示三個用戶端裝置，就是用戶端裝置 130、132 和 134。在此範例中，用戶端裝置例示為桌上型電腦。不過，用戶端裝置可為接收來自伺服器資訊的任何裝置。如此除了桌上型電腦以外，用戶端裝置可為膝上型電腦或其他可攜式計算裝置。依據裝置所執行的特定操作，具備相當大量處理資源的裝置也可成為用戶端。

除了伺服器和用戶端以外，電腦系統 100 可包含一或多個多埠裝置，像是多埠裝置 136。一般來說，網路內的多埠裝置執行繞送、交換或其他流量處理功能，幫助定址至特定裝置的封包到達所要的目的地。多埠裝置的範例包含路由器和交換器，以及負載平衡器、WAN 最佳化器以及侵入偵測/預防系統。

除了多埠裝置 136，圖中顯示電腦系統 100 包含作為指定位址空間之間中間裝置的多埠裝置。在第 1A 圖內，[S]

顯示中間裝置 140A、140B、140C 和 140D。每一這些中間裝置都可作為閘道器，如此至或來自指定位址空間內裝置的訊息可通過，例如：中間裝置 140A 可作為指定位址空間 110A 內裝置的閘道器。中間裝置 140B 可作為閘道器，如此至或來自指定位址空間 110B 內裝置的訊息可通過。類似地，中間裝置 140C 可作為指定位址空間 110C 內裝置的閘道器，並且中間裝置 140D 可作為指定位址空間 110D 內裝置的閘道器。

不過，並未要求中間裝置須為指定位址空間的閘道器。中間裝置可用將來自一個指定位址空間的訊息轉送至另一個之方式，來連接在網路內。例如：中間裝置 140C 可接收任何指定位址空間 110A、110B、110C 或 110D 內產生的訊息，並且基於訊息內的目的地位址，繞送訊息至任何其他指定位址空間。

吾人應該瞭解，第 1A 圖只為其中可運用本發明的一種企業電腦系統可能實施之簡略圖。為了簡化，第 1A 圖內只例示四個指定位址空間。其實可具有任何合適數量的指定位址空間，並且大企業的電腦系統內可具有四個以上的指定位址空間。

不論指定位址空間的數量，指定位址空間可用任何合適的方式來定義。在某些具體實施例當中，由網路管理員定義指定位址空間。這些指定位址空間可基於網路拓 S1

撲來定義，如此每一指定位址空間由至少一個中間裝置與其他指定位址空間分隔。此外，指定位址空間可定義成只有共用管理控制之下的裝置，才會分組至相同的指定位址空間。在此方式中，適用類似存取控制的裝置可在相同指定位址空間內，如此該指定位址空間內的裝置可共享不包含資訊安全的指定位址空間金鑰。

第 1A 圖例示每一指定位址空間可由不同數量與類型的裝置所形成。為了支援階層金鑰產生與散佈系統，指定位址空間內的某些裝置可具有與金鑰產生或散佈相關聯的特定功能。第 1B 圖顯示指定位址空間的放大圖。第 1B 圖例示指定位址空間可與伺服器相關聯，該等伺服器執行與階層金鑰產生和散佈相關聯之特定功能。

如第 1B 圖內所示，指定位址空間 150 包含伺服器，像是伺服器 170A 和 170B。在操作中，伺服器 170A 和 170B 可形成與用戶端裝置的安全相聯，這兩伺服器都在指定位址空間 150 內以及指定位址空間 150 可透過網路連結的其他指定位址空間內。在第 1B 圖內，用戶端裝置 180、182 和 184 例示在指定位址空間 150 內，並且伺服器 170A 和 170B 可形成與這些用戶端裝置的安全相聯。雖然第 1B 圖內並未明確例示其他指定位址空間內的用戶端裝置，伺服器 170A 和 170B 也可透過中間裝置 192 與其他指定位址空間內的用戶端裝置通訊。 [S]

可使用一或多種加密技術確保伺服器與用戶端之間的通訊安全，這種加密技術可用來加密或提供驗證資訊的機制。不論包含加密技術的目的為何，使用像是加密金鑰這類安全參數可執行加密技術，如業界內所熟知。用於加密時，根據密碼函數，加密金鑰會與要加密的資訊結合。具有加密金鑰者可從加密資訊當中復原原始資訊，但是密碼函數的複雜性使得若沒有金鑰，在實際情況中不可能從加密的資訊當中確定原始資訊。相較之下，驗證可能牽涉到其中資訊搭配金鑰結合來產生簽章的密碼函數。在此情況下，密碼函數相當複雜，使得在實際情況中無加密金鑰之下無法產生簽章。為了驗證已經透過網路通訊的資訊，可在接收資訊時於其上再次執行密碼函數，並且在傳輸時與資訊相關聯的簽章做比較。若資訊已經改變，則產生的簽章不匹配，如此迅速識別已經改變的資訊。

在此處所描述的範例中，描述關於加密的密碼函數。不過，本發明並未要求散佈通過電腦系統的金鑰要用於加密。金鑰可另外或額外用於驗證。在某些具體實施例內，可提供獨立的金鑰用於加密與驗證。因此，雖然此處描述的範例討論單一金鑰用於兩裝置之間形成之每一安全相聯，不過任何數量金鑰都可形成每一安全相聯的一部分。例如：可產生加密金鑰與驗證金鑰，每一這種

金鑰都可根據此處所討論的技術來產生與散佈。再者，可為了資料加密或驗證之外的原因而運用加密金鑰作為密碼函數的一部分。因此，吾人應該瞭解，本發明並不受限於金鑰的任何數量或種類，或以這些金鑰執行的密碼函數。

不論加密金鑰的數量與用途，指定位址空間 150 內每一伺服器都可與一或多個用戶端裝置形成安全相聯。藉由在每一安全相聯主機裝置之間共享安全參數來建立每一安全相聯，其中之安全參數包含加密金鑰或金鑰。安全參數用來在使用安全相聯輸送的資訊上執行密碼函數，該資訊可作為封包傳遞通過網路。舉例來說，封包可內含資訊，該資訊使用產生用於安全相聯的安全參數來加密。

該安全參數可包含避免未授權者存取該資訊的任何資訊。在此處提供的範例中，使用有時稱為安全相聯金鑰的交談金鑰，作為安全參數的範例。安全相聯金鑰是用來將從安全相聯中的一主機傳送至其他處的資訊加密。為了簡化，在此處的範例中，使用相同的安全相聯金鑰將在主機之間雙向傳遞的資訊加密。不過吾人應該瞭解，安全參數可包含在每一主機上用來傳送與接收資訊的多個金鑰。

兩主機之間可用任何合適的方式共享安全參數，包含[S]

使用業界內熟知的技術。舉例來說，已經研發出 IPsec 通訊協定來進行安全通訊。IPsec 支援通過主機之間封包的加密及/或驗證。除了使用安全資訊定義所保護的封包之格式，Ipsec 還包含主機之間初始互動的協定，如此主機可獲得要用來作為安全相聯一部分的安全參數共用集合。這種協定的範例為網際網路金鑰交換協定(Key exchange protocol，「IKE」)以及 AuthIP 協定。根據這些協定，伺服器可產生安全協定金鑰並傳送至用戶端。接著，用戶端與伺服器可使用此金鑰，用於其間傳遞資訊的加密。

在範例具體實施例內，安全相聯金鑰位於金鑰階層的最低等級上。當每一伺服器，像是伺服器 170A 和 170B，形成新的安全相聯時，該伺服器產生安全相聯金鑰。每一伺服器都從伺服器金鑰產生安全相聯金鑰。在此，每一伺服器，像是伺服器 170A 和 170B，可包含一組伺服器金鑰。該伺服器金鑰可為配對金鑰，如此每一伺服器金鑰都可關聯於不同對指定位址空間。因此，伺服器產生安全相聯金鑰時，首先決定用戶端所在的指定位址空間，並且選擇用於指定位址空間配對的適當伺服器金鑰，此配對包含用戶端指定位址空間與伺服器自有的指定位址空間。

每一伺服器都可從指定位址空間金鑰伺服器 160 接收[S1]

其伺服器金鑰。指定位址空間金鑰伺服器 160 可組態成為指定位址空間 150 內每一伺服器產生伺服器金鑰，其中各伺服器係被授權接收這種伺服器金鑰。指定位址空間金鑰伺服器 160 可使用任何合適的機制來識別經授權的伺服器，並且將金鑰通訊至這些授權的伺服器。例如：一旦伺服器 170A 和 170B 驗證了其本身，則 IPsec 協定可用來從指定位址空間金鑰伺服器 160 安全通訊金鑰至伺服器，像是 170A 和 170B。

在例示的具體實施例內，指定位址空間金鑰伺服器 160 從一組配對的指定位址空間金鑰中產生金鑰給伺服器，像是伺服器 170A 和 170B。在例示的具體實施例內，指定位址空間金鑰伺服器 160 可基於從組織金鑰伺服器 148 接收的資訊(內含組織金鑰)，產生配對的指定位址空間金鑰。同樣地，組織金鑰伺服器 148 可提供配對的指定位址空間金鑰給其他指定位址空間內的指定位址空間金鑰伺服器。

第 2A 圖例示金鑰階層產生的示意圖。在此範例中，階層的頂級為組織金鑰 210。組織金鑰 210 可儲存在組織金鑰伺服器 148 (第 1A 圖)內，或可提供在要存取使用第 2B 圖內例示金鑰階層之電腦系統內所有資訊等級之任何裝置內。不論哪個裝置接收該組織金鑰，可用任何合適的方式提供組織金鑰 210 給這些裝置。例如可由網路 S1

管理員提供，或用任何合適的方式在裝置內產生。

不論如何提供組織金鑰 210，都可用來產生多個指定位址空間配對金鑰，如例示的配對金鑰 224A、224B、224C 和 224D。在第 2A 圖內例示的具體實施例當中，基於組織金鑰 210 上執行的擬亂函數(pseudorandom function) 220，結合指定位址空間配對衍生輸入 222，來產生每一指定位址空間配對金鑰。此函數可在組織金鑰伺服器 148 (第 1B 圖)內執行。如此，組織金鑰 210 可被維持在組織金鑰伺服器 148 內的安全環境中，或在將具備最高網路存取等級的任何其他裝置內，即使用它來(至少間接)產生所有階層等級上的金鑰。

密碼函數 220 可為任何合適的擬亂函數。如同業界內所熟知，在實際情況中，若其計算內所使用的金鑰足夠長並且亂(或擬亂)，則擬亂函數為從輸入至輸出顯現亂數性的函數。其中一項實施特性為金鑰無法從輸入-輸出配對確認。因此，雖然作為函數輸出而計算的指定位址空間配對金鑰 224A、224B、224C 和 224D 可提供給組織金鑰伺服器 148 外側之裝置，提供這些金鑰並不會危害組織金鑰 210 的安全性。

指定位址空間金鑰衍生輸入 222 可為任何合適的資訊，該資訊可用於讓裝置從組織金鑰 210 當中產生指定位址空間配對金鑰。舉例來說，指定位址空間配對金鑰[S]

衍生輸入 222 可為指定位址空間的識別碼，例如：若指定位址空間 110A (第 1A 圖)被識別為指定位址空間(1)並且指定位址空間 110B 被識別為指定位址空間(2)，則可使用金鑰衍生輸入(1、2)的配對，產生在指定位址空間 110A 和 110B 之間通訊的指定位址空間配對金鑰。

使用指定位址空間的識別碼作為指定位址空間配對金鑰衍生輸入 222，允許具有組織金鑰 210 存取權限的任何裝置產生相同的指定位址空間配對金鑰組，例如：若將電腦系統 100 內所有訊息流量的存取權限給予中間裝置 140C (第 1A 圖)，則中間裝置 140C 可存取組織金鑰 210。如此，中間裝置 140C 可用與組織金鑰伺服器 148 相同的方式，產生指定位址空間配對金鑰 224A...224D。中間裝置 140C 內產生的指定位址空間配對金鑰接著可用來產生較低金鑰階層等級上的金鑰。此後續金鑰產生可用來產生任何階層等級上的金鑰，包含用來將在兩主機之間通訊，屬於安全相聯一部分的封包加密之安全相聯金鑰。

在例示的具體實施例內，可產生用於每一唯一指定位址空間配對的配對指定位址空間金鑰 $EK_{i,j}$。在此具體實施例內，相同配對金鑰用來從第一指定位址空間內的伺服器通訊至第二指定位址空間內的用戶端，如同從第二指定位址空間內的伺服器通訊至第一指定位址空間內的[S]

用戶端。因此，配對金鑰 $EK_{i,j}$ 等同於配對金鑰 $EK_{j,i}$。不過在某些具體實施例內，產生不同的金鑰給每一階指定位址空間配對。

第 2A 圖例示已經產生一整組指定位址空間配對金鑰。在某些具體實施例內，可動態產生配對金鑰，如此只為正在通訊的指定位址空間對產生配對金鑰。不論何時以及有多少指定位址空間配對金鑰產生，都可使用配對金鑰來產生一或多個伺服器金鑰。

如所示，從配對的指定位址空間金鑰當中使用擬亂密碼函數 230 產生每一伺服器金鑰。在具有擬亂密碼函數 220 之下，擬亂密碼函數 230 以一方式從階層內較高等級上的金鑰產生伺服器金鑰，該方式藉由無法實際計算出之特性，從隨機產生之函數中區隔出輸入-輸出配對，尤其是復原函數內所使用來從該輸入計算伺服器金鑰輸出之較高等級金鑰。不過，基於伺服器金鑰衍生輸入 232 以可預測的方式產生每一伺服器金鑰。因此，假設該裝置已經存取至伺服器金鑰衍生輸入，具有指定位址空間配對金鑰 $EK_{i,j}$ 存取權限的任何裝置都可產生一金鑰，指定位址空間 i 內的伺服器將使用此金鑰與指定位址空間 j 內的用戶端通訊，或指定位址空間 i 內的伺服器將使用此金鑰與指定位址空間 j 內的伺服器通訊。在例示的具體實施例內，伺服器金鑰衍生輸入可僅為產生金鑰的伺

服器之識別碼。因為這種識別碼可迅速存取其他裝置，所以具有指定位址空間配對金鑰存取權限的裝置可重新建立伺服器金鑰，例如：在第 1A 圖的範例中，若要組態成監控離開指定位址空間 110A 的網路流量，則中間裝置 140A 可具有指定位址空間配對金鑰 $EK_{1,1}...EK_{1,M}$ 的存取權限，這足夠產生指定位址空間 110A 內裝置要使用的任何伺服器金鑰。

第 2A 圖例示用指定位址空間配對金鑰 $EK_{i,j}$ 來產生用於在指定位址空間 i 和 j 內裝置之間通訊的金鑰。指定位址空間 i 內的伺服器 k 需要金鑰用來與指定位址空間 j 內用戶端通訊時，則使用伺服器 k 的識別碼作為伺服器金鑰衍生輸入，來產生伺服器金鑰 $Sk_{i,j,k}$。如此產生多個伺服器金鑰，如所例示的伺服器金鑰 234A、234B、234C 和 234D。在此範例中，這些伺服器金鑰可用於不同伺服器，不過根據所通訊的用戶端裝置之位置，每一伺服器也可具有多個伺服器金鑰。在具有其他金鑰之下，伺服器金鑰可事先產生，或可在裝置間之通訊產生另一伺服器金鑰的需要時，動態產生。

從伺服器金鑰可產生個別安全相聯金鑰，像是金鑰 244A、244B、244C 和 244D。在具有其他金鑰之下，可使用單向密碼函數輸入下一個較高階層等級上的金鑰，來產生安全相聯金鑰。如此，擬亂密碼函數 240 使用伺[S]

服器金鑰，並且基於安全相聯金鑰衍生輸入 242 產生安全相聯金鑰。指定位址空間 i 內的伺服器 k 與指定位址空間 j 內的用戶端通訊時，產生不同的安全相聯金鑰給每一用戶端 m。因此，每一安全相聯可使用唯一的安全相聯金鑰 $CK_{i,j,k,m}$。

安全相聯金鑰 $CK_{i,j,k,m}$ 可從伺服器金鑰 $SK_{i,j,k}$ 以及與安全相聯 m 相關聯的安全相聯金鑰衍生輸入 242 產生。安全相聯金鑰衍生輸入 242 可為任何合適值。較佳是，該值相對於伺服器的現有安全相聯中為唯一值，因此可作為安全相聯的識別碼。在某些具體實施例內，安全相聯金鑰衍生輸入可為亂數產生之值。不過，該值可取決於時間戳記，或任何其他合適的資訊來源。

為了允許裝置從較高階層等級上的金鑰產生安全相聯金鑰，則這些裝置可取得安全相聯金鑰衍生輸入，例如：若中間裝置 140A (第 1A 圖)要監控從指定位址空間 110A (第 1A 圖)傳送的流量，則提供用來為牽涉到指定位址空間 110A 內裝置的所有安全相聯產生安全相聯金鑰之安全相聯金鑰衍生輸入給中間裝置 140A。任何合適的機制都可用來讓安全相聯金鑰衍生輸入可用。舉例來說，安全相聯金鑰衍生輸入可包含在使用這些輸入所產生安全相聯金鑰來加密之訊息內。

在第 2A 圖的具體實施例內，從組織金鑰 210 直接產生

每一配對指定位址空間金鑰，在此也可用其他方式。在替代具體實施例內，可從組織金鑰間接產生某些配對指定位址空間金鑰。第 2B 圖例示一具體實施例，其中基於指定位址空間金鑰伺服器之間的互動，從組織金鑰中間接產生指定位址空間配對金鑰。

第 2B 圖的程序從方塊 250 開始。在方塊 250 上，產生指定位址空間金鑰。在方塊 250 上產生的指定位址空間金鑰可用來產生在相同指定位址空間內裝置之間通訊之金鑰。因此，i 等於 j 時，方塊 250 上產生的指定位址空間金鑰可視為與指定位址空間配對金鑰 $EK_{i,j}$ 相等。方塊 250 上產生的指定位址空間金鑰可用合適的方式產生。舉例來說，可從組織金鑰 210 使用擬亂密碼函數產生指定位址空間金鑰，如第 2A 圖內所例示。不過在某些具體實施例內，由網路管理員直接在指定位址空間金鑰伺服器內提供指定位址空間金鑰，或用其他合適的方式取得，例如其可隨機產生。

一旦已經為每一指定位址空間產生金鑰，該程序前往迴圈起點 252。迴圈起點 252 為重複用於每一指定位址空間 i 的迴圈起點。從迴圈起點 252 開始，該程序前往迴圈起點 254。迴圈 254 為重複用於每一其他指定位址空間 j 的子迴圈起點。

該程序前往決策方塊 256。在決策方塊 256 上，處理

根據指定位址空間配對(i,j)是否需要配對金鑰來分支。若需要配對指定位址空間金鑰，則處理分支前往方塊258。在方塊258上，產生用於指定位址空間配對(i,j)的配對指定位址空間金鑰。

可使用任何合適的方式產生配對金鑰。舉例來說，可在指定位置空間 i 內的指定位置空間金鑰伺服器與指定位置空間 j 內的指定位置空間金鑰伺服器之間執行金鑰交換協定，此金鑰交換可用來獨力產生並共享配對金鑰 $EK_{i,j}$。

不過，使用任何合適密碼函數的任何合適機制都可用來產生配對金鑰。一旦產生配對金鑰後，該程序前往決策方塊 260，在此若要處理更多指定位址空間配對，則該程序回到迴圈起點 254。該程序用此方式在子迴圈內從迴圈起點 254、決策方塊 254、決策方塊 256、處理方塊 258 和決策方塊 260 持續進行，直到已經處理過每一指定位址空間。對於不需要金鑰配對的指定位址空間配對，可能是因為在指定位址空間配對內裝置之間並未發生通訊，處理從決策方塊 256 分支到決策方塊 260，繞過方塊 258 內的金鑰產生步驟。

一旦牽涉到迴圈起點 252 上所選指定位址空間 i 的每一指定位址空間配對已經完成從迴圈起點 254 開始的子迴圈內之處理，則處理將從決策方塊 260 前往決策方塊[S]

262。在決策方塊262上，處理將回到迴圈起點252選取下一個指定位址空間。然後針對下一個指定位址空間重複子迴圈254內的處理。處理將以此方式巡迴，直到已經針對發生通訊的每一指定位址空間配對產生配對指定位址空間金鑰。

不論產生配對指定位置空間金鑰的方式，該等配對指定位置空間金鑰可用來產生較低階層等級上的金鑰，最終形成電腦系統內裝置配對之間的安全相聯。來自配對金鑰集合的特定配對金鑰用於根據其中用於該安全相聯的主機所在之指定位址空間，形成特定安全相聯。這種方式牽涉到擁有可用資訊，此資訊關於其中特定主機可能所在的指定位址空間。

在某些具體實施例內，每一主機都可被提供其所在指定位址空間的指示。然後由主機提供指定位址空間識別給金鑰伺服器，或產生金鑰供主機使用的其他裝置。另外在某些具體實施例內，提供機制允許主機動態發現其所在的指定位址空間。在某些具體實施例內，動態指定位址空間發現程序也允許主機發現其中要作為安全相聯相對端點的其他主機所在之指定位址空間。

在某些具體實施例內，指定位址空間發現程序可併入形成安全相聯的協定內。第3圖例示形成安全相聯允許至少一個主機確定其中一或兩主機所在指定位址空間的

已知協定之修改。

第 3 圖例示作為伺服器 340 的第一主機與作為用戶端 350 的第二主機間之通訊。在例示的具體實施例內，伺服器 340 根據安全相聯產生通訊用的金鑰，然後伺服器 340 將金鑰分散到用戶端 350。在產生並分散金鑰之前，伺服器 340 和用戶端 350 交換一或多個控制金鑰產生與散佈處理的控制封包。因此，第 3 圖例示程序 308 內用於交換控制資訊作為產生與分散金鑰一部分之步驟。

程序 308 可為形成業界內已知安全相聯的一種程序或部分程序，例如：程序 308 代表根據網際網路金鑰交換(IKE)協定或 AuthIP 協定的封包交換。每一這些協定都牽涉到伺服器 340 與用戶端 350 之間控制封包的交換。

在第 3 圖的範例中，程序 308 牽涉到伺服器 340 傳送至用戶端 350 的控制封包 310。用戶端 350 回應而傳送控制封包 320 至伺服器 340。控制封包 310 和 320 可根據已知的協定或用任何其他合適的方式格式化。在第 3 圖的範例中，每一控制封包 310 和 320 都包含多個欄位。該協定未指定的資訊可插入一或多個這些欄位內，來支援指定位址空間發現而不背離該協定。

例如：圖中顯示控制封包 310 具有欄位 312、314 和 316。在此為了簡化所以顯示三個欄位，但是控制封包可具有比例示還要多的欄位。在此範例中，伺服器 340 將[S1

資訊元件 318 插入欄位 314 內。資訊元件 318 可用來作為指定位址空間發現程序的一部分，

同樣地，圖中顯示控制封包 320 具有欄位 322、324 和 326。在此範例中，支援指定位址空間發現的資訊元件已經插入欄位 326 內。在第 3 圖的範例中，資訊元件 330、332 和 334 已經插入欄位 326 內。每一這些資訊元件都由中間裝置插入，該中間裝置處理從用戶端 350 通過網路繞送至伺服器 340 的控制封包 320。伺服器 340 接收封包 320 時，擷取資訊元件 330、332 和 334 來決定其指定位址空間，以及用戶端 350 所在的指定位址空間(此為可選擇的)。

在例示的具體實施例內，使用資訊元件 318 發出信號給位於伺服器 340 與用戶端 350 之間網路內的中間裝置，告知伺服器 340 正根據指定位址空間發現程序搜尋資訊。資訊元件 318 可用任何合適的方式併入控制封包 310 內。舉例來說，資訊元件可加入控制封包 310 的 vendorID 欄位內，其可為某些已知通訊協定內定義的欄位。加入控制封包 310 中 vendorID 欄位之值可為發出指定位址空間發現程序為所要之任何預定程式碼。

控制封包 310 通過伺服器 340 與用戶端 350 之間的網路時，首先通過中間裝置 360。中間裝置 360 可為路由器或以已知方式處理控制封包 310 的其他多埠裝置，如 S1

此控制封包 310 繼續送往用戶端 350。除了這種已知的處理以外，中間裝置 360 可試驗欄位 314 的內容。在偵測到資訊元件 318 具有一值，指示伺服器 340 正在搜尋介入指定位址空間發現程序後，中間裝置 360 可儲存伺服器 340 正在搜尋指定位址空間發現資訊的指示 318'。然後中間裝置 360 可監控網路流量，來偵測定址至伺服器 340 的封包。

控制封包 310 可從中間裝置 360 傳遞至其他中間裝置，此處例示為中間裝置 362。中間裝置 362 用類似方式處理控制封包 310，也儲存伺服器 340 正在搜尋指定位址空間發現資訊的指示 318'。針對中間裝置 362，控制封包 310 可傳遞至要到用戶端 350 的路徑上之其他中間裝置。在此顯示一個額外的中間裝置，即中間裝置 364，再加上中間裝置 362 和 360。中間裝置 364 儲存伺服器 340 正在搜尋指定位址空間發現資訊的指示 318'。

用戶端 350 可回應控制封包 310，如業界內所熟知。對於控制封包 310 的一部分回應可為後續控制封包的產生，在此例示為控制封包 320。控制封包 320 通過網路朝向伺服器 340 時，通過處理控制封包 310 的中間裝置 364、362 和 360。因此，每一這些中間裝置檢查導引至伺服器 340 的網路封包，其中該中間裝置可將指定位址空間發現資訊插入該伺服器 340。因此，中間裝置 364

識別控制封包 320 為其中已經插入指定位址空間發現資訊的控制封包。

在例示的具體實施例內，控制封包 320 包含欄位 322、324 和 326。可利用建立安全相聯時使用的協定來定義欄位的特定數量與內容。不過在例示的具體實施例內，欄位 326 為可伸展欄位，表示協定未定義針對欄位 326 的內容需求。因此，中間裝置可將資訊插入欄位 326 內，不用改變形成伺服器 340 與用戶端 350 之間安全相聯所需之資訊。

中間裝置 364 將資訊插入欄位 326，伺服器 340 可用此作為決定用戶端 350 及/或伺服器 340 的指定位址空間之一部分處理。在例示的具體實施例內，中間裝置 364 插入資訊元件 330。資訊元件 330 指示已經指派中間裝置 364 的指定位址空間。因為中間裝置 364 為用戶端 350 所傳送封包首先遇到的中間裝置，中間裝置 364 可能為與用戶端 350 相同的指定位址空間相關聯之閘道器或其他多埠裝置。如此，資訊元件 330 可作為其中用戶端 350 所在的指定位址空間之指示器。

控制封包 320 通過網路後，接著由中間裝置 362 進行處理。因為中間裝置 362 正監控導引至伺服器 340 的封包，中間裝置 362 同樣偵測控制封包 320 並且插入資訊元件 332，該元件識別中間裝置 362 所在的指定位址空[S]

間。

資訊元件 332 以反映控制封包 320 處理順序的方式插入欄位 326 內。一種反映處理順序的簡單機制為將資訊元件 332 插入資訊元件 330 之後的清單內，不過可使用任何合適的結構來保留順序。

控制封包 320 通過網路繼續時，接著由中間裝置 360 進行處理。在具有中間裝置 362 和 364 之下，中間裝置 360 插入資訊元件 334，指示中間裝置所在的指定位址空間。資訊元件 334 同樣以保留處理順序的方式插入，例如將其附加至已經在欄位 326 內的資訊清單。

因此，控制封包 320 到達伺服器 340 時，伺服器 340 可分析欄位 326 的內容，來判定控制封包 320 從用戶端 350 傳遞至伺服器 340 中經過的指定位址空間。路徑兩端上的指定位址空間可能是伺服器 340 和用戶端 350 所在的指定位址空間之指示器。該指定位址空間配對由欄位 326 內清單兩端上的資訊元件所識別，在此為資訊元件 330 和 334，其可用來選擇配對金鑰，產生用於伺服器 340 與用戶端 350 之間安全相聯的安全相聯金鑰。在第 2A 圖例示的具體實施例內，此資訊可用來選擇產生安全相聯金鑰時所要使用的特定伺服器金鑰。

吾人應該瞭解，第 3 圖例示指示位址空間發現程序之一範例，而可有其他變型。例如在某些具體實施例內，[S]

通過網路不同的路徑可導致控制封包通過不同的中間裝置。結果，並非所有案例中伺服器 340 都接收自己指定位址空間的一致指示。在該案例中，伺服器 340 可維持不同時間上所接收有關其所指示指定位址空間之資訊。伺服器 340 可分析此資訊來判定其指定位址空間位置。作為一進一步的變型，用戶端 350 知道其指定位址空間時，可插入資訊到欄位 326 內作為清單內第一資訊元件，否則發出其指定位址空間位置的信號。在又另一變型中，中間裝置可搭配其被指派的指定位址空間插入額外資訊，例如：中間裝置可包含識別指定位址空間金鑰為其所傳遞的其他指定位址空間之資訊，如此該伺服器可判定，沿著該路徑的所有中間裝置是否都具有必要的配對金鑰，來處理用戶端發現的指定位址空間與伺服器發現的指定位址空間間之流量。

第 3 圖例示中間裝置每次將用於發現指定位址空間的資訊元件插入該第一封包內，該封包係由該等中間裝置偵測到其在資訊元件 318 接收之後導引至伺服器 340。中間裝置可在任何合適的時間上，相關於資訊元件 318 的接受，將資訊元件插入任何合適數量的封包內。或者，中間裝置可將資訊元件插入多個封包內，或用於資訊元件 318 接受之後預定時間量。

作為其他變型範例，中間裝置可插入資訊元件用於指[S]

定位址空間發現，而不需要來自需要指定位址空間發現資訊的伺服器之特定指示。在這種具體實施例內，中間裝置可將指定位址空間發現資訊插入所有封包內，或只插入特定類型的封包內。例如：中間裝置可將用於指定位址空間發現的資訊元件插入形成安全相聯所使用的所有控制封包內，而不論是否中間裝置之前已經偵測到需要這種指定位址空間發現的資訊元件。

不論提供給伺服器 340 的指定位址空間發現資訊所指定為何，一旦伺服器 340 可識別其指定位址空間以及用戶端 350 的指定位址空間，則可產生安全相聯金鑰或金鑰並且使用已知通訊協定或用任何其他合適的方式，完成與用戶端 350 形成安全相聯的處理。此後，伺服器 340 和用戶端 350 可依照安全相聯來通訊。第 3 圖例示緊接著程序 308，用戶端 350 和伺服器 340 可根據安全相聯交換封包。封包 370 作為範例來例示。

封包 370 可根據定義用戶端 350 與伺服器 340 之間安全相聯的協定來格式化。封包 370 可包含多個欄位，例示有欄位 372、374 和 376。每一欄位都可包含不同的資訊類型。例如：欄位 376 可包含已經用安全相聯金鑰簽署或加密的資料。封包 370 內的其他欄位可用來繞送封包 370 通過網路，否則用來處理封包 370。

封包 370 內一個這種欄位可包含金鑰衍生資訊，其用[S]

來產生用戶端 350 與伺服器 340 之間安全相聯的安全相聯金鑰。在封包 370 內併入金鑰衍生資訊允許具有所使用金鑰階層內任何等級上金鑰存取權限的任何裝置，衍生該安全相聯金鑰來再生安全相聯金鑰並處理封包 370。在第 2A 圖內例示的金鑰階層當中，這種金鑰衍生資訊可包含用戶端 350 與伺服器 340 所在的指定位址空間配對、產生安全相聯金鑰的伺服器識別以及用來產生安全相聯金鑰的金鑰衍生輸入 242。

此資訊可用任何合適的方式併入封包 370 內。在第 3 圖的範例中，此資訊記錄在封包 370 的欄位 374 內。在例示的範例中，欄位 374 內含一個伺服器 ID 380，可識別產生安全相聯金鑰的伺服器。另外，欄位 374 可包含安全參數索引(Security parameter index，「SPI」)，其可包含或識別其他金鑰衍生輸入。SPI 可識別用來作為金鑰衍生輸入 242 (第 2A 圖)的亂數，以及/或其中用戶端 350 和伺服器 340 所在的指定位址空間配對。不過，吾人應該瞭解，第 3 圖只例示機制的一個範例，其中金鑰衍生資訊可用於裝置處理封包 370。

如所示，金鑰衍生資訊欄位 374 並未加密。儘管如此，因為欄位 374 內的金鑰衍生輸入只對於內含來自安全相聯金鑰所產生金鑰之裝置有用，所以可維持封包 370 的安全。 [S]

被授權從產生安全相聯金鑰中獲得金鑰的任何裝置可再生用於處理封包 370 的安全相聯金鑰，此處理可由伺服器 340 執行或由任一個中間裝置執行，像是中間裝置 360、362 和 364。

在某些具體實施例內，產生安全相聯金鑰如此可處理封包 370 的處理可被卸載至網路界面卡內之硬體，或電腦裝置的其他合適組件。該硬體若已經存取適當金鑰，則可在處理封包 370 時即時產生安全相聯金鑰，然後使用產生的金鑰處理封包 370 內之資訊。第 4A 圖例示可在像是伺服器 340 這類伺服器內執行之程序 400。不過，在任何裝置內都可執行可比較的處理，像是任何中間裝置 360、362 或 364。

程序 400 從方塊 410 開始。在方塊 410 上，伺服器獲得伺服器所在的指定位址空間之配對金鑰。伺服器所在的指定位址空間可用上述關於第 3 圖之指定位址空間發現程序，或用任何其他合適的方式來識別。

在方塊 410 上獲得的配對金鑰可為指定位址空間配對金鑰，像是第 2A 圖內例示的配對金鑰 224A...224D。或者，在其中從指定位址空間配對金鑰產生伺服器配對金鑰的具體實施例內，在方塊 410 上獲得的配對金鑰可為伺服器配對金鑰，像是第 2A 圖內的金鑰 234A...234D。不論配對金鑰的特定格式，其可從任何合適的來源獲

得，像是內含用來產生安全相聯金鑰的伺服器之指定位址空間之內或之外的金鑰伺服器。

在方塊 412 上，配對金鑰儲存在伺服器上。該金鑰可儲存在與伺服器相關聯的任何合適電腦儲存媒體內。不過，在其中要執行密碼函數之硬體卸載的具體實施例內，配對金鑰可儲存在網路界面硬體內，像是網路界面卡(Network interface card，「NIC」)。

然後該程序前往迴圈起點 420，即對伺服器將輸入的每一安全相聯執行之迴圈的起點。在開始於迴圈起點 420 之迴圈內，伺服器可執行適用於一個安全相聯的處理。該處理從方塊 422 開始，在該方塊 422 中伺服器傳送訊息給用戶端，也就是安全相聯的第二主機。這種訊息可為控制封包 310 的形式(第 3 圖)，不過任何合適的訊息格式都可使用，包含一經特別格式化的訊息，其係為了從用戶端或從訊息路徑上中間裝置引出其所在指定位址空間的指示。

然後該程序前往方塊 424，在此伺服器接收來自用戶端的回應。這種回應可為控制封包 320 的格式(第 3 圖)，其中中間裝置已經插入指定位址空間發現資訊。不過，方塊 424 上接收的回應可為任何合適的格式，包含由用戶端用於傳輸其指定位址空間所特殊格式化的訊息。

不論方塊 422 上所傳送訊息的格式以及方塊 424 上所[S]

接收的回應為何，伺服器可處理方塊 426 和 428 上的回應，來確定用戶端與伺服器的適當指定位址空間配對。在方塊 426 上，從回應當中擷取識別伺服器指定位址空間的資訊，並且在方塊 428 上，從回應當中擷取識別用戶端指定位址空間的資訊。方塊 426 和 428 上的處理可牽涉到處理資訊元件，像是 330、332 和 334 (第 3 圖)的清單。不過，方塊 426 和 428 上的處理可用任何合適的方式執行，以確定用於用戶端與伺服器的適當指定位址空間配對。

一旦已經識別適當指定位址空間配對，在方塊 430 上選擇配對金鑰。在某些具體實施例內，選擇配對金鑰必須存取金鑰伺服器。在其他具體實施例內，選擇配對金鑰必須從一組之前下載至伺服器的配對金鑰當中讀取。例如，選擇可基於方塊 410 上獲得的金鑰。

熟習此項技術者將瞭解，第 4A 圖為簡化圖並且程序 400 的步驟不需確實依照範例內的順序來執行。作為可能變型的一個範例，吾人應該瞭解，在方塊 430 上選擇配對金鑰可形成在方塊 410 上獲得配對金鑰所需處理的一部分。例如若有大量配對金鑰可以使用，則可使用這種程序。在該案例中，當方塊 430 上識別與其他指定位址空間內用戶端一起形成安全相聯所需特定配對金鑰之處理，可動態並且遞增下載配對金鑰。 [S]

不論何時與何處獲得該選取的配對金鑰，該程序都前往方塊 432。在方塊 432 上，獲得產生安全相聯金鑰的金鑰衍生輸入。在某些具體實施例內，金鑰衍生輸入可包含一亂數，如此方塊 432 上的處理可包含該亂數的產生。或者，或此外，金鑰衍生輸入可包含在方塊 426 上偵測到的伺服器指定位址空間之識別碼，以及方塊 428 上偵測到的用戶端指定位址空間之識別碼。

不論特定衍生輸入與來源獲得之處，處理繼續前往方塊 434，在此衍生安全相聯金鑰。方塊 434 上的處理可牽涉到使用方塊 430 上選取的配對金鑰，在方塊 432 上獲得的金鑰衍生輸入內執行密碼函數。不過，使用任何合適的方式可產生安全相聯金鑰。

產生安全相聯金鑰必須在伺服器與用戶端之間互動，如此用戶端與伺服器都具有安全相聯金鑰的副本。安全相聯金鑰可由伺服器產生，然後用任何合適的方式通訊至用戶端，包含業界內已知的金鑰交換協定。該金鑰也可使用伺服器與用戶端之間共享的其他資訊來在這兩者之上產生。合適金鑰交換協定的範例為 IKE 和 AuthIP。因此，第 4B 圖顯示金鑰交換子程序 436。吾人應該瞭解，第 4B 圖示意指示由共享金鑰的用戶端和伺服器發生互動，並且這些互動可在第 4B 圖內所示以外時間上交換資訊。 [S]

不論安全相聯金鑰如何通訊至用戶端，該程序也可包含在方塊 438 上傳遞金鑰衍生資訊至用戶端。雖然用戶端可能不使用金鑰衍生資訊進行封包上的加密處理，不過用戶端可使用某些或全部金鑰衍生資訊來標示通過安全相聯來傳送的封包。用此方式標示封包允許裝置(尤其是不直接參與金鑰交換的中間裝置)再生安全相聯金鑰，如此可處理通過安全相聯傳送的封包。

緊接在子程序 436 內金鑰交換之後，方塊 448 例示包含在方塊 438 上提供金鑰衍生資訊，在方塊 448 上，用戶端與伺服器可使用由某些或全部金鑰衍生資訊標示的封包透過安全相聯來通訊。

程序 400 可用與伺服器相關聯的任何合適硬體來執行。某些或全部程序 400 可由伺服器內一或多個處理器上執行之軟體來控制。另外程序 400 的某些或全部步驟可卸載至伺服器內隨附的其他硬體，例如：在方塊 440 上通訊的處理封包隨附之密碼函數可卸載至伺服器網路界面內的硬體。

如上面所提及，階層散佈系統允許具有金鑰存取權限的中間裝置處理安全相聯內之封包。在某些電腦系統內，並非要處理安全相聯內封包的所有中間裝置都能夠支援這種階層金鑰產生。在這些具體實施例內，伺服器可支援與授權的中間裝置直接金鑰交換。直接金鑰交換[S]

可用任何合適的方式觸發，例如：中間裝置可透過類似於指定位址空間發現所使用的發訊機制，發訊給末端主機，告知直接金鑰交換的需求。

第 4B 圖例示在偵測封包形成安全相聯給不具有安全相聯金鑰的中間裝置時，中間裝置可在指引至伺服器的封包內提供資訊。該資訊可作為對伺服器之請求，使其加入與中間裝置的直接金鑰交換，例如：第 3 圖例示當做建立安全相聯一部分來傳遞的控制封包。中間裝置可例如在指引至伺服器 340 的控制封包 320 之欄位內設定一旗標，這種旗標可作為對伺服器 340 之請求，使其加入與中間裝置的直接金鑰交換協定。

第 4B 圖例示伺服器接收這種旗標封包時，處理可從決策方塊 442 分支到方塊 444。在方塊 444 上，伺服器可與中間裝置共享安全相聯金鑰。伺服器可用業界內已知的合適方式共享金鑰，包含使用金鑰交換協定。這種程序可包含驗證中間裝置被授權存取通過安全相聯通訊之資訊。

在例示的具體實施例內，可附加方塊 442 上所偵測之旗標於其上的封包為建立安全相聯時伴隨之控制封包。在某些案例中，在已經建立安全相聯之後，中間裝置可進入或離開用戶端與伺服器間之通路。網路組態的改變，或是因負載或其他條件在網路操作其間可能改變而[S]

改變封包路由之多埠裝置的條件處理改變，會導致發生這種網路路徑內的改變。在其中之被授權處理與安全相聯相關聯之封包的每一中間裝置從封包中獲得金鑰衍生資訊之具體實施例內，在形成安全相聯之後進入通路的任何新中間裝置，與形成安全相聯時徑路內的中間裝置相同，都可存取封包。不過，無法如上述使用階層金鑰執行動態金鑰產生的中間裝置，在形成安全相聯之後新增至通路時，無法發訊給伺服器作為安全相聯形成的一部分，來與中間裝置執行直接金鑰交換。因此，根據某些具體實施例的電腦系統可併入不支援動態金鑰產生的中間裝置以獲得適當安全相聯金鑰之機制。

在第 4B 圖內例示的範例中，這種中間裝置可標示指引至伺服器的任何封包。這種旗標可由伺服器解譯為重新產生安全相聯之要求。作為重新產生金鑰的一部分，中間裝置可要求從伺服器直接產生金鑰，如決策方塊 442 和方塊 444 之結合所描述。因此，第 4B 圖的程序包含決策方塊 450，其中若伺服器從中間裝置接收具有標示要求的封包時，則處理分支來執行重新產生金鑰操作。

若接收到這種要求，則該程序從決策方塊 450 分支到決策方塊 452。在決策方塊 452 上，根據伺服器是否判定插入旗標的中間裝置為有效中間裝置，程序再次分支。用來決定有效中間裝置的任何合適方式都可使用。[S]

舉例來說，接收這種旗標封包時，伺服器可確認封包的整體性，來確定設定旗標的中間裝置位於一通路內，該通路係由在參與安全相聯的伺服器與用戶端之間流動的驗證封包所流過。

不論如何判定中間裝置的有效性，若中間裝置無效，則該程序分支到決策方塊 454。相對地，若要求來自有效的中間裝置，則該程序回到迴圈起點 420，重複建立安全相聯的程序。

可對每一作動中的安全相聯執行方塊 422、424、426、428、430、432、434、436、438、440、442、444、450 和 452 上的處理。因此，第 4B 圖例示對一個安全相聯完成處理時，該程序從決策方塊 454 回到迴圈起點 420，在此重複對其他作動中的安全相聯之處理。吾人應該瞭解，雖然第 4A 圖和第 4B 圖例示順序處理，此係為了簡化所以才依序例示此處理，因此可同時或用任何其他合適的時間來執行多安全相聯的處理。

第 4A 圖和第 4B 圖例示伺服器上執行的處理，該伺服器屬於安全相聯中一部主機。處理也在用戶端上執行，該用戶端屬於安全相聯的第二主機。第 5 圖提供可在用戶端上執行的處理範例。

第 5 圖的程序從方塊 510 開始，在此開始與伺服器的安全連線。該連線可由用戶端上的處理、利用伺服器上[S]

的處理或回應任何合適的事件開始執行。

安全連線可用任何合適方式形成。形成安全連線就可從用戶端將一或多個控制訊息傳送至伺服器，如同方塊512上的處理。方塊512上的處理可由用戶端傳送控制訊息，像是控制訊息320(第3圖)，或傳送及/或接收一或多個控制訊息。

形成安全連線也可執行與伺服器的金鑰交換協定。在方塊520上，由於用戶端從伺服器獲得安全相聯金鑰，所以用戶端可參與這種金鑰交換。

在某些具體實施例內，並未要求修改用戶端，以便如上述使用階層金鑰。因此，方塊510、512和520上的處理可用業界內熟知的技術來執行，不過，可執行任何合適的處理。

一旦已經形成安全相聯，該程序前往方塊522，在此用戶端接收金鑰衍生資訊。如上述，使用安全相聯傳送的訊息可使用金鑰衍生資訊標示，如此接收到這些封包的任何被授權之裝置都可產生適當的安全相聯金鑰。在例示的具體實施例內，依照安全相聯通訊的封包(不論由用戶端或伺服器開始)使用金鑰衍生資訊標示。因此在方塊522上，用戶端接收並儲存金鑰衍生資訊。在方塊522上接收衍生資訊可從內含金鑰衍生資訊的伺服器接收封包。不過，方塊522上可使用提供金鑰衍生資訊給用戶[S]

端的任何合適機制。

一旦用戶端同時擁有安全相聯金鑰與金鑰衍生資訊，則開始使用安全相聯傳遞封包。在方塊 524 上，使用安全相聯金鑰產生封包。為了產生根據安全相聯的封包，可使用業界內已知的技術執行方塊 524 上的處理，。

在方塊 526 上，在方塊 522 上接收的金鑰衍生資訊附加至方塊 524 上產生之封包。在像是第 2A 圖中例示的具體實施例內，其中有四個金鑰階層等級，金鑰衍生資訊可包含來自所有金鑰產生等級的金鑰衍生資訊。因此，方塊 526 上新增的資訊可包含指定位址空間配對資訊、伺服器識別資訊以及伺服器用來產生安全相聯金鑰之值。不過，方塊 526 上新增的特定資訊可取決於金鑰階層內的等級數，以及用來產生每一階層等級上金鑰之特定衍生資訊。

一旦封包已經格式化，處理前往方塊 528。在方塊 528 上，用戶端傳輸封包至伺服器。在方塊 530 上，用戶端從伺服器接收封包。在方塊 532 上，用戶端可使用方塊 520 內獲得的安全相聯金鑰，解密及/或驗證接收的封包。方塊 528、530 和 532 上的處理可用業界內熟知的技術來執行，不過可使用任何合適的傳輸、接收與解密及/或驗證封包之機制。

然後該程序前往決策方塊 540，在此根據是否有更多[S]

資料要使用安全相聯傳送或接收，該程序可進行分支。有更多資料需要處理時，該程序回到方塊 524，在此用戶端使用安全相聯產生及/或接收其他封包。用戶端與伺服器之間沒有其他資料要通訊時，第 5 圖的程序結束。

第 6 圖例示可由中間裝置執行的程序。如上述，中間裝置可參與指定位址空間發現程序。此外，中間裝置可監控與處理依照其他裝置牽涉其中的安全相聯來傳輸之封包。

第 6 圖例示中間裝置可在方塊 610 上監控封包。在方塊 610 上，中間裝置偵測通過網路的封包，此監控可使用業界內已知的電路及技術來執行，不過可使用任何合適的方式來偵測通過網路傳輸的封包。

中間裝置偵測到封包時，根據封包是否標示為發現封包，處理可在決策方塊 612 上分支。在第 3 圖的具體實施例內，利用在欄位內，像是欄位 314，包含資訊元件 318，封包可標示為發現封包。不過，任何合適的機制都可用來指定發現封包。

不論識別發現封包的定方法為何，只要發現一個發現封包，則處理就從決策方塊 612 分支到方塊 614。在方塊 614 上，中間裝置將其指定位址空間的指示附加至一或多個封包。在某些具體實施例內，指定位址空間資訊所附加的封包與發現封包相同。在該案例中，由與產生

發現封包的主機相對之主機接收方塊 614 上之指定位址空間發現資訊。或者如第 3 圖內所指示，指定位址空間資訊可附加至後續封包，其指引至產生發現封包的主機。不論對於發現封包的特定回應為何，一旦完成該回應，則第 6 圖的處理結束。

若藉由在方塊 610 上監控，偵測到封包不含發現封包，則該程序從決策方塊 612 分支到方塊 630。在方塊 630 上，中間裝置可在封包上執行密碼函數，其可基於所接收封包內金鑰衍生資訊，以及可用於中間裝置之較高階層等級上的金鑰，來產生安全相聯金鑰。中間裝置所執行的特定密碼函數取決於中間裝置的性質以及封包內的資訊。不論執行的密碼函數為何，一旦完成，第 6 圖的程序結束。

如上述，階層金鑰散佈系統之一用途，係幫助將能夠使用安全相聯監控封包傳遞的中間裝置併入電腦系統。能夠監控透過安全相聯保護的網路流量之中間裝置可執行多個網路管理或保護功能。在某些具體實施例內，可提供金鑰給中間裝置，以允許使用網路封包伴隨的金鑰衍生資訊產生安全相聯金鑰。這種裝置可用提供支援安全指定位址空間卸載的網路界面硬體來實施，不過在大型企業內，並非所有中間裝置都可具有這種網路界面硬體，並且可能不支援使用金鑰衍生資訊來產生安全相聯 51

金鑰，或可能沒有提供較高等級金鑰來衍生安全相聯金鑰的金鑰伺服器之存取權限。因此在某些具體實施例內，電腦系統內使用的協定可提供用於一或多安全相聯或直接提供給中間裝置的較高等級金鑰之機制。第 7 圖為伺服器與中間裝置之間互動的範例，其中該中間裝置可發訊給伺服器，告知需要直接傳輸安全相聯金鑰或較高等級金鑰，並且伺服器以此金鑰回應。

第 7 圖的程序從子程序 700 開始，在此伺服器建立與用戶端的安全相聯，同時透過直接金鑰交換提供安全相聯金鑰給中間裝置。子程序 700 開始於方塊 710，在此伺服器使用指示器標示用於建立安全相聯的控制封包中至少一者，讓伺服器支援與中間裝置的直接金鑰交換。方塊 710 上加入的標記可為任何合適形式。例如：在第 3 圖內指示的訊息交換內，類似於資訊元件 318 但是具有不同值的資訊元件可放入控制封包 310 內。

在方塊 712 上，伺服器可開始建立與用戶端的安全相聯之處理。建立安全相聯可包含傳送方塊 710 上產生的標記封包。

在伺服器與用戶端之間交換作為建立安全相聯一部分的封包將傳遞通過中間裝置。在方塊 720 上，中間裝置監控網路流量，並且偵測在伺服器與用戶端之間傳遞並且與建立安全相聯相關聯的封包。偵測到這種封包時，[S]

處理前往決策方塊 722，在此該程序根據中間裝置是否可使用安全指定位址空間金鑰產生來產生用於處理該封包的金鑰來分支。若可使用，子程序 700 可完成，處理為中間裝置而前往方塊 752，以及為伺服器而前往方塊 750。

在方塊 750 上，伺服器可使用與用戶端建立的安全相聯來產生網路流量。在方塊 752 上由中間裝置偵測作為安全相聯一部分來傳送的封包，因為中間裝置支援使用安全指定位址空間金鑰的處理，則中間裝置可產生在方塊 750 上產生的網路流量上執行加密處理所需之安全相聯金鑰。因此在方塊 752 上，中間裝置可監控並且處理該網路流量。

相反地，若中間裝置無法產生金鑰，則該程序從決策方塊 722 分支到決策方塊 724。中間裝置可能因為一些因素無法產生金鑰，例如：中間裝置可能完全無法支援安全指定位址空間金鑰產生。或者，該裝置可支援金鑰產生，但是缺乏適當等級上的金鑰來處理接收的封包。在例示的具體實施例內，不論中間裝置為何無法產生金鑰，處理均分支至決策方塊 714。不過，可能用其他具體實施例，其中根據無法產生金鑰的因素來執行不同處理。

在決策方塊 724 上，該程序再度分支。在方塊 724 上 [S]

該程序根據中間裝置是否具有伺服器所建立之安全相聯金鑰的存取權限來分支。金鑰可透過某些外界程序或以任何其他合適方式，而可用於中間裝置。不論這些金鑰如何可用於中間裝置，若中間裝置具有安全相聯金鑰，且其中該金鑰為在伺服器與用戶端之間產生的網路流量上執行加密處理作為安全相聯一部分之所必要，則該程序從決策方塊 724 分支到方塊 752 和 750，如上述其中伺服器與用戶端可產生網路流量，而流量受到中間裝置的監控。

不過，若中間裝置不支援產生安全相聯金鑰或不具有安全相聯金鑰或任何較高等級金鑰的存取權限，該程序從決策方塊 724 分支到方塊 726。在方塊 726 上，中間裝置發訊給伺服器，告知需要安全相聯金鑰或較高等級金鑰用於方塊 712 上建立的安全相聯。中間裝置可用任何合適的方式發出此需求給伺服器。舉例來說，中間裝置標記一控制封包，例如具有需要安全相聯金鑰的指示之控制封包 320 (第 3 圖)。任何合適的資訊元件都可新增至封包，發訊給伺服器告知需要安全相聯金鑰或較高等級金鑰。

在 726 上伺服器接收中間裝置標示的封包時，在方塊 740 上伺服器開始金鑰交換程序。在方塊 740 上，伺服器與中間裝置執行金鑰交換。金鑰交換的協定可與用來[S]

提供安全相聯金鑰給用戶端的協定相同，不過，任何合適的協定都可用於方塊 740 與 742 上的金鑰交換。該金鑰交換訊息也可包含在伺服器與用戶端之間傳遞的控制封包內，包含指出支援或需要直接金鑰交換的標記。再者，金鑰交換牽涉到接觸金鑰伺服器來獲得適合用於中間裝置的較高層金鑰之伺服器，如此只有中間裝置(並非伺服器)可進行加密。

一旦完成金鑰交換，該程序繼續前往方塊 750 和 752，如上述其中伺服器和用戶端可使用安全相聯來產生網路流量，這在方塊 752 上由中間裝置使用方塊 742 上獲得的安全相聯金鑰來監控。

因為伺服器與中間裝置都支援根據第 7 圖內例示的協定，所以第 7 圖內的程序係為可能。在其中伺服器不支援直接金鑰交換的具體實施例內，在方塊 720 上接收的封包將不會標示方塊 710 上提供的指示。在此案例中，中間裝置放棄要求直接金鑰交換，如方塊 726 上所指示。而是中間裝置採取一或多種其他動作，試圖以其他方式獲得安全相聯金鑰，或可記錄無法為安全相聯監控網路流量的錯誤或其他指示。

另外吾人應該瞭解，第 7 圖的程序依賴控制封包交換當中在伺服器與中間裝置之間傳遞之資訊，而伺服器建立與用戶端的安全相聯。在某些案例中，在已經建立安[S]

全相聯時，中間裝置並不在用戶端與伺服器間之通路內。儘管如此，中間裝置可觸發直接金鑰交換。第 8 圖例示可在該案例中執行之處理。

第 8 圖的處理從方塊 812 開始，其中伺服器已經根據建立的安全相聯與用戶端通訊。

在方塊 820 上，中間裝置可監控在用戶端與伺服器之間交換的封包，不過因為中間裝置缺乏用於該安全相聯的安全相聯金鑰，所以無法在這些封包上執行密碼函數。例如在轉送已驗證封包時，無法將封包內已加密的資訊解密，或無法用任何方式改變已經指派的封包。不過，如同方塊 820 上監控的一部分，中間裝置可識別已經建立安全相聯的伺服器。

在決策方塊 822 上，程序根據中間裝置是否支援產生安全相聯金鑰存並且獲得必要較高層金鑰來分支。若是如此，處理分支到方塊 850 和 852。在方塊 852 上，伺服器產生網路流量作為與用戶端的安全相聯一部分。在方塊 852 上，中間裝置可監控網路流量，包含使用所產生的安全相聯金鑰來執行密碼函數。

相反地，若中間裝置不支援產生安全協定金鑰，則該程序分支到決策方塊 824。在決策方塊 824 上，該程序根據中間裝置是否另外獲得安全相聯金鑰來分支。若獲得，則該程序分支到方塊 850 和 852，其中用戶端與伺[S1]

服器產生網路流量作為安全相聯的一部分，該流量受到使用安全相聯金鑰的中間裝置之監控。

若中間裝置不具有安全相聯金鑰並且無法產生時，則該程序從決策方塊 824 分支到方塊 826。在方塊 826 上，中間裝置提供信號給伺服器，指示不具有安全相聯金鑰。此信號可用任何合適的方式提供，例如：封包根據 IPsec 通訊時，方塊 826 上的處理可牽涉到在目的地為伺服器的 IPsec 封包內設定旗標。在第 3 圖的範例中，此旗標可設定在封包內，像是封包 370。方塊 826 上可運用任何合適的機制來發訊給伺服器。

伺服器偵測到來自中間裝置的信號時，伺服器上的處理繼續前往方塊 830。在方塊 830 上，伺服器確認在伺服器與用戶端之間通路內的已授權中間裝置已經標示方塊 826 上標示的封包。任何合適的機制都可用來做出此判定。例如：伺服器可確認封包的整合度，如此推論其發自於用戶端，因此必須由具有伺服器與用戶端之間通路上封包存取權限的中間裝置來標示。

方塊 830 上的處理判定中間裝置為應該獲得安全相聯金鑰之已授權中間裝置時，伺服器開始與用戶端的安全相聯重新產生金鑰操作。重複此重新產生金鑰操作，允許中間裝置要求直接金鑰產生。因此，遵照方塊 830 上的確認，可執行上述第 7 圖內的子程序 700。當然，若[S]

無法確認中間裝置，該程序可終止或採取其他動作，避免讓未授權的裝置觸發重新產生金鑰。

執行子程序 700 之後，中間裝置可具有安全相聯金鑰，用於伺服器與用戶端之間的安全相聯。因此在方塊 850 和 852 上，伺服器與用戶端可產生網路流量，其能夠由中間裝置監控。因為中間裝置具有安全相聯金鑰的存取權限，所以監控可包含執行密碼函數。

上述處理可在使用任何合適硬體資源的主機以及中間裝置內執行。不過階層金鑰散佈系統的一用途為可行使某些密碼函數的硬體卸載處理。第 9A 圖例示可使用階層金鑰支援硬體卸載處理的計算裝置架構。

在第 9A 圖的範例中，裝置 910 包含網路界面硬體 920。網路界面硬體 920 可為網路界面卡或其他合適的硬體組件。網路界面硬體 920 可包含以任何合適方式實施的電路，例如：可包含一或多個應用積體電路、可程式邏輯裝置或使用微程式碼寫入程式的微處理器，來執行與網路(示意例示為網路 922)之界面連接相關聯的功能。

網路界面硬體 920 可包含業界內已知用於執行已知網路界面功能之硬體組件。此外，網路界面硬體 920 可包含硬體組件，其可基於來自網路界面卡上所儲存較高金鑰階層等級的金鑰，產生安全相聯金鑰。因此，第 9A 圖例示包含記憶體 926 的網路界面硬體 920。儲存於記

憶體 926 內者可為含有一或多配對金鑰的資料結構 928，從此資料結構 928 可產生安全相聯金鑰。在第 9A 圖的範例中，例示資料結構 928 處於其中保有三個配對金鑰，標示為金鑰 $K_{1,1}$、$K_{1,2}$ 和 $K_{1,3}$ 的狀態。裝置 910 位於指定位址空間 1 內，並且與指定位址空間 1 內其他裝置和指定位址空間 2 與 3 內裝置通訊時，則適用此狀態。不過吾人應該瞭解，第 9A 圖為網路裝置的簡略圖，並且網路裝置可包含超過三個金鑰。

不論資料結構 928 內含的金鑰數量，安全相聯金鑰產生器電路 930 都可存取這些金鑰。安全相聯金鑰產生器電路 930 可接收金鑰衍生資訊結合透過網路 922 所接收的封包。在回應上，安全相聯金鑰產生器電路 930 可存取記憶體 926，從資料結構 928 中獲得適當的配對金鑰。運用配對金鑰，安全相聯金鑰產生器 930 可產生安全相聯金鑰。

產生的安全相聯金鑰可提供給網路界面硬體 920 上其他組件，用於執行密碼函數。在第 9A 圖內例示的範例中，提供安全相聯金鑰給解密/驗證電路 924。解密/驗證電路 924 使用安全相聯金鑰來解密或驗證封包，一旦已經解密或驗證，則可提供封包給裝置 910 內較高架構等級上的組件。

如第 9A 圖內所例示，一旦已經在接收的封包上執行密[S]

碼函數，則透過驅動器 940 提供封包給作業系統 950 內的網路堆疊 952。如此封包可提供給應用程式 960。這種驅動器 940、作業系統 950 和應用程式 960 內的處理可使用已知的技術來執行。如業界內所熟知，驅動器 940、作業系統 950 和應用程式 960 的可能實施為裝置 910 內中央處理單元所執行的電腦可執行指令。

除了執行與封包接收相關聯的處理以外，網路界面硬體 920 可選擇性地被操作來執行與封包傳輸相關聯的處理。用於傳輸而非透過網路 922 接收金鑰衍生資訊時，安全相聯金鑰產生器 930 可從驅動器 940 或裝置 910 內某些其他組件接收金鑰衍生資訊。不論金鑰衍生資訊的來源，安全相聯金鑰產生器電路 930 可存取資料表 922，來獲得適當配對金鑰並且提供安全相聯金鑰給網路界面硬體 920 內其他組件。

第 9A 圖例示經組態作為安全指定位址空間內伺服器之裝置。類似架構可用於電腦系統內其他裝置，例如：一般來說相同架構可用於中間裝置，雖然中間裝置可具有至少兩個網路連接，並且可具有兩個網路界面硬體 920 副本。

用來實施中間裝置時，應用程式 960 可為執行網路監控功能或中間裝置可執行之其他功能之應用程式。此外，中間裝置可儲存與伺服器不同的配對金鑰。第 9B 圖[S]

例示資料表 958 的替代組態，若裝置 910 設置成為中間裝置時該替代組態可用來取代資料表 928。如第 9B 圖內所見，經組態用於中間裝置時，資料表 958 可包含用於超過一個指定位址空間的配對金鑰。

在此情況下，圖中顯示資料表 958 包含與指定位址空間 1 相關聯的配對金鑰。此外，資料表 958 內含用於指定位址空間 2 和 3 的配對金鑰。此資料表 958 的組態可適用於例如中間裝置，其接收來去指定位址空間 1 的通訊以及指定位址空間 2 和 3 之間的通訊。吾人應該瞭解，內含配對金鑰的資料庫組態可基於資料表所在整體系統內裝置的位置，以及裝置要存取訊息流量的指定位址空間。

經過至少一個本發明具體實施例的各種態樣之探討後，吾人應該瞭解，熟習此項技術者可輕易瞭解各種改變、修正和改善。

這些改變、修正與改善都屬於本發明一部分，並且隸屬於本發明的精神與範疇。因此，上面的說明與圖式都僅只為範例。

上面說明的本發明具體實施例可有各種實施方式，例如：可使用硬體、軟體或其組合來實施。在軟體內實施時，軟體程式碼可在單一電腦或分散在許多電腦之間的任何合適處理器或處理器集合上執行。 [S]

再者，吾人應該瞭解，電腦可具體實施在任何形式中，像是機櫃型電腦、桌上型電腦、膝上型電腦或平板電腦。此外，電腦可內嵌在一般並非認定為電腦但是具有合適處理能力的裝置內，包含個人數位助理(PDA)、智慧型電話或任何其他合適的可攜式或固定式電子裝置。

另外，電腦可具有一或多個輸入與輸出裝置，這些裝置可用來呈現使用者界面。可用來提供使用者界面的輸出裝置範例包含：以視覺方式表現輸出的印表機或顯示螢幕，以聽覺方式表現輸出的揚聲器或其他聲音產生裝置。可用於使用者界面的輸入裝置範例包含：鍵盤與指標裝置，像是滑鼠、觸控板以及數位板。作為另一範例，電腦可透過語音辨識或其他聲音格式接收輸入資訊。

這種電腦可用任何合適格式的一或多個網路互連在一起，包含區域網路或廣域網路，像是企業網路或網際網路。這種網路可根據任何合適的技術，並可根據任何合適的通訊協定來操作，並且包含無線網路、有線網路或光纖網路。

另外，此處所述的各種方法或處理都可編碼成軟體，可在運用各種作業系統或平台任一的一或多個處理器上執行。此外，這種軟體可使用任何數量的合適程式語言及/或程式或描述工具來撰寫，並且也可編譯為可執行的機械語言碼或可在框架或虛擬機器上執行的中間程式SI

碼。

在此方面，本發明也可具體實施為使用一或多種程式編碼的電腦可讀取媒體(或多重電腦可讀取媒體)(例如電腦記憶體、一或多種軟碟、光碟、磁帶、快閃記憶體、場可程式閘道陣列或其他半導體裝置內的電路組態或其他實體的電腦儲存媒體)，其在一或多部電腦或其他處理器上執行時，執行實施上述本發明各種具體實施例的方法。電腦可讀取媒體可為可傳送，如此上面儲存的程式可載入一或多部不同電腦或其他處理器，實施上述本發明的許多態樣。

此處所用的「程式」或「軟體」等詞一般就是指任何一種電腦程式碼或電腦可執行指令集，其可用來設計程式而使電腦或其他處理器實施上述本發明各種態樣。另外，吾人應該瞭解根據此具體實施例的一個態樣，執行時會執行本發明方法的一或多個電腦程式並不需要常駐在單一電腦或處理器上，可用模組方式分散在許多不同電腦或處理器之間，來實施本發明各種態樣。

電腦可執行指令可為一或多部電腦或其他裝置可執行的任何形式，像是程式模組。一般而言，程式模組包含執行特定工作或實施特定摘要資料類型的常式、程式、物件、組件、資料結構等。一般而言，程式模組的功能性可依各種具體實施例之需要而結合或分散。 [S]

另外，資料結構可以任何合適形式儲存在電腦可讀取媒體內。為了簡化例示，資料結構可顯示成與資料結構內所在位置相關的欄位。這種關係也可利用指派儲存空間給具有電腦可讀取媒體內位置的欄位(傳達欄位之間關係)來達成，不過任何合適的機制都可用來建立資料結構欄位內資訊之間的關係，包含透過使用指標、標籤或建立資料元件之間關係的其他機制。

本發明的各種態樣可單獨使用、組合使用或以上面說明具體實施例內未特別討論的各種配置來使用，因此並不將其應用限制於上述所揭示或圖式內所說明組件的細節與配置。例如：具體實施例內說明的態樣可用任何方式與其他具體實施例內說明的態樣結合。

另外，本發明可具體實施為一種方法，其中提供一種範例。屬於方法一部分所執行的動作可用任何合適方式排列，因此具體實施例可建構成其中用與所說明不同的順序來執行動作，這可包含同時執行某些動作，即使所說明具體實施例內顯示成依序動作也一樣。

申請專利範圍內使用「第一」、「第二」、「第三」等順序詞來修飾專利元件時並非暗示專利元件之間的任何優先順序、優先權或順序或執行方法的時間順序，而只是用來作為標示，以區隔具備特定名稱的一專利元件與具有相同名稱(要不是使用該順序詞)的其他專利元件，來[S]

區分各專利元件。

另外，此處所使用的措辭和用語係用來說明而非限制。此處所使用的「包含」、「包括」或「具有」、「內含」、「牽涉到」以及變型都用於涵蓋其後所列項目及其同等項以及附屬項。

【圖式簡單說明】

附圖並未依照比例繪製。在圖式當中，各圖內所圖示之一致或近乎一致的組件都用相同編號表示。為了清晰起見，圖內並非所有組件都會標示編號。圖式中：

第 1A 圖為內含多個安全指定位址空間的企業計算系統之略圖；

第 1B 圖為根據本發明某些具體實施例而可形成部分企業計算系統的安全指定位址空間之展開圖；

第 2A 圖為根據本發明某些具體實施例的階層金鑰產生之示意圖；

第 2B 圖為根據本發明某些具體實施例產生配對指定位址空間金鑰的程序流程圖；

第 3 圖為根據本發明某些具體實施例的指定位址空間發現與通訊協定之示意圖；

第 4A 圖和第 4B 圖以標示為 A 和 B 的點連接時，為操作安全指定位址空間內伺服器的程序流程圖；

第 5 圖為根據本發明某些具體實施例操作安全指定位址空間內用戶端的程序流程圖；

第 6 圖為根據本發明某些具體實施例操作中間裝置的程序流程圖；

第 7 圖為牽涉到中間裝置直接從伺服器接收金鑰期間，中間裝置與伺服器之間互動的處理流程圖；

第 8 圖為牽涉到中間裝置觸發安全相聯重新產生金鑰期間，中間裝置與伺服器之間互動的處理流程圖；

第 9A 圖為根據本發明某些具體實施例的伺服器之簡化示意圖；以及

第 9B 圖為根據本發明某些具體實施例可存在於中間裝置網路界面硬體內的記憶體結構之略圖。

【主要元件符號說明】

100 電腦系統
110A 指定位址空間
110B 指定位址空間
110C 指定位址空間
110D 指定位址空間
120A 伺服器
120B 伺服器
120C 伺服器
130 用戶端裝置
132 用戶端裝置
134 用戶端裝置
136 多埠裝置
140A 中間裝置
140B 中間裝置
140C 中間裝置
140D 中間裝置

[S]

148 組織金鑰伺服器

150 指定位址空間

160 指定位址空間金鑰伺服器

170A 伺服器

170B 伺服器

180 用戶端裝置

182 用戶端裝置

184 用戶端裝置

192 中間裝置

210 組織金鑰

224A 配對金鑰

224B 配對金鑰

224C 配對金鑰

224D 配對金鑰

220 擬亂函數

222 指定位址空間配對衍生輸入

230 擬亂密碼函數

232 伺服器金鑰衍生輸入

234A 伺服器金鑰

234B 伺服器金鑰

234C 伺服器金鑰

234D 伺服器金鑰

240 擬亂密碼函數

242 安全相聯金鑰衍生輸入

244A 金鑰

244B 金鑰

244C 金鑰

244D 金鑰

308 程序

310 控制封包

312 欄位

314 欄位

316 欄位

318 資訊元件

318'指示

320 控制封包

322 欄位

324 欄位

326 欄位

330 資訊元件

332 資訊元件

334 資訊元件

340 伺服器

350 用戶端

360 中間裝置

[S]

362 中間裝置

364 中間裝置

370 封包

372 欄位

374 欄位

376 欄位

380 伺服器 ID

910 裝置

920 網路界面硬體

922 網路

924 解密/驗證電路

926 記憶體

928 資料結構

928 資料表

930 安全相聯金鑰產生器

940 驅動器

950 作業系統

952 網路堆疊

958 資料表

960 應用程式

[S]

201135508

發明專利說明書

（本說明書格式、順序，請勿任意更動，※記號部分請勿填寫；惟已有申請案號者請填寫）

※ 申請案號：99114865

※ 申請日期：99 年 5 月 10 日　　※IPC 分類：G06F 21/00 (2006.01)
H04L 9/00 (2006.01)

一、發明名稱：（中文/英文）

在安全網路指定位址空間中的金鑰管理 / KEY MANAGEMENT IN SECURE NETWORK ENCLAVES

二、中文發明摘要：

本發明揭示一種用於電腦系統內的階層金鑰產生與散佈機制，其中裝置被組織成為安全指定位址空間。該機制可讓網路存取為了每一裝置而被裁剪，以逼近最小權限需求。在階層的最低等級上，使用金鑰形成裝置之間的安全相聯。每一階層等級上的金鑰都從較高階層等級上的金鑰以及金鑰衍生資訊來產生。金鑰衍生資訊可迅速從裝置識別碼或內含訊息來確定，支援密碼函數的硬體卸載。因為可根據參與安全相聯的主機所在之指定位址空間來產生金鑰，該系統包含一機制，讓裝置可發現其所在的指定位址空間。

三、英文發明摘要：

A hierarchical key generation and distribution mechanism for a computer system in which devices are organized into secure enclaves. The mechanism enables network access to be tailored to approximate minimum needed privileges for each device. At the lowest level of the

hierarchy, keys are used to form security associations between devices. Keys at each level of the hierarchy are generated from keys at a higher level of the hierarchy and key derivation information. Key derivation information is readily ascertainable, either from identifiers for devices or from within messages, supporting hardware offload of cryptographic functions. Because keys may be generated based on the enclaves in which the hosts participating in a security association are located, the system includes a mechanism by which devices can discover the enclave in which they are located.

[S]

七、申請專利範圍：

1. 一種操作一電腦系統來提供安全通訊之方法，該電腦系統包含複數個由一網路互連的主機裝置，並且組織成為指定位址空間，並且該方法包含以下步驟：

在該複數個指定位址空間的每一指定位址空間內，提供複數個配對指定位址空間金鑰，該複數個配對指定位址空間金鑰對應內含該指定位址空間之複數個指定位址空間配對中之每一者，而各包含一配對指定位址空間金鑰；

對複數個指定位址空間中之每一者，在至少一處理器內，為該指定位址空間內複數個伺服器裝置中之每一者計算複數個伺服器金鑰，該複數個伺服器金鑰中之每一者都從一配對指定位址空間金鑰所計算出，用於包含該伺服器的該指定位址空間之一對指定位址空間；

在該複數個指定位址空間的一第一指定位址空間內之一第一主機裝置與該複數個指定位址空間的一第二指定位址空間內之一第二主機裝置之間建立一安全相聯，該建立步驟包含以下步驟：

使用該第一主機裝置，產生該安全相聯的安全參數，該安全參數從被計算出來用於該第一主機裝置的該複數個伺服器金鑰中之一選取的伺服器金鑰來產[S]

生，該伺服器金鑰包含從一配對指定位址空間金鑰計算出的一伺服器金鑰，用於該第一指定位址空間和該第二指定位址空間。

2. 如申請專利範圍第 1 項所述之方法，其中在該複數個指定位址空間中之每一者內提供複數個配對指定位址空間金鑰之步驟，包含以下步驟：從一共用組織金鑰，產生該複數個配對指定位址空間金鑰給該複數個指定位址空間中之每一者。

3. 如申請專利範圍第 2 項所述之方法，其中：

該計算系統額外包含一組織金鑰伺服器；並且該方法另包含以下步驟：

驗證該複數個指定位址空間中之每一者內之一金鑰伺服器給該組織金鑰伺服器；以及

提供對一指定位址空間所產生的該複數個配對指定位址空間金鑰，給該指定位址空間內該金鑰伺服器，來回應已經驗證的該金鑰伺服器。

4. 如申請專利範圍第 1 項所述之方法，其中：

建立該安全相聯之步驟另包含以下步驟：執行該第一主機裝置與該第二主機裝置之間的一金鑰交換 [S]

協定。

5. 如申請專利範圍第4項所述之方法，進一步包含以下步驟：

在該第一主機裝置的網路界面硬體內：

儲存該選取的伺服器金鑰；

使用該安全相聯接收一封包後，即產生該安全相聯的該安全參數；以及

使用該產生的安全參數執行一密碼函數於該封包上。

6. 如申請專利範圍第5項所述之方法，其中：

該第一主機裝置與該計算系統內其他主機形成複數個安全相聯；

該方法另包含以下步驟：儲存複數個伺服器金鑰，該複數個伺服器金鑰中之每一者都從一配對指定位址空間金鑰中衍生，並且每一者都關聯於複數個安全相聯；

在使用該安全相聯接收一封包後，即產生該安全相聯的該安全參數之步驟包含以下步驟：基於該封包內的資訊，選擇該複數個伺服器金鑰中的一伺服器金鑰，並且使用該選取的伺服器金鑰以及該封包內資

訊，產生該安全參數。

7. 如申請專利範圍第 1 項所述之方法，其中：

該計算系統包含至少一中間裝置，該中間裝置連接在該底一主機裝置與該第二主機裝置之間一網路路徑內；並且該方法另包含以下步驟：

提供具有複數個配對指定位址空間金鑰的該中間裝置；

使用該安全相聯偵測到一封包後，即使用該複數個配對指定位址空間金鑰的一配對指定位址空間金鑰來產生該安全相聯的該安全參數；以及

使用該產生的安全參數執行一密碼函數於該封包上。

8. 如申請專利範圍第 7 項所述之方法，其中：

該複數個指定位址空間中之每一者都包含一金鑰伺服器；

產生一伺服器金鑰給一伺服器。

9. 如申請專利範圍第 8 項所述之方法，其中

提供複數個配對指定位址空間金鑰之步驟包含以下步驟：

[S]

對每一指定位址空間提供一指定位址空間金鑰；以及

使在該複數個指定位址空間中之每一者內的該等金鑰伺服器在該網路上互動，該互動之步驟包含以下步驟：對該複數個指定位址空間的複數個指定位址空間配對中之每一者，產生一配對指定位址空間金鑰。

10. 一種操作一計算裝置來在一計算系統內提供安全通訊之方法，該計算系統包含複數個由一網路互連的主機裝置並且組織成為指定位址空間，每一指定位址空間包含至少一主機裝置，該方法包含以下動作：

在一計算裝置內：

偵測一第一指定位址空間內一第一主機與一第二指定位址空間內一第二主機之間依照該第一主機與該第二主機之間一安全相聯來傳輸的一訊息；

基於該訊息內金鑰衍生資訊以及用於該第一指定位址空間和該第二指定位址空間的一配對指定位址空間金鑰，產生一安全相聯金鑰；

使用該產生的安全相聯金鑰執行一密碼函數於該訊息上。

[S]

11. 如申請專利範圍第 10 項所述之方法，其中：

該計算裝置包含網路界面硬體；以及

偵測、產生和執行一密碼函數之該等動作都在該網路界面硬體內執行。

12. 如申請專利範圍第 11 項所述之方法，其中：

該網路硬體具有電腦儲存媒體，其儲存著複數個配對指定位址空間金鑰；以及

該方法包含以下動作：基於該金鑰衍生資訊，從該電腦儲存媒體內該複數個配對指定位址空間金鑰選擇該配對指定位址空間金鑰。

13. 如申請專利範圍第 12 項所述之方法，其中：

產生該安全相聯金鑰之動作，包含以下動作：

從該選取的配對指定位址空間金鑰以及該金鑰衍生資訊內一伺服器識別碼來產生一伺服器金鑰；以及

從該產生的伺服器金鑰以及一安全相聯的一識別碼中產生該安全相聯金鑰。

14. 如申請專利範圍第 13 項所述之方法，其中：

產生該伺服器金鑰之動作包含以下動作：執行一

[S]

單向加密操作於該選取的配對指定位址空間金鑰以及該金鑰衍生資訊內該伺服器識別碼上；以及

產生該安全相聯金鑰之動作包含以下動作：執行一單向加密操作於該產生的伺服器金鑰以及該安全相聯的該識別碼上。

15. 如申請專利範圍第 14 項所述之方法，其中該密碼函數包含解密該訊息之動作。

16. 一種操作一計算系統來提供安全通訊之方法，該計算系統包含複數個由一網路互連的主機裝置並且組織成為指定位址空間，並且該方法包含以下動作：

對該複數個指定位址空間的每一指定位址空間，提供複數個配對指定位址空間金鑰；以及

在該複數個指定位址空間的一第一指定位址空間內之一第一主機裝置與該複數個指定位址空間的一第二指定位址空間內之一第二主機裝置之間建立一安全相聯，該建立之動作包含以下動作：

產生一配對指定位址空間給該第一指定位址空間和該第二指定位址空間；以及

使用該第一主機裝置，產生該安全相聯的安全參數，該產生動作包含以下動作：

[S]

從該配對指定位址空間金鑰以及與該第一主機相關聯的一伺服器識別碼來產生一伺服器金鑰；

從該伺服器金鑰以及用於該安全相聯的一金鑰衍生值來產生一安全相聯金鑰；

以及將該安全參數通訊至該第二主機裝置。

17. 如申請專利範圍第 16 項所述之方法，其中：

產生該伺服器金鑰之動作包含以下動作：執行一單向加密操作於該配對指定位址空間金鑰以及該第一指定位址空間中一金鑰伺服器內該伺服器識別碼上；以及

產生該安全相聯金鑰之動作包含以下動作：執行一單向加密操作該伺服器金鑰以及該安全相聯上。

18. 如申請專利範圍第 16 項所述之方法，進一步包含以下動作：

在與該第一主機裝置相關聯的網路界面硬體內：

使用該安全相聯接收來自該第二主機裝置的一訊息，該接收的訊息包含金鑰衍生資訊；

使用之前從用於該第一指定位址空間和該第二指定位址空間的該配對指定位址空間金鑰產生之一 [S]

伺服器金鑰，以及該訊息內的金鑰衍生資訊，再生該安全相聯參數；以及

使用該再生的安全相聯參數執行一密碼函數於該訊息內的資訊上。

19. 如申請專利範圍第 18 項所述之方法，進一步包含以下動作：

在與連接在該第一主機裝置與該第二主機裝置之間該網路內的一中間裝置相關聯之網路界面硬體內：

使用該安全相聯偵測從該第二主機裝置到該第一主機的一訊息，該偵測的訊息包含金鑰衍生資訊；

使用用於該第一指定位址空間和該第二指定位址空間的該配對指定位址空間金鑰以及該訊息內的金鑰衍生資訊，再生該等安全相聯參數；以及

使用該等再生的安全相聯參數執行一密碼函數於該訊息內的資訊上。

20. 如申請專利範圍第 16 項所述之方法，進一步包含以下動作：

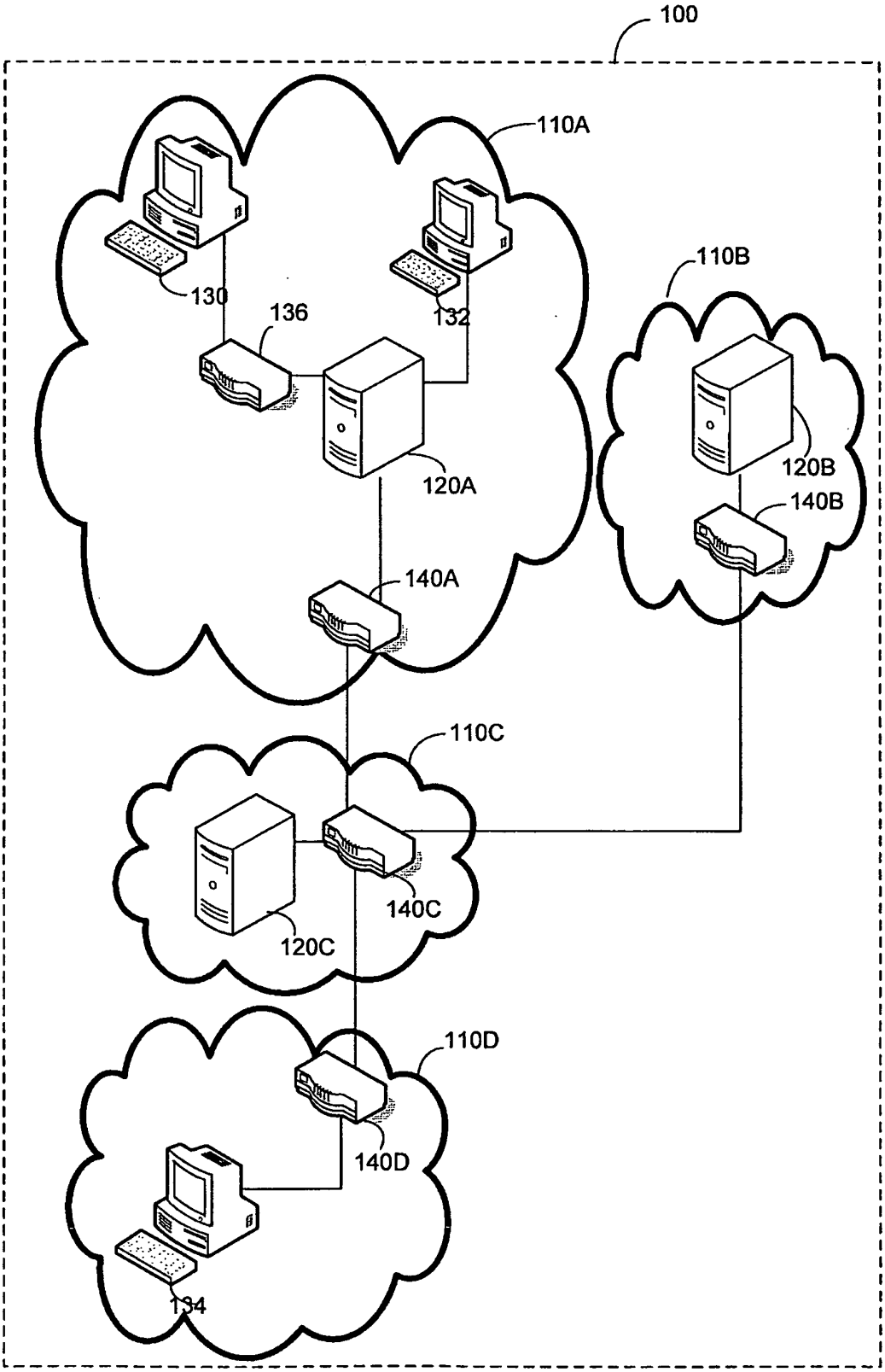
在該第一主機上，接收來自該第二主機的一訊息，該訊息包含一標記，該標記指出一中間裝置缺乏 [S]

資訊來使用該安全相聯監控訊息；以及

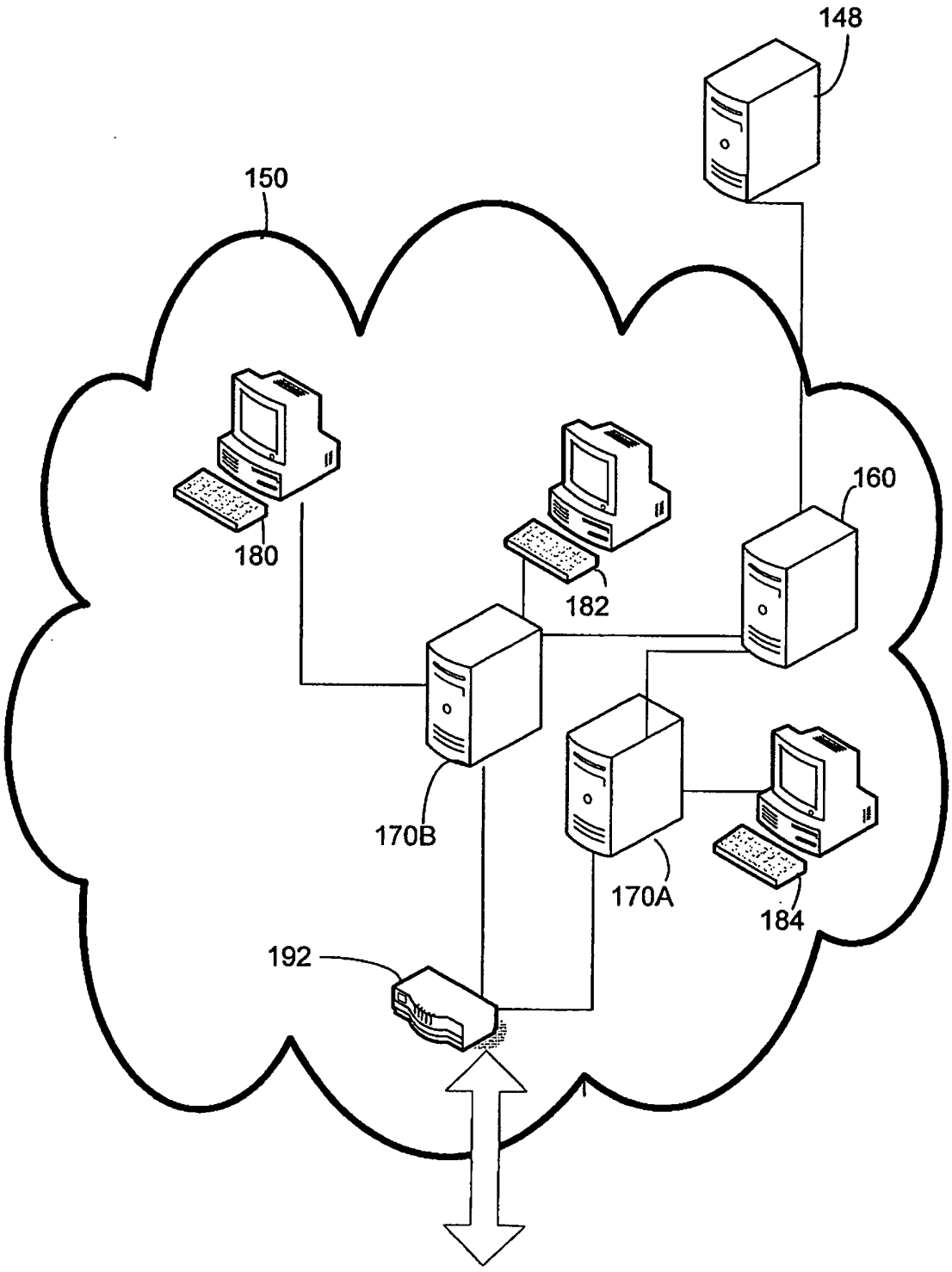
回應該指示，而重複在該第一主機與該第二主機之間建立該安全相聯之該動作。

[S]

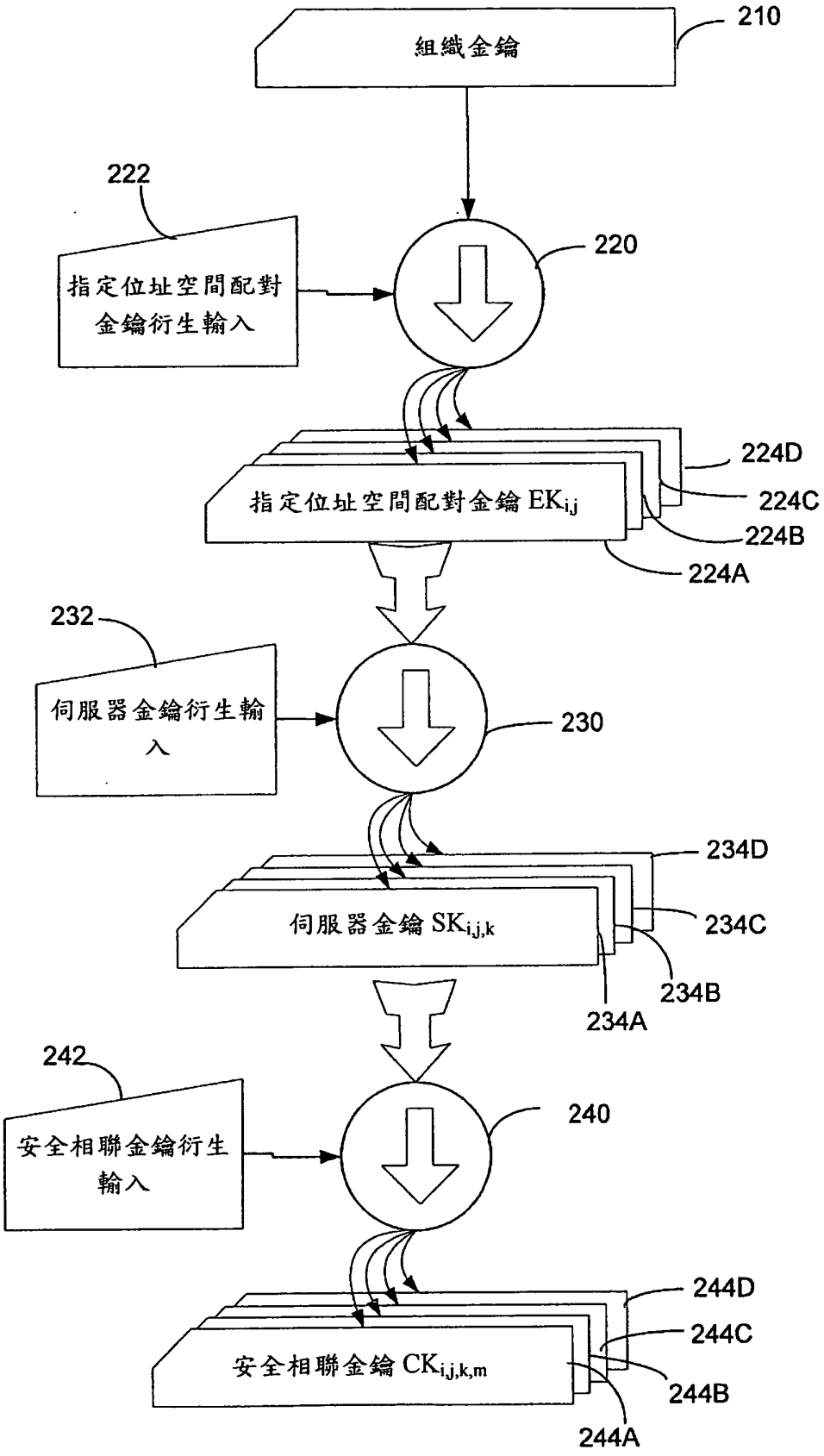
八、圖式：


100
110A
130
136
132
120A
110B
120B
140B
140A
110C
140C
120C
110D
140D
134

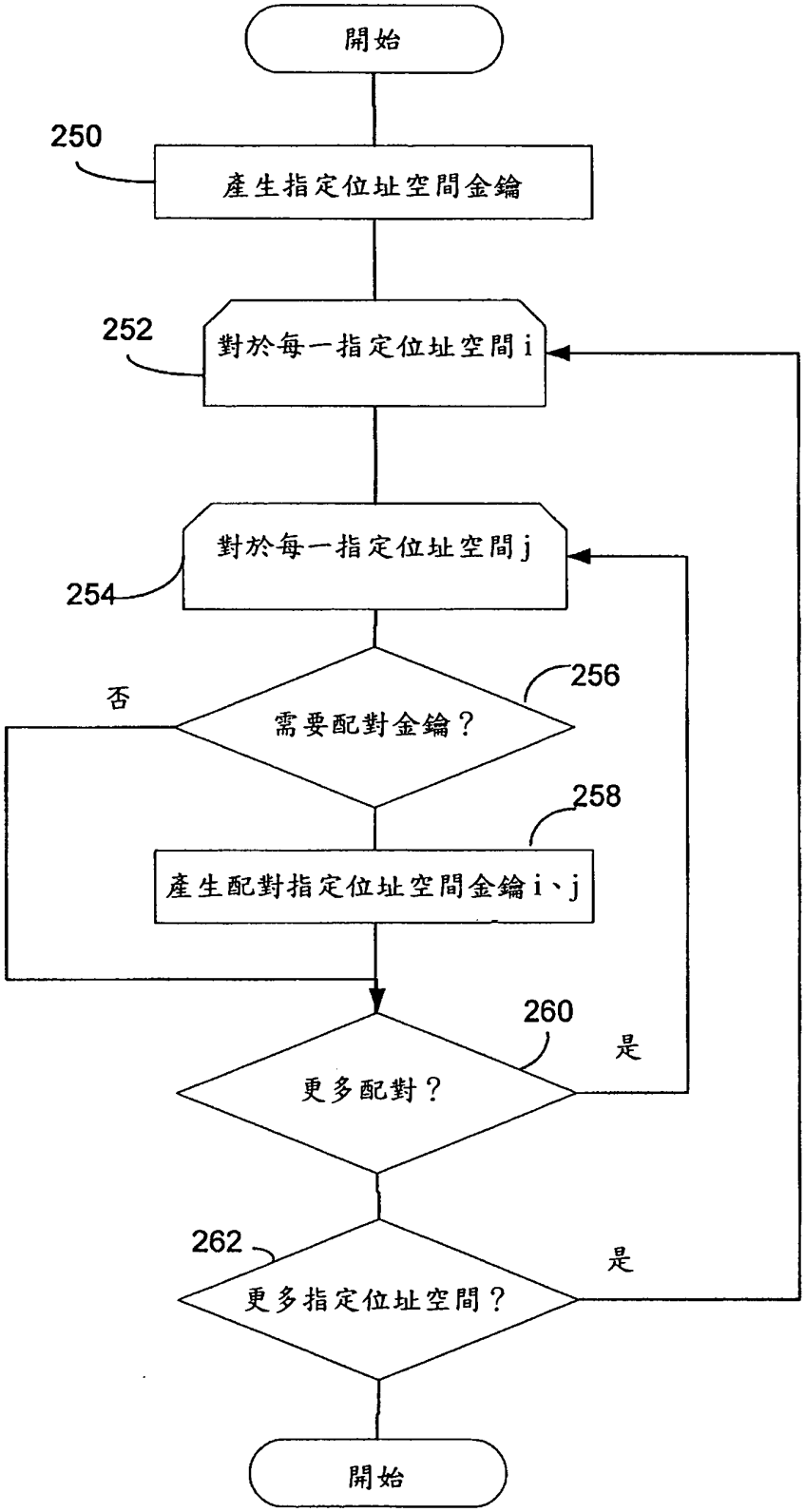
第 1A 圖



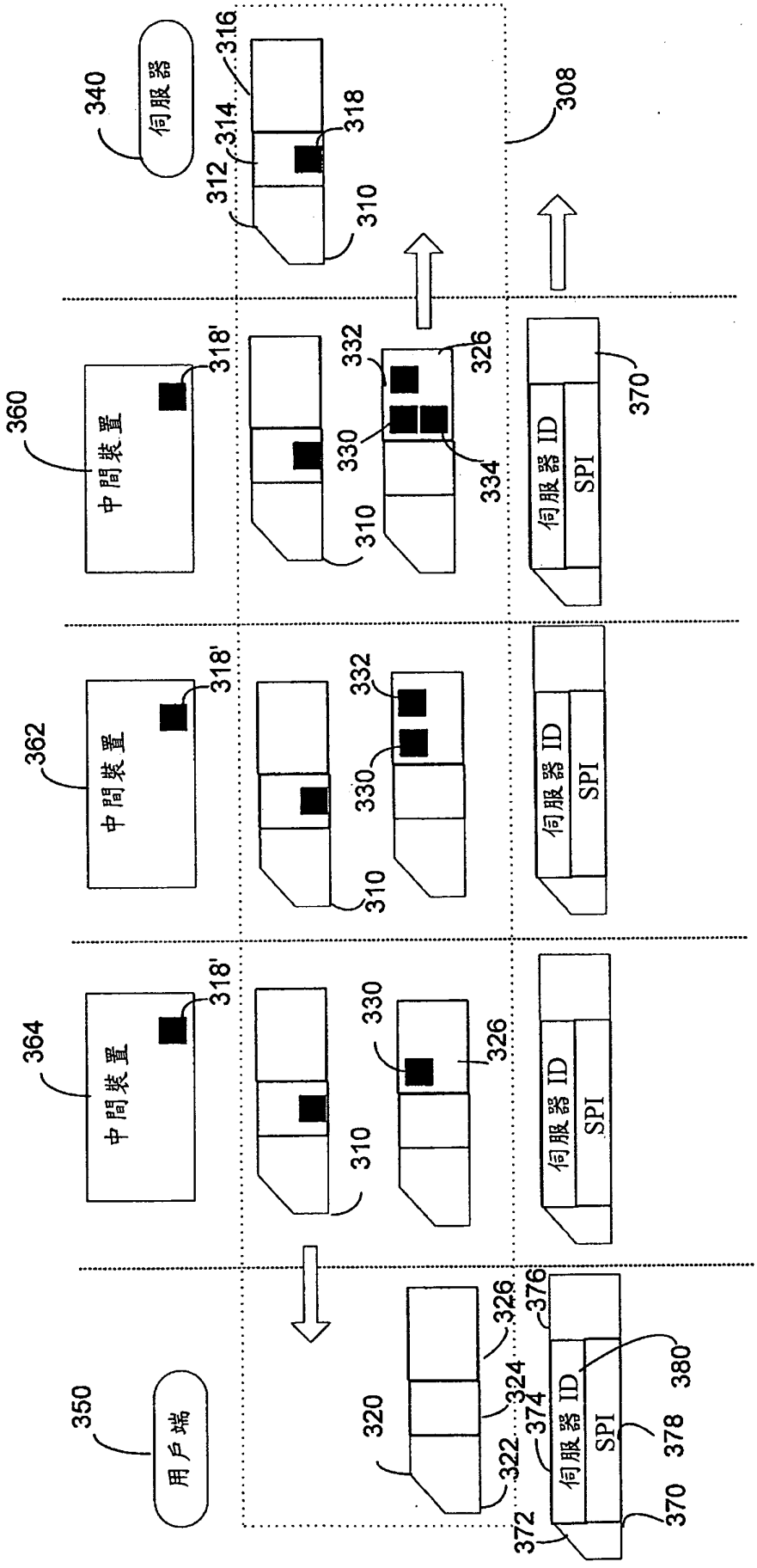
第 1B 圖


組織金鑰
210
222
指定位址空間配對金鑰衍生輸入
220
指定位址空間配對金鑰 $EK_{i,j}$
224D
224C
224B
224A
232
伺服器金鑰衍生輸入
230
伺服器金鑰 $SK_{i,j,k}$
234D
234C
234B
234A
242
安全相聯金鑰衍生輸入
240
安全相聯金鑰 $CK_{i,j,k,m}$
244D
244C
244B
244A

第 2A 圖

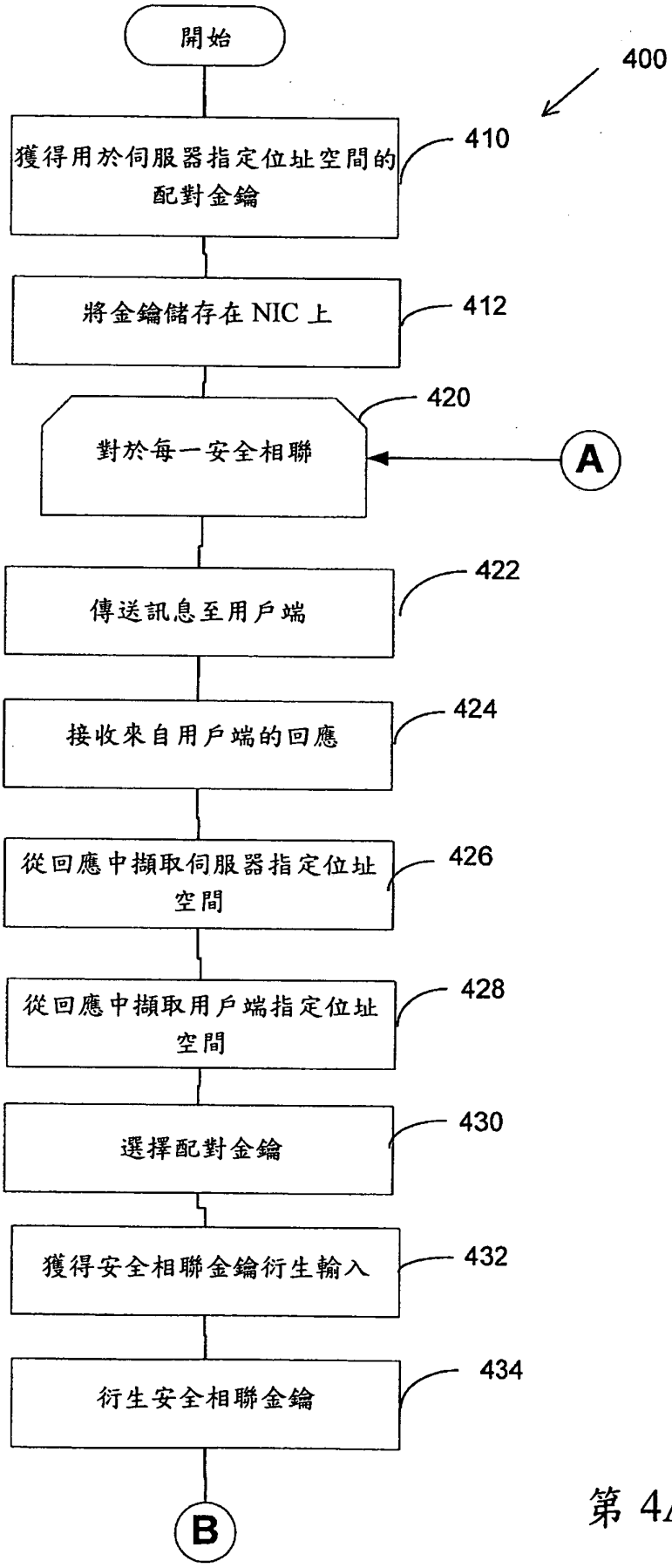

開始
250
產生指定位址空間金鑰
252
對於每一指定位址空間 i
對於每一指定位址空間 j
254
256
否
需要配對金鑰？
258
產生配對指定位址空間金鑰 i、j
260
是
更多配對？
262
是
更多指定位址空間？
開始

第 2B 圖


340
伺服器
316
314
318
312
310
308
360
中間裝置
318'
332
326
330
334
310
伺服器 ID
SPI
370
362
中間裝置
318'
332
330
310
伺服器 ID
SPI
364
中間裝置
318'
330
326
310
伺服器 ID
SPI
350
用戶端
326
376
320
324
374
380
伺服器 ID
SPI
378
322
370
372

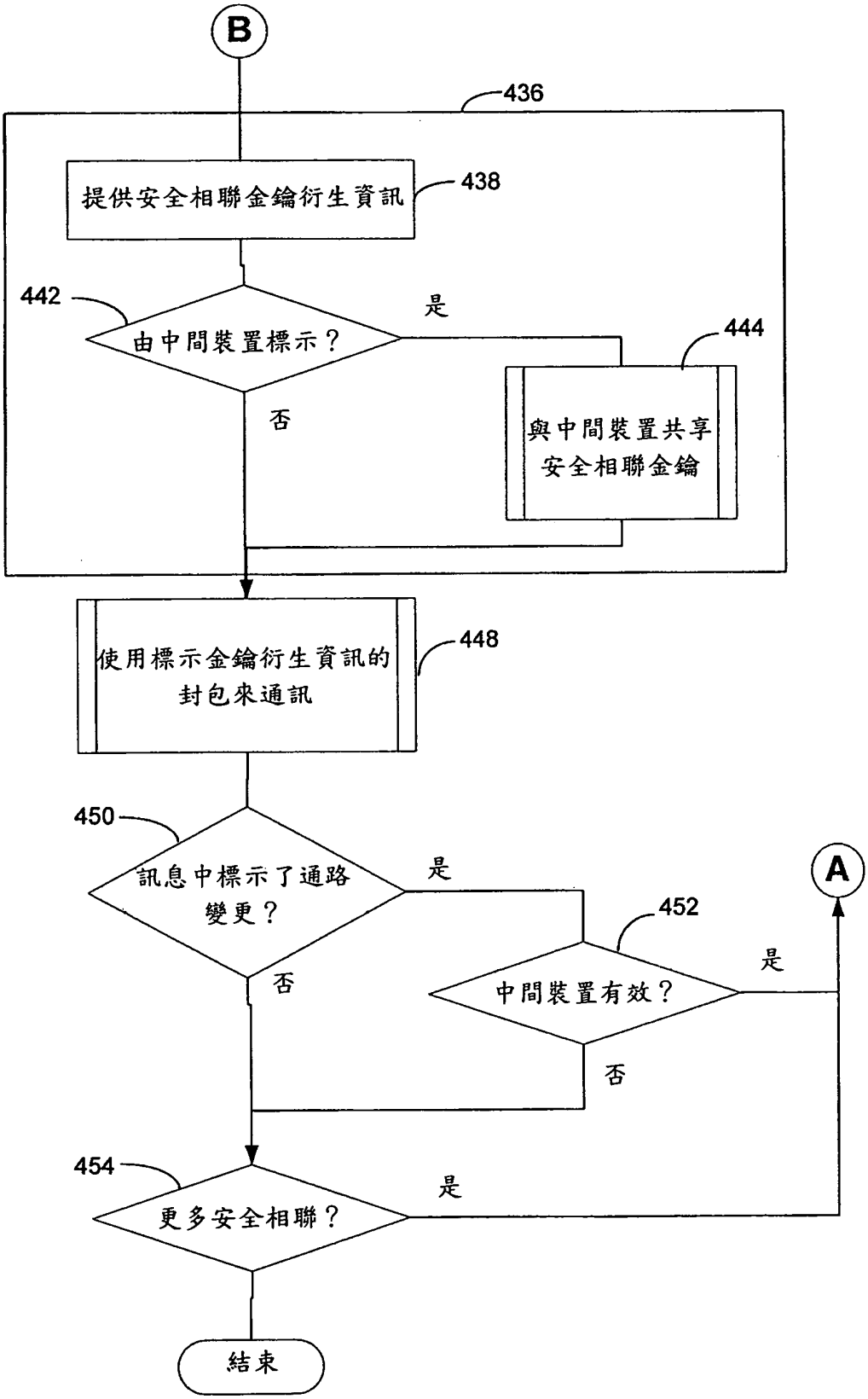
第 3 圖

[S]

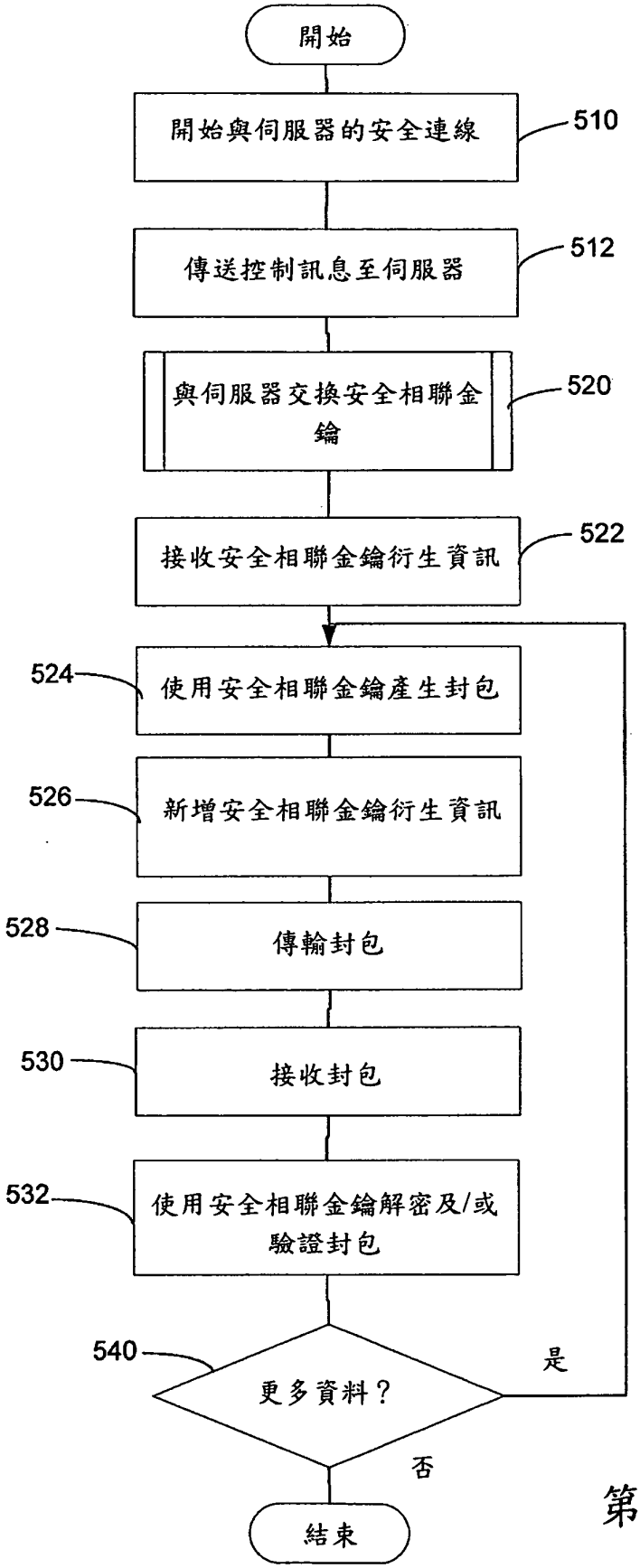

開始
400
獲得用於伺服器指定位址空間的配對金鑰
410
將金鑰儲存在 NIC 上
412
對於每一安全相聯
420
A
傳送訊息至用戶端
422
接收來自用戶端的回應
424
從回應中擷取伺服器指定位址空間
426
從回應中擷取用戶端指定位址空間
428
選擇配對金鑰
430
獲得安全相聯金鑰衍生輸入
432
衍生安全相聯金鑰
434
B

第 4A 圖

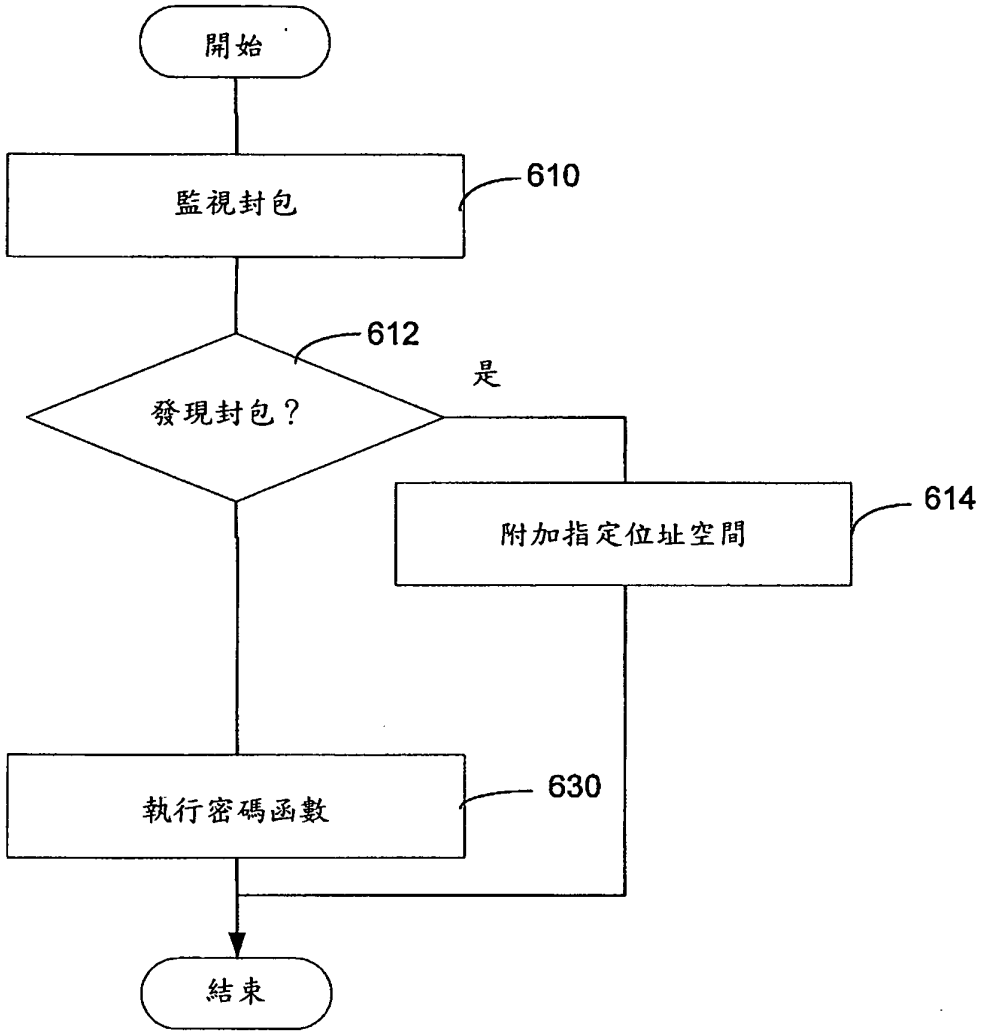
[S]


B
436
提供安全相聯金鑰衍生資訊
438
442
由中間裝置標示？
是
444
與中間裝置共享安全相聯金鑰
否
使用標示金鑰衍生資訊的封包來通訊
448
450
訊息中標示了通路變更？
是
A
452
中間裝置有效？
是
否
否
454
更多安全相聯？
是
結束

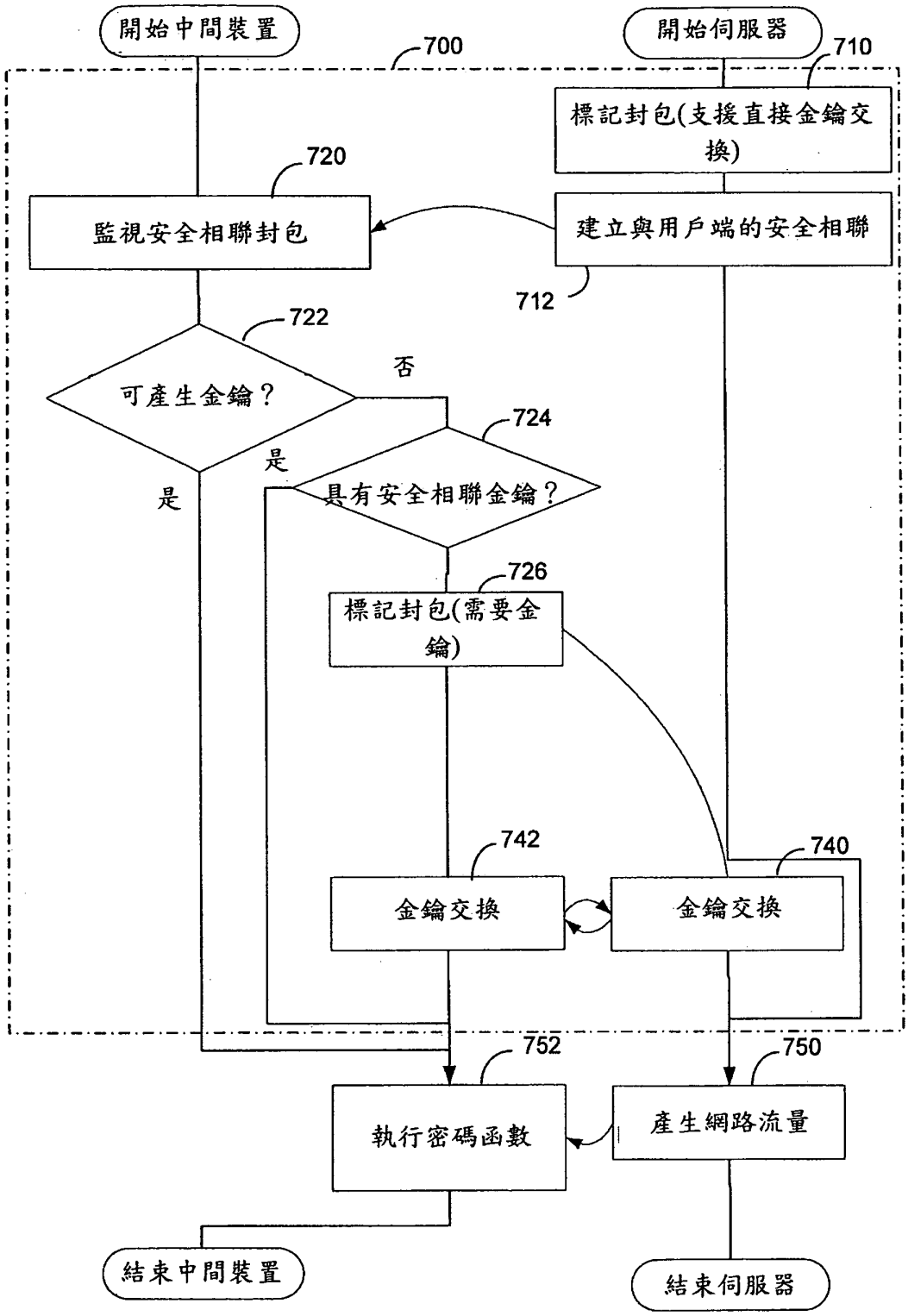
第 4B 圖


開始
開始與伺服器的安全連線
510
傳送控制訊息至伺服器
512
與伺服器交換安全相聯金鑰
520
接收安全相聯金鑰衍生資訊
522
524
使用安全相聯金鑰產生封包
526
新增安全相聯金鑰衍生資訊
528
傳輸封包
530
接收封包
532
使用安全相聯金鑰解密及/或驗證封包
540
更多資料？
是
否
結束

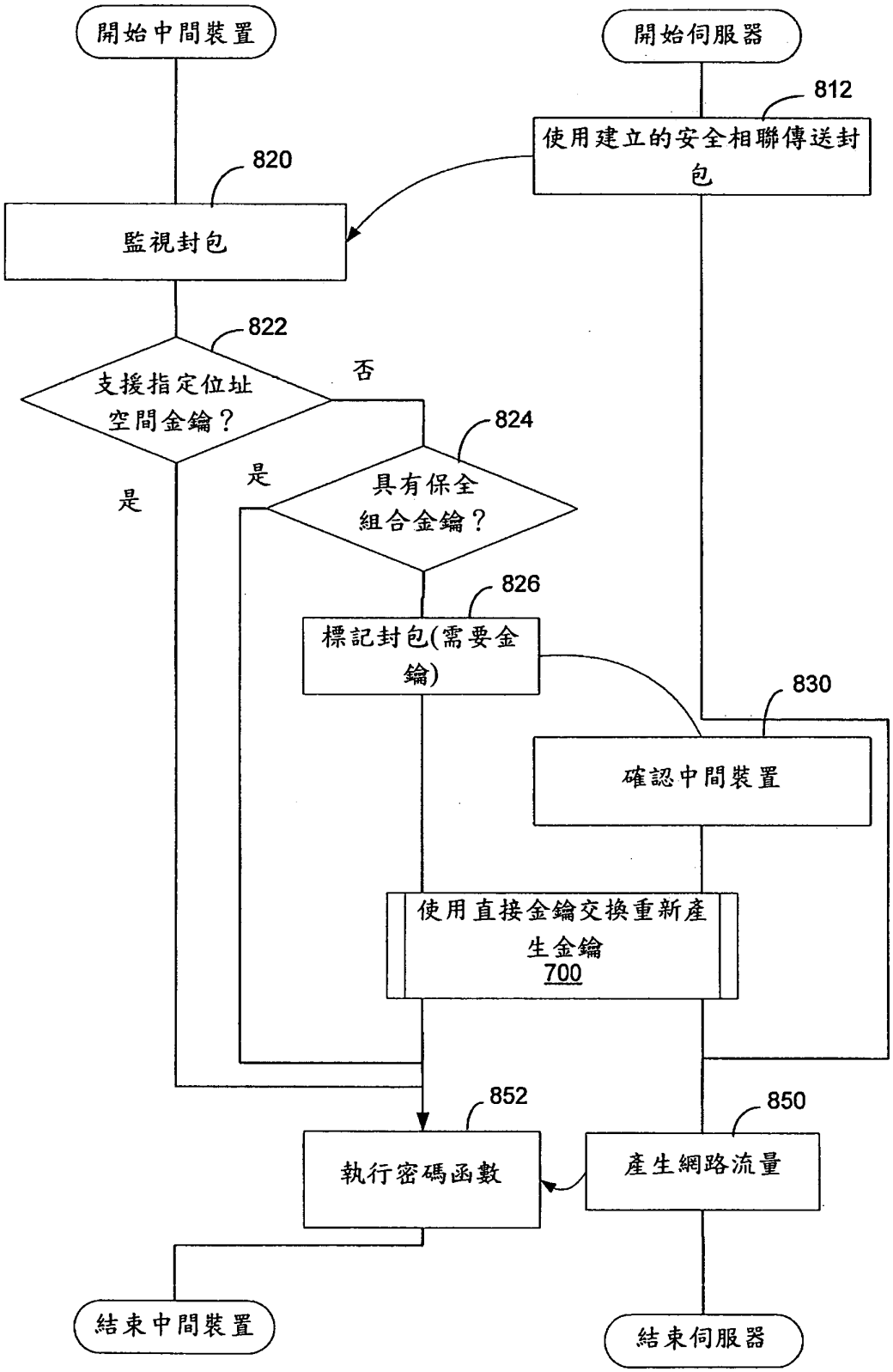
第 5 圖



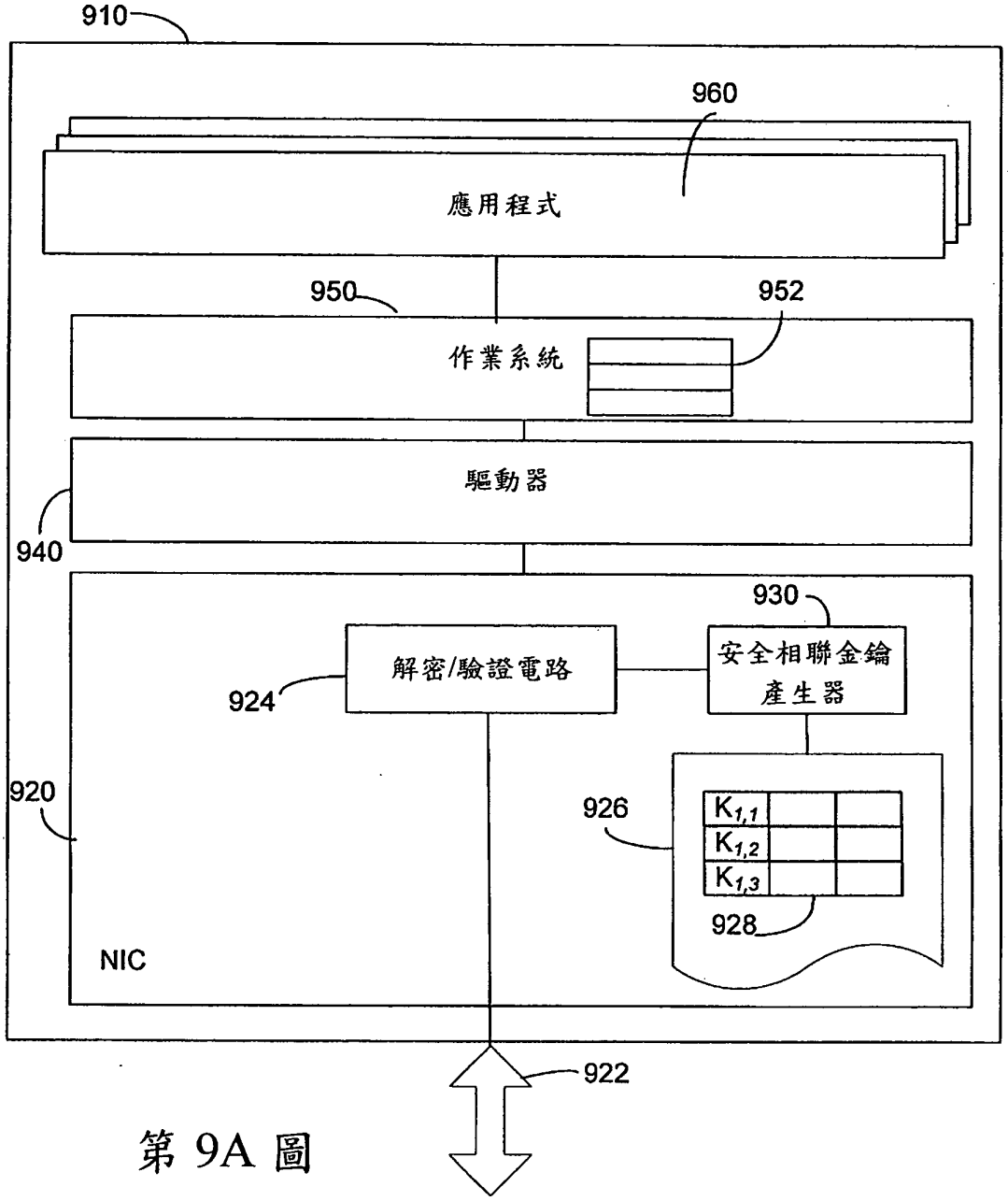
第 6 圖


開始中間裝置
開始伺服器
700
710
標記封包(支援直接金鑰交換)
720
監視安全相聯封包
建立與用戶端的安全相聯
712
722
可產生金鑰？
否
724
是
具有安全相聯金鑰？
是
726
標記封包(需要金鑰)
742
740
金鑰交換
金鑰交換
752
750
執行密碼函數
產生網路流量
結束中間裝置
結束伺服器

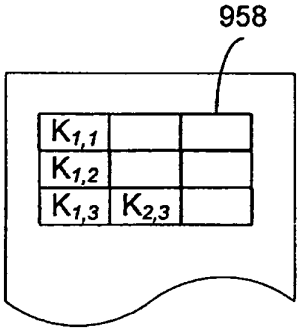
第 7 圖


開始中間裝置
開始伺服器
812
使用建立的安全相聯傳送封包
820
監視封包
822
支援指定位址空間金鑰？
否
是
是
824
具有保全組合金鑰？
826
標記封包(需要金鑰)
830
確認中間裝置
使用直接金鑰交換重新產生金鑰
700
852
850
執行密碼函數
產生網路流量
結束中間裝置
結束伺服器

第 8 圖


910
960
應用程式
950
952
作業系統
驅動器
940
930
解密/驗證電路
安全相聯金鑰產生器
924
920
926
$K_{1,1}$
$K_{1,2}$
$K_{1,3}$
928
NIC
922

第 9A 圖


958
$K_{1,1}$
$K_{1,2}$
$K_{1,3}$
$K_{2,3}$

第 9B 圖

四、指定代表圖：

(一)本案指定代表圖為：第（2A）圖。

(二)本代表圖之元件符號簡單說明:

210 組織金鑰

220 擬亂函數

222 指定位址空間配對衍生輸入

224A 配對金鑰

224B 配對金鑰

224C 配對金鑰

224D 配對金鑰

230 擬亂密碼函數

232 伺服器金鑰衍生輸入

234A 伺服器金鑰

234B 伺服器金鑰

234C 伺服器金鑰

234D 伺服器金鑰

240 擬亂密碼函數

242 安全相聯金鑰衍生輸入

244A 金鑰

244B 金鑰

244C 金鑰

244D 金鑰

[S]

五、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

[S]