公告本

I234975

申請日期	91.7.16
案號	91115809
類別	H04L 9/00

A4
C4

（以上各欄由本局填註）

發明 新型 專利說明書

一、發明 新型 名稱	中文	用於在具有複數個保密通道之高速系統中解決保密結合資料庫更新整合之設備及方法
	英文	APPARATUS AND METHOD FOR RESOLVING SECURITY ASSOCIATION DATABASE UPDATE COHERENCY IN HIGH-SPEED SYSTEMS HAVING MULTIPLE SECURITY CHANNELS
二、發明 創作 人	姓名	(1)夏德 W. 默塞 (2)李 P. 諾倫 (3)史地夫 J. 布朗
	國籍	美國
	住、居所	(1)美國亞利桑納州 85296 吉伯特東罕普敦巷 287 號 (2)美國亞利桑納州 85310 葛林代爾北 67 路 22415 號 (3)美國亞利桑納州 85044 鳳凰城東烏特街 4412 號
三、申請人	姓名（名稱）	可倫特公司
	國籍	美國
	住、居所（事務所）	美國亞利桑納州 85284 天普市西綠林路 201 室 1711 號
	代表人 姓名	李察 J. 高橋

裝 訂 線

（由本局填寫）

承辦人代碼：	
大　　類：	
ＩＰＣ分類：	

A6
B6

本案已向：

國（地區）	申請專利，申請日期：	案號：	，☑有 □無主張優先權
美	2001.08.03	09/921,677	

有關微生物已寄存於：　　，寄存日期：　　，寄存號碼：

（請先閱讀背面之注意事項再填寫本頁各欄）

裝 訂 線

五、發明說明（ 1 ）

發明背景

發明之領域

本發明係關於在具有複數個通道之系統中解決資料庫更新整合之設備及方法。且尤其係關於在具有複數個保密通道之高速系統中解決保密結合資料庫更新整合之設備及方法。

相關先前技藝之描述

透過一個諸如網際網路之互連電腦網路而被轉移之資料係易遭受到許多形式之攻擊。這些攻擊可以造成諸如隱密漏失、資料整體性漏失、身份失竊、拒絕服務或者這些攻擊之任意組合之情事。用於保密通訊、電子商務及許多其他交易之網際網路的曾經廣泛流行係導致透過類似網際網路之非保密互連電腦網路對於如此之攻擊係安全的之通訊之需求。

爲了強調上述關切事項，該所謂的“網際網路工程特遣隊（Internet Engineering Task Force，IETF）”係發展一個用於確保透過網際網路之私密通訊的穩密性、完整性及驗證性之開放標準的架構。該標準架構係爲熟悉本項技藝人士所知之網際網路保密協定（Internet Security Protocol，IPSec）。該網際網路保密協定係於一個系統之網際網路層提供保密服務,且允許一個系統選擇需要的保密協定，決定使用之保密資料的演算法，及實施提供該保密服務所需之任何密碼密鑰。因爲這些保密服務係於該網際網路層之

五、發明說明（ㄚ）

內實施，所以該網際網路保密協定服務係可以由任何較商層之協定所使用，諸如傳輸控制協定（Transmission Control Protocol），使用者資料包協定（User Datagram Protocol），網際網路控制訊息協定（Internet Control Message Protocol），邊界閘路器協定（Border Gateway Protocol），或者許多其他熟悉本項技藝人士已知之協定。網際網路保密協定係能夠被使用於建立主電腦之間、諸如一個路由器或者防火牆之保密閘路器之間或者主電腦及保密閘路器之間之一或多個保密通訊通道。

如同熟悉本項技藝人士所知，網際網路資料係通過一個互連之電腦網路而作爲個別的資料封包，俗稱爲網際網路資料包。該網際網路保密協定係提供一組新的網際網路保密協定標頭，其係被加入至網際網路資料包之中。該新的網際網路保密協定標頭係格外提供關於當網際網路資料包酬載係通過一個互連之電腦網路時用於保密該網際網路資料包酬載之保密協定之資訊。這些保密協定係被認知爲驗證標頭（Authentication Header）及密封保密酬載（Encapsulating Security Payload）。該驗證標頭保密協定係提供無連接之完整性，資料原始驗證，及一個可選擇之反重來服務，且係使用協定號碼５１而予以表示。該密封保密酬載保密協定係提供私密性，完整性，資料原始驗證，及一個可選擇之反重來服務，且係使用協定號碼５０而予以表示。該驗證標頭保密協定及該密封保密酬載保密協定係能夠獨立地使用或者彼此組合，以提供一個期望之保密

五、發明說明（ 7 ）

服務組。

對於該網際網路保密協定之使用及瞭解之基本係爲保密結合（Security Association）。一般而言，一個保密結合係爲兩個或更多個裝置之間之關係，其敘述該些裝置係如何使用網際網路保密協定保密服務，以彼此作保密通訊。一個保密結合係爲單向的。因此，爲了保密於一個互連之電腦網路中之兩個節點之間之雙向通訊通道，係需要兩個保密結合，每一個方向係使用一個保密結合。這些個別的保密通訊通道係稱爲一個“入站隧道”及“出站隧道”，其中，一個裝置之入站隧道係爲另一個裝置之出站隧道，且反之亦然。

一個裝置之所有主動保密結合係被儲存於一個中央化之資料庫而作爲保密結合資料結構，該中央化之資料庫係稱爲保密結合資料庫（Security Association Database）。因此，每一個入站及出站之主動保密結合係於該保密結合資料庫中具有一個入口。當一個裝置係傳送一個需要網際網路保密協定保護之網際網路協定封包時，傳輸該被保護之網際網路協定資料包之該裝置將於該保密結合資料庫中定位一個適當的保密結合的入口，更新該保密結合資料庫之入口，及根據位於該封包保密結合資料庫內之該保密結合而處理，諸如加密及／或驗證，該封包。然後，該加密之封包係透過諸如一個網路處理器而被傳輸至該非保密網路。類似地，當一個裝置係接收一個被保護之網際網路協定資料包時，該接收裝置係於該保密結合資料庫中定位一

五、發明說明（4）

個適當的保密結合的入口，根據位於該封包保密結合資料庫內之該保密結合而處理該封包，及更新該保密結合資料庫之入口。

保密資料傳輸及處理之目標係爲較高及更高之速度。因此，所實施之裝置係包含複數個處理通道，每一個處理通道係能夠處理複數個封包。有可能的情況爲，於該些複數個通道系統內之個別通道係可能需要同時存取相同的保密結合資料庫。如上所述，保密結合資料庫之入口的更新係爲網際網路保密協定處理之一部分，其係於該網際網路保密協定資料包之入站及出站處理期間產生。因此，假如兩個或更多個通道同時存取相同的保密結合資料庫的入口時，這些相同的通道可能企圖同時或者實質上同時更新該相同之保密結合資料庫之入口。假如此情況產生，則某些保密結合資料庫之入口的更新係將漏失，其係能夠造成一個保密之危害。雖然用於解決如此一致性問題之複雜的演算法及裝置係爲熟悉本項技藝人士所熟知，然而這些已知之演算法及裝置係複雜的，且相反地影響系統之效能。

因此，係需要一種解決上述無效率之設備及方法。亦即，一個解決保密結合資料庫之入口更新一致性問題而不必依賴複雜的演算法或裝置之設備及方法。此外，亦需要一個解決保密結合資料庫之入口更新一致性問題而不會對於網際網路保密協定之交通導入相當大的延遲之設備及方法。

五、發明說明（ 5 ）

發明概要

本發明係提供一種用於在具有複數個保密通道之系統中更新網際網路保密協定之保密結合資料庫入口之設備及方法，其係藉由選擇性地允許複數個多重保密通道對於保密結合資料庫之存取而達成，其係可以使用一個先進先服務之機制而更新該相同的保密結合資料庫之入口。

於本發明之一個觀點中，其係提供一種修改保密結合資料庫中之入口的方法，該保密結合資料庫係於一個具有複數個保密通道之系統中，該方法係結合每一個頻道，該方法係包含下列步驟：決定是否該複數個保密通道之另一個係具有存取位於該保密結合資料庫中之一個預定位址位置之一個保密結合資料結構的較高優先權。當無其他保密通道係具有較高之優先權而實施存取該保密結合資料結構時，該保密結合資料結構係由該預定位址位置取出。該取出之保密結合資料結構係被修改，且被寫入至該保密結合資料庫內之該預定位址位置。

根據本發明之另一個觀點，本發明係提供一種用於管理對於一個保密結合資料庫中之一個入口之存取的控制器，其係於一個具有複數個保密通道之系統中，該控制器係包含一個暫存器電路及一個仲裁器電路。該暫存器電路係包含複數個第一暫存器，該複數個第一暫存器之每一個係個別地與該複數個保密通道之一個作通訊，且該複數個第一暫存器之每一個係可操作於接收由其結合之保密通道而來之一個請求，以取得位於該保密結合資料庫中之一個預

五、發明說明（ b ）

定位址處之一個保密結合資料結構。該仲裁器電路係與該暫存器電路之每一個作通訊，且係可操作於（i）優先權化由該複數個第一暫存器之每一個所接收而來之該取得的請求爲最高優先權至最低優先權，及（ii）允許該取得之請求傳送至具有最高優先權之保密通道。

根據本發明之又另一個觀點，本發明係提供一種用於管理對於一個保密結合資料庫中之一個入口之存取的控制器，其係於一個具有複數個保密通道之系統中，該控制器係包含一個加權控制邏輯電路，一個允許樹邏輯電路及一個允許邏輯電路。該加權控制邏輯電路係可操作於指定一個加權值至該控制器由該複數個保密通道所接收而來之取得的請求。該允許樹邏輯電路係連接至該加權控制邏輯電路，且係可操作於（i）決定哪一個取得請求係具有一個最高加權值；及（ii）對於該取得請求以該最高加權值產生一個允許訊號。該允許邏輯電路係連接成接收由該允許樹邏輯電路而來之該允許訊號，且回應於該允許訊號，允許該取得請求給具有該最高加權值之該保密通道。

圖式簡單說明

第 1 圖係一個說明透過一個互連電腦網路而通訊之許多電腦之功能方塊圖；

第 2 圖係說明一個網際網路資料包之一般結構；

第 3 圖係說明用於隧道模式操作之一個網際網路保密協定資料包之一般結構；

五、發明說明（ 7 ）

第 4 圖係說明用於傳輸模式操作之網際網路保密協定之一般結構；

第 5 圖係說明被儲存作爲一個保密結合資料庫中之一個入口的出站保密結合資料結構之一個範例；第 6 圖係說明被儲存作爲一個保密結合資料庫中之一個入口的入站保密結合資料結構之一個範例；第 7 圖係說明根據本發明之一個實施例之使用於具有複數個保密通道之電腦系統中之該內部網際網路保密協定處理硬體之一部分的方塊圖；

第 8 圖係爲根據本發明之一個實施例之一個訊號控制器之功能方塊圖；及

第 9 圖係一個說明用於更新具有複數個保密通道之系統中之保密結合資料庫之入口的程序之流程圖。

〔元件符號說明〕

100	系統
102	第一本地網路
104	第二本地網路
106	非保密電腦網路
108－1，108－2，108－3，...108－N	第一個別電腦工作站
110	第一閘路器電腦
112－1，112－2，112－3，...112－N	第二個別電腦工作站
114	第二閘路器電腦
116	保密結合資料庫
118	保密結合資料庫

五、發明說明（ 8 ）

200	網際網路協定資料
202	網際網路協定標頭部分
204	上層協定標頭
206	資料酬載
300	網際網路保密協定資料包
302	網際網路協定標頭部分
304	網際網路保密協定標頭部分
306	加密及／或驗證酬載部分
400	網際網路保密協定資料包
402	網際網路協定標頭部分
404	網際網路保密協定標頭部分
406	加密及／或驗證酬載部分
500	出站保密結合資料結構
502	保密結合序列數域
503	保密結合硬位元組壽命域
504	保密結合目前位元組計數域
505	保密結合硬時間壽命域
506	8位元密鑰域
507	保密結合軟位元組壽命域
508	電晶體電晶體邏輯／HOP 旗標域
510	旗標域
512	封包最大傳輸單元域
514	保密策略指標域

五、發明說明（9）

516	指標器域
518	隧道源位址域
520	隧道目的地位址域
522	域
600	入站保密結合資料結構
602	保密結合序列數域
603	保密結合硬位元組壽命域
604	保密結合目前位元組計數域
605	保密結合硬時間壽命域
606	保密策略指標域
608	旗標域
610	保密結合密鑰資訊指標器域
612	反重演遮罩域
614	網際網路協定版本址域
700	電腦系統
702	複數頻道網際網路保密協定硬體元件
704	控制器電路
706	記憶體儲存裝置
708	記憶體仲裁器
802	暫存器區塊
804	訊號仲裁器
806	寫入緩衝器
808	寫入緩衝器控制區塊

五、發明說明（10）

810	訊號位址暫存器
812	訊號控制暫存器
814	寫入緩衝器控制暫存器
816	寫入緩衝器資料暫存器

較佳實施例詳細說明

第１圖係顯示一個說明透過一個互連電腦網路而通訊之許多電腦之功能方塊圖。該系統１００係說明一個透過一個諸如網際網路之外部非保密電腦網路１０６而連接至一個第二本地網路１０４之第一本地網路１０２。該第一本地網路１０２係包含：複數個第一個別電腦工作站１０８－１，１０８－２，１０８－３，・・・１０８－N，該複數個第一個別電腦工作站１０８－１，１０８－２，１０８－３，・・・１０８－N 係連接至一個第一閘路器電腦１１０。且該第二本地網路１０４係包含：複數個第二個別電腦工作站１１２－１，１１２－２，１１２－３，・・・１１２－N，該複數個第二個別電腦工作站１１２－１，１１２－２，１１２－３，・・・１１２－N 係連接至一個第二閘路器電腦１１４。可以瞭解的是，圖示於第１圖之該系統１００僅係爲一個實施例之範例，且其他實施例係落入本發明之範疇。舉例而言，該系統可以包含直接連接至該網際網路１０６之個別電腦工作站，或者透過一個服務提供者而連接至該網際網路１０６。

如同上文所注意到，資料係通過該網際網路１０６而

五、發明說明（11）

作爲網際網路協定資料包。如示於第２圖之一個網際網路協定資料包２００典型地係包含一個網際網路協定標頭部分２０２，一個上層協定標頭２０４，及一個資料酬載２０６。一個出站之網際網路保密協定資料包之範例，亦即用於網際網路保密協定處理且用於傳輸至一個想要之目的地之一個網際網路協定資料包，係示於第３及４圖，其係分別用於隧道模式及傳輸模式。如於此所顯示，一個網際網路保密協定資料包３００及４００係包含：一個網際網路協定標頭部分３０２，４０２；一個網際網路保密協定標頭部分３０４，４０４；及一個加密及／或驗證酬載部分３０６，４０６。該網際網路協定標頭部分３０２，４０２係可以爲：假如於網際網路保密協定隧道模式之下操作，則爲一個新的網際網路協定標頭部分３０２（第３圖）；假如於傳輸模式之下操作，則爲該未加密之網際網路協定資料包２００之該原始網際網路協定標頭部分４０２（第４圖）。該加密及／或驗證酬載部分３０６，４０６（由該對角線所表示）係包含由該未加密之網際網路協定資料包２００而來之該資料酬載部份２０６之加密及／或驗證形式。且，假如於隧道模式下操作，則該加密及／或驗證酬載部分３０６將可以包含該原始的網際網路協定標頭部分２０２及該上層協定標頭２０４之一個加密形式。或者，於該傳輸模式之下，該原始的上層協定標頭２０４係包含於其原始的形式之中。該隧道及傳輸模式係爲熟悉本項技藝人士所熟知，且係詳細解釋於 RFC２４０１“用

五、發明說明（17）

於該網際網路協定之系統架構”，該文件整體係於此併入作爲參考。

此外，應注意的是，一個裝置之所有主動的入站及出站之保密結合係儲存於一個保密結合資料庫內作爲保密結合資料結構。儲存於一個保密結合資料庫１１６，１１８之內作爲入口之出站及入站保密結合資料結構係分別顯示於第５圖及第６圖。應瞭解的是，雖然該資料結構係敘述對於特定元件於每一個資料結構內之特定位置，這些特定元件之配置係僅爲較佳實施例之一個範例。事實上，該些特定元件之每一個係能夠儲存於除了顯示及敘述之位置。

於任何情況下，首先參照第５圖，於一個較佳實施例中，一個出站保密結合資料結構５００係包含一個保密結合序列數域５０２、一個保密結合硬位元組壽命域５０３、一個保密結合目前位元組計數域５０４、一個保密結合硬時間壽命域５０５及一個保密結合軟位元組壽命域５０７，該保密結合序列數域５０２之目的係爲提供反重演偵測。該保密結合硬位元組壽命域５０３係界定一個特定的保密結合能夠處理之絕對最大位元組數。一旦此最大數係超過時，該保密結合係不再可使用，且該保密密鑰係被標示爲過期。該保密結合硬時間壽命域５０５係界定一個特定保密結合能夠使用之秒的絕對最大數。一旦此時間係超過時，該保密結合係不再可使用，且該保密密鑰係被標示爲過期。該保密結合軟位元組壽命域５０７係界定一個特定的保密結合於辨認之前能夠處理之臨限位元組數。一旦

五、發明說明（17）

該臨限位元組數係超過，則該保密結合係需要辨認網際網路密鑰交換（Internet Key Exchange，IKE）係被通知。該保密結合係能夠持續被使用，直到辨認完成爲止，或者直到該該硬位元組壽命值係第一次產生超過爲止。該保密結合目前位元組計數域５０４係包含由一個特定的保密結合所處理之目前位元組，且係與於該保密結合硬時間壽命域５０５及該保密結合軟位元組壽命域５０７內之值相比較。如同將進一步於下文所敘述，該出站保密結合資料結構５００之至少該保密結合序列數域５０２、該保密結合硬位元組壽命域５０３、該保密結合目前位元組計數域５０４、該保密結合硬時間壽命域５０５及該保密結合軟位元組壽命域５０７係被修改，而成爲用於出站資料封包之處理路徑之一部分。

該出站保密結合資料結構５００係進一步包含一個８位元密鑰域５０６，一個電晶體電晶體邏輯／HOP 旗標域５０８，一個旗標域５１０，一個封包最大傳輸單元域５１２，一個保密策略指標域５１４，一個指標器域５１６，一個隧道源位址域５１８，及一個隧道目的地位址域５２０。該電晶體電晶體邏輯／HOP 旗標域５０８係使用於驗證由該網路處理器所指定之特定保密結合資料庫之入口係爲一個有效的保密結合資料庫入口。該電晶體電晶體邏輯／HOP 旗標域５０８係決定是否由該保密結合資料庫入口或者由正被處理之封包的內部標頭而來之電晶體電晶體邏輯／HOP 域係被拷貝。該旗標域５１０係包含使用於控

五、發明說明（18）

制許多出站封包處理之旗標。與該些旗標之每一個相關之細節對於本發明之瞭解係不需要，且因此係將不予以詳細敘述。該封包最大傳輸單元域５１２係指示該最大封包長度，包含該內部及外部標頭，其係被建立用於該出站保密隧道。該保密策略指標域５１４係包含一個當該出站保密結合係被建立時被同意之保密策略指標值。如同熟悉本項技藝人士所熟知，該保密策略指標值係與網際網路保密協定資料包之每一個一起被傳輸，且係與其他資料值一起被接收該網際網路保密協定封包之節點所使用，以於該保密結合資料庫內定位該同意的保密結合。該指標器域５１６係儲存一個被使用於定位用於出站封包處理之適當保密結合密鑰結構之指標器。該隧道源位址域５１８及該隧道目的地位址域５２０係於每一個內涵指明於該特定的保密結合已經被建立之互相通訊之電腦之間之來源位址及目的地位址。最後，應注意的是，敘明於第５圖之該特別的出站資料結構係包含係被保留作爲未來使用之一或多個域５２２。

現請參照第６圖，於一個較佳實施例中，一個入站保密結合資料結構６００係類似於該出站保密結合資料結構５００，該入站保密結合資料結構６００係包含一個保密結合序列數域６０２、一個保密結合硬位元組壽命域６０３、一個保密結合目前位元組計數域６０４及一個保密結合硬時間壽命域６０５。該保密結合序列數域６０２、該保密結合硬位元組壽命域６０３、該保密結合目前位元組

五、發明說明（16）

計數域６０４及該保密結合硬時間壽命域６０５係於該入站保密結合資料結構６００中作爲與該出站資料結構中相同的目的，如同該出站保密結合資料結構５００，係被修改爲該入站資料封包處理路徑之一部分。

該入站保密結合資料結構６００係進一步包含一個保密策略指標域６０６，一個旗標域６０８，一個保密結合密鑰資訊指標器域６１０，一個反重演遮罩域６１２，及一個網際網路協定版本址域６１４。類似於該出站保密結合資料結構５００之該保密策略指標域６０６係包含當該入站保密結合係對於該保密隧道建立時同意之該保密策略指標值。亦類似於該出站保密結合資料庫５００，該旗標域６０８係包含使用於控制許多入站封包處理。該保密結合密鑰資訊指標器域６１０係包含一個與被使用之該保密密鑰相關之指標器值。該反重演遮罩域６１２係包含許多當該反重演服務係被致能時能夠被使用之反重演遮罩。且最後，該網際網路協定版本址域６１４係包含根據是否使用網際網路協定４．０版或者網際網路協定６．０版而定之許多資料。此資訊對於瞭解本發明係不需要，且將不作進一步之討論。

作爲本發明之一個更詳細敘述之先驅，將首先提供使用網際網路保密協定之兩個電腦之間之保密通訊。關於此方面，且再次參照第１圖，當舉例爲１０８－１之該第一個別電腦工作站之一之該操作人員想要與舉例爲１１２－１之該第二個別電腦工作站之一之該操作人員作通訊時，

五、發明說明（16）

該第一個別電腦工作站１０８－１之該操作人員係傳輸資料給該第二個別電腦工作站１１２－１之該操作人員。如同剛剛討論過，該資料係以網際網路保密協定資料包之形式傳輸。該第一閘路器電腦１１０係接收由該電腦工作站而來之該第一資料包，且以該第二閘路器電腦１１４決定是否一個網際網路保密協定保密結合係存在。假如網際網路保密協定保密結合係不存在，則該第一閘路器電腦１１０係較佳地透過所謂的網際網路密鑰交換（Internet Key Exchange，IKE）軟體，請求由該第二閘路器電腦１１４而來之一個網際網路保密協定保密結合。較佳的情況爲，該網際網路密鑰交換軟體係駐存於該第一閘路器電腦１１０及該第二閘路器電腦１１４之每一個內之一個軟體堆疊之中。該使用之網際網路密鑰交換軟體係可以爲熟悉本項技藝人士所知之許多傳統的網際網路密鑰交換軟體組件之任何一個。範例之傳統的網際網路密鑰交換軟體組件係包含但不限於（Lucent™）或者安全網路（SafeNet™）而來之網際網路密鑰交換軟體。

假如該第一閘路器電腦１１０及該第二閘路器電腦１１４係已經共享一個網際網路密鑰交換軟體，則該網際網路保密協定保密結合係能夠被相當快速地產生。假如該第一閘路器電腦１１０及該第二閘路器電腦１１４係尚未共享一個網際網路密鑰交換軟體，則一個網際網路密鑰交換軟體保密結合首先必須於一個網際網路保密協定保密結合能夠被建立之前被建立。爲了建立一個網際網路密鑰交換

五、發明說明（17）

軟體保密結合，該第一閘路器電腦１１０及該第二閘路器電腦１１４係交換已經由一個可信賴的第三者認證機構１１５所數位化簽名之數位認證。其後，當該網際網路密鑰交換軟體會談變成主動時，該第一閘路器電腦１１０及該第二閘路器電腦１１４係能夠建立該網際網路保密協定保密結合。

爲了建立該網際網路保密協定保密結合，該第一閘路器電腦１１０及該第二閘路器電腦１１４必須同意一個加密演算法，一個保密策略指標值及一個共享會談密鑰。當此完成時，該網際網路保密協定保密結合係已經被建立，且該第一閘路器電腦１１０及該第二閘路器電腦１１４係儲存該網際網路保密協定保密結合於其個別的保密結合資料庫１１６及１１８之內之一個入口。如同下文將予以更詳細敘述，該保密結合資料庫１１６及１１８係駐存於可以結合於該第一閘路器電腦１１０及該第二閘路器電腦１１４內之一個記憶體儲存裝置之中或者如示於第１圖爲實體上彼此分離之記體體儲存裝置之中。

一旦該保密結合已經被建立，當一個於該第一閘路器電腦１１０內之網際網路保密協定硬體元件（未示於第１圖中）係由該第一個別電腦１０８－１而來之用於網際網路保密協定處理之一個網際網路協定資料包２００時，該網際網路保密協定硬體元件係於一個非圖示之保密策略資料庫（Security Policy Database, SPD）內查詢一個保密策略。然後，該網際網路保密協定硬體元件係選擇該複數個

五、發明說明（18）

獨立通道之一以處理該資料包。較佳的情況爲，係選擇一個最不忙的通道。然後，根據由該保密策略資料庫查表之資訊，一個出站保密結合資料結構５００係由該保密結合資料庫１１６內之一個適當的入口被取出至一個緩衝器之中。其後，該出站保密結合資料結構５００係被更新，且被寫回至該相同的保密結合資料庫入口。特別是，如同上文所注意到，該保密結合序列數域５０２及該保密結合目前位元組計數域５０４之每一個係被增加而作爲該保密結合資料庫之更新。如同將於下文中作更詳細之敘述，於該出站保密結合資料結構係被讀入至該緩衝器之內且隨後被更新且寫回至該保密結合資料庫內之期間，一個訊號（或者“鎖”）係被置放於該特別的保密結合資料庫之內。此係確保該保密結合資料庫之入口係未被另一個通道同時或者實質上同時讀入及更新。

於該第一閘路器電腦１１０內之該保密結合資料庫硬體元件然後係藉由加密及／或驗證該網際網路資料包２００及藉由實施該保密結合資料庫保密結合而形成一個新的保密結合資料庫資料包３００，４００。然後，該第一閘路器電腦１１０係傳輸該新的網際網路保密協定保密結合資料庫３００，４００至該第二閘路器電腦１１４。

當該第二閘路器電腦１１４接收該新的網際網路保密協定資料包３００，４００時，該第二閘路器電腦１１４係藉由分析由該網際網路保密協定標頭４０４而來之資訊而決定該入站保密結合資料庫１１８中之適當的網際網路

五、發明說明（19）

保密協定保密結合。該網際網路保密協定硬體元件然後選擇該複數個獨立通道之一個，以處理該接收到的資料包。根據由該網際網路保密協定標頭４０４分析而來之資訊，一個入站保密結合資料結構６００係由該入站保密結合資料庫１１８中之適當的入口取出而至一個緩衝器。其後，該入站保密結合資料結構６００係被更新及被寫回至該相同的保密結合資料庫入口。然後，於該第二閘路器電腦１１４中之該網際網路保密協定硬體元件係適當地處理該網際網路保密協定資料包３００，４００，且轉送該網際網路保密協定資料包３００，４００至該第二個性電腦工作站１１２－１。類似於上述之一個出站網際網路協定資料包之處理，於該入站保密結合資料結構係被讀入至該緩衝器之內且隨後被更新且寫回至該保密結合資料庫１１８內之期間，一個訊號係被置放於該特別的保密結合資料庫之入口，以防止該保密結合資料庫之入口係未被另一個通道同時或者實質上同時讀入及更新。

已經大致上敘述一個網際網路保密協定資料包３００，４００，一個出站及一個入站保密結合資料結構５００，６００，一個網際網路保密協定保密結合如何被建立，及一旦被建立，一個網際網路保密協定保密結合如何被利用以處理出站及入站網際網路保密協定資料包，本發明之一個更詳細的敘述將被提供。於實施時，首先參照第７圖，第７圖係顯示使用於一個具有複數個保密通道之電腦系統中之該內部網際網路保密協定保密結合處理硬體。該電

五、發明說明（20）

腦系統７００可以爲一個閘路器或者路由器，諸如該第一閘路器電腦１１０及該第二閘路器電腦１１４，或者一個獨立的電腦，諸如該第一個別電腦工作站１０８－１，１０８－２，１０８－３，．．．１０８－N 及該第二個別電腦工作站１１２－１，１１２－２，１１２－３，．．．１１２－N。於任何情況下，該電腦系統７００係包含一個複數頻道網際網路保密協定硬體元件７０２，該複數頻道網際網路保密協定硬體元件７０２係使用於接收網際網路保密協定資料包３００，４００，且適當地處理該網際網路保密協定資料包３００，４００成爲網際網路協定資料包。如所示，該複數頻道網際網路保密協定硬體元件７０２係可以被設計成爲包含許多數量之通道，例如達到 N 個通道。然而，於一個較佳實施例中，該通道數量係爲８。此外，該複數頻道網際網路保密協定硬體元件７０２可以爲一個一般目的之微處理器，或者於一個較佳實施例中，其係爲一個特別設計用於網際網路保密協定之實施的等定應用硬體裝置（例如特殊應用積體電路）。

由於實施之功能而於此被稱爲一個訊號控制器之一個控制器電路７０４係與該複數頻道網際網路保密協定硬體元件７０２之每一個通道通訊。一個包含複數個具有該電腦之保密結合資料庫之記憶體區域（或者“入口”）之記憶體儲存裝置７０６係連接至該訊號控制器７０４及一個記憶體仲裁器７０８。雖然第７圖係顯示一個包含一個入站及一個出站保密結合資料庫之單一記憶體儲存裝置７０

五、發明說明（ 7 ）

6，應瞭解的是，其係僅爲一個範例之實施例，且該保密結合資料庫係能夠被配置成實體上分離之記憶體儲存裝置之一部分。

因爲第6圖僅顯示一部分之該電腦系統７００係包含可能需要存取該記憶體儲存裝置７０６之許多其他裝置，所以該記憶體仲裁器７０８係被提供。該記憶體儲存裝置７０６係類似於上述參照第１圖之該保密結合資料庫１１６，１１８，且該記憶體儲存裝置７０６之功能係相同於上述參照第１圖之該保密結合資料庫１１６，１１８。因此，雖然第７圖係顯示該記憶體儲存裝置７０６爲實體上包含於該電腦７００作爲一部分，其係僅爲一個較佳實施例之範例。應瞭解的是，該記憶體儲存裝置７０６可以實體上與該電腦７００分離。

現請參照第８圖，其係提供一個包含該訊號控制器７０４之功能方塊圖之更詳細的敘述。如第８圖所示，該訊號控制器７０４係包含一個暫存器區塊８０２，一個訊號仲裁器８０４，一個寫入緩衝器８０６，及一個寫入緩衝器控制區塊８０８。該暫存器區塊８０２係包含 N 個通道，該些通道之每一個係與該複數頻道網際網路保密協定硬體元件７０２中之該 N 個通道之一個作介面接觸。於該暫存器區塊８０２中之該 N 個通道之每一個係包含複數個個別的暫存器。於每一個暫存器區塊通道之內之該些個別的暫存器係包含一個訊號位址暫存器８１０，一個訊號控制暫存器８１２，一個寫入緩衝器控制暫存器８１４，及一

五、發明說明（ㄨㄚ）

個寫入緩衝器資料暫存器８１６。應瞭解的是，每一個暫存器區塊通道係可以包含於該四個上述之暫存器額外的暫存器。這些額外的暫存器係將被使用於瞭解本發明不需要之功能，且因此係不作進一步之敘述。當由該訊號控制器７０４所實施以更新保密結合資料庫之入口之程序係被敘述時，於每一個暫存器區塊通道中之每一個上述之暫存器之目地將變成明顯的。

該訊號仲裁器８０４係爲確保一次僅有該 N 個保密通道之一個係存取一個特別的保密結合資料庫之該訊號控制器７０４之該部分。因此，該訊號仲裁器８０４係防止複數個通道同時（或者實質上同時）更新該相同之保密結合資料庫之入口。該訊號仲裁器８０４係以一個先到先服務之基礎而提供每一個通道存取一個保密結合資料庫之入口。爲了達成此目的，於一個較佳實施例中，該訊號仲裁器８０４係利用三個邏輯區塊：一個加權控制邏輯區塊８０１，一個訊號允許樹邏輯區塊８０３及一個允許邏輯區塊８０５，該加權控制邏輯區塊８０１，該訊號允許樹邏輯區塊８０３及該允許邏輯區塊８０５之每一個係將於下文中予以敘述。

該加權控制邏輯區塊８０１係對於該 N 個通道之每一個指定一個加權值。於一個較佳實施例中，指定給每一個通道之加權值係一個（$\log_2(N)+1$）位元加權值。舉例而言，於一個較佳實施例中，其係具有８個通道，當設定時，係連接成爲該加權值之最高位元。於開機時，與每一個

五、發明說明（２）

通道相關之該加權值係被起始化爲零。其後，當一個通道係對於一個特別的保密結合資料庫請求一個訊號時，如同由其被設定之請求位元所指示，且於該請求係被允許之前，另一個通道係確認一個用於相同入口之請求，該通道之加權係增加１。此外，所有具有對於尚未被允許之相同的特別的保密結合資料庫入口之訊號請求的其他通道之加權將被增加１。應瞭解的是，該加權控制邏輯區塊８０１之實施僅係爲一個較佳實施例之範例，且其他實施係能夠被使用。實際上，於一個特定的替代實施例中，與該 N 個通道之每一個相關之該 $\log_2(N)$位元加權值係未與該通道之請求位元相連結。該加權控制邏輯區塊８０１之剩餘的操作將實質上相同。

該訊號允許樹邏輯區塊８０３係連接至該加權控制邏輯區塊８０１，且決定該 N 個通道之哪一個對於一個特定的保密結合資料庫入口係具有最高加權值，且對於具有該最高加權值之該通道發出一個允許訊號。於具有複數個對於一個特定的保密結合資料庫入口訊號請求具有相同加權值之請求的情況下，該允許樹邏輯區塊８０３係實施一個優先權機制，以決定哪一個通道係接收該允許訊號。於一個較佳實施例中，該優先權機制係將最低優先權給予該最低之通道，且將最高優先權給予該第 N 個通道。熟悉本項技藝人士將可以瞭解，其他優先權機制係能夠被實施。

該允許邏輯區塊８０５係與該訊號允許樹邏輯區塊８０３作通訊。特別是，假設一個明顯的保密結合資料庫入

五、發明說明（26）

口訊號請求係對於該通道爲懸而未決之情況下，根據由該訊號允許樹邏輯區塊８０３所發出之該允許訊號，該允許邏輯區塊８０５係於該適當的通道之該訊號控制暫存器８１２中設定一個允許位元（進一步敘述於下文中）。一旦該允許位元係設定於請求通道之訊號控制暫存器８１２中，則該允許邏輯區塊８０５重置該通道之加權值爲零。

當該寫入緩衝器８０６由該寫入緩衝器控制區塊８０８所命令時，該寫入緩衝器８０６係將該更新過的保密結合寫入至該適當的保密結合資料庫入口之內。該寫入緩衝器８０６係包含 N 個６４位元之寫入緩衝器暫存器。於一個較佳實施例中，其中係具有８個通道，該寫入緩衝器８０６係包含１６個入口，３２位元寬先進先出暫存器。如同將於下文更詳細地敘述，該更新過的保密結合資料結構係首先被寫入至該寫入緩衝器８０６中之該適當的通道之先進先出。然後，當該通道之保密結合資料庫入口訊號請求係被釋放，該通道之寫入緩衝器先進先出之內容係被寫入至該適當的保密結合資料庫入口。

如同剛剛敘述之該寫入緩衝器８０６之操作係被該寫入緩衝器控制區塊８０８所控制。此外，當對於該記憶體儲存裝置６０６之請求存取係特別包含該入站及出站保密結合資料庫入口時，該寫入緩衝器控制區塊８０８係與該記憶體仲裁器６０８作介面接觸。於一個較佳實施例中，該寫入緩衝器控制區塊８０８係包含一個由韌體所控制之有限狀態機。由後續之討論，該寫入緩衝器控制區塊８０

五、發明說明（25）

８之操作之瞭解將變成明顯的，該後續之討論係敘述由該訊號控制器６０４所實施之程序，以更新該入站及出站保密結合資料庫入口。

現請參照第９圖結合第８圖，更新保密結合資料庫入口之程序９００當由該訊號控制器７０４所實施時，係將被提供。關於此點，對於“方塊”之括號的參考係對應於示於第９圖之該程序流程之特別的參考符號。應瞭解的是，於一個較佳實施例中，該訊號控制器７０４係由韌體所控制，以實施該程序，然而，本發明亦包含該訊號控制器係由軟體所控制之一個實施例。此外，下文所詳細討論之該程序係用於該 N 個保密通道之一。應瞭解的是，該程序可以實質上同時地由該 N 個保密通道之其他包含該系統之保密通道之每一個所實施。

雖然如此，當於該道網際網路保密協定硬體元件７０２中之一個通道係需要將一個更新過的保密結合資料結構寫入至一個保密結合資料庫（方塊９０２）時，該程序９００係開始。當此產生時，需要被更新之該保密結合資料庫入口之位址係被寫入至該位址暫存器８１０（方塊９０４），且一個請求位元係於該訊號控制暫存器８１２中被設定（方塊９０６）。當該訊號仲裁器８０４係決定該通道應該被允許該訊號時，一個於該訊號控制暫存器８１２中之允許位元係被設定（方塊９０８）。然後，爲了回應該被允許之訊號，位於該具有於該位址暫存器８１０中之位址之保密結合資料庫中之該保密結合資料結構係被取出

五、發明說明（九）

而至每一個通道中之先前提及之本地緩衝器（方塊９１０）。然後，需要被更新之該取出之保密結合資料結構之該些部分係於本地被修改（方塊９１２）。

其後，一個於該寫入緩衝器控制暫存器８１４中之一個“忙碌位元”係被檢查，以決定是否該寫入緩衝器８０６係忙碌的（方塊９１４）。一旦該寫入緩衝器８０６係被重置，其指示該寫入緩衝器８０６係可以被寫入，則該更新過的保密結合資料結構部分係被寫入至該寫入緩衝器８０６，於該訊號控制暫存器８１２中之該請求位元係於韌體之控制之下被重置（方塊９１６），且該寫入緩衝器忙碌位元係再次被設定（方塊９１８）。該寫入緩衝器控制區塊８０８特別地監視於該訊號控制暫存器８１２中之該請求位元。當該請求位元係被設定時，且當該記憶體仲裁器７０８係允許對於該保密結合資料庫之存取，該寫入緩衝器控制區塊８０８係導致該寫入緩衝器８０６將其內容寫入至具有於該位址暫存器８１０中之該位址之該保密結合資料庫入口（方塊９２０）。然後，該訊號仲裁器８０４係允許該訊號傳輸至該下一個通道，假如可以的話，請求對於該保密結合資料庫入口之存取（方塊９２２）。

雖然本發明已經參照一個較佳實施例而予以敘述，熟悉本項技藝人士將可以瞭解，於不偏離本發明之範疇之下，許多改變可以被實施且均等物係可以取代本發明之元件。此外，於不偏離本發明之基本範疇之下，根據本發明之教示，許多修改可以被實施，以適用於一個特定的情況或

五、發明說明（ㄋ）

者物質。因此，係意欲本發明係不受限於用於實施本發明之揭示爲被認爲是最佳模式之該特定實施例，而本發明係將包含所有落入後附申請專利範圍之範疇之內之所有實施例。

A5
B5

四、中文發明摘要（發明之名稱：　　）

用於在具有複數個保密通道之高速系統中解決保密結合資料庫更新整合之設備及方法

本發明係提供一種用於在具有複數個保密通道之系統中更新保密結合資料庫入口之設備及方法，其係藉由選擇性地允許複數個多重保密通道對於保密結合資料庫之存取而達成，其係可以使用一個先進先服務之機制而更新該相同的保密結合資料庫之入口。該設備係包含一個控制器電路，其之作用爲對於該複數個保密通道之每一個實施該方法，該方法係包含下列步驟：決定是否該複數個保密通道之另一個係具有存取一個特定保密結合資料庫入口的較高

英文發明摘要（發明之名稱：APPARATUS AND METHOD FOR RESOLVING SECURITY ASSOCIATION DATABASE UPDATE COHERENCY IN HIGH-SPEED SYSTEMS HAVING MULTIPLE SECURITY CHANNELS　　）

An apparatus and method for updating security association database entries in a system having multiple security channels by selectively granting access to the entries by a plurality of the multiple security channels that may need to update the same entry using a first-come, first-served scheme. The apparatus includes a controller circuit that functions to carry out the method which, for each of the multiple security channels, includes determining whether another of the security channels has a higher priority to access a particular security association database entry. If no other channel has a higher priority, then the channel requesting access to the entry retrieves it from its address location, modifies it, and writes the modified entry back to its address location. The controller prevents other channels from simultaneously, or substantially simultaneously, retrieving and modifying the same entry.

（請先閱讀背面之注意事項再填寫本頁各欄）

訂

線

A5
B5

四、中文發明摘要（發明之名稱：　　）

優先權。當無其他保密通道係具有較高之優先權時，該通道請求存取該入口係由其位址位置取出，修改且將其寫回至其位址之位置。該控制器係防止其他通道同時或者實質上同時取出或者修改該相同之入口。

英文發明摘要（發明之名稱：　　）

（請先閱讀背面之注意事項再填寫本頁各欄）

訂

線

六、申請專利範圍

1．一種修改於保密結合資料庫中之入口的方法，該保密結合資料庫係於一個具有複數個保密通道之系統中，該方法係結合每一個頻道，該方法係包含下列步驟：

決定是否該複數個保密通道之另一個係具有存取位於該保密結合資料庫中之一個預定位址位置之一個保密結合資料結構的較高優先權；

當無其他保密通道係具有較高之優先權而實施存取該保密結合資料結構時，由該預定位址位置取出該保密結合資料結構；

修改該取出之保密結合資料結構；及

將該修改過之保密結合資料結構寫入至該保密結合資料庫內之該預定位址位置。

2．如申請專利範圍第1項之修改於保密結合資料庫中之入口的方法，其中，該決定是否該複數個保密通道之另一個係具有較高優先權以取出該保密結合資料結構之步驟係包含下列步驟：

請求存取該預定位址之位置；

根據相對於由其他保密通道所實施之存取請求之一個序列次序，而對於該請求指定一個加權值；及

允許具有該最高被指定之加權值之該保密通道之該存取請求。

3．如申請專利範圍第2項之修改於保密結合資料庫中之入口的方法，其中，該請求存取之步驟係包含於一個控制暫存器內設定一個請求位元。

六、申請專利範圍

4．如申請專利範圍第3項之修改於保密結合資料庫中之入口的方法，其中，該允許該存取請求之步驟係包含於該控制暫存器內設定一個允許位元。

5．如申請專利範圍第1項之修改於保密結合資料庫中之入口的方法，其中，該將該修改過之保密結合資料結構寫入至該預定位址位置之步驟係包括下列步驟：

於將該修改過之保密結合資料結構寫入至該預定位址位置之前，將該修改過之保密結合資料結構寫入至一個寫入緩衝器；及

將該修改過之保密結合資料結構由該寫入緩衝器寫入至該預定位址位置。

6．如申請專利範圍第5項之修改於保密結合資料庫中之入口的方法，其中，該請求存取之步驟係包含於一個控制暫存器內設定一個請求位元，且其中，該方法係進一步包括下列步驟：

於將該修改過之保密結合資料結構由該寫入緩衝器寫入至該預定位址位置之前，重置該請求位元。

7．如申請專利範圍第5項之修改於保密結合資料庫中之入口的方法，其係進一步包括下列步驟：

於將該修改過之保密結合資料結構寫入至該預定位址位置之前，決定是否該寫入緩衝器係忙碌的。

8．如申請專利範圍第1項之修改於保密結合資料庫中之入口的方法，其係進一步包括下列步驟：

儲存該取出之保密結合資料結構於一個本地記憶體之

六、申請專利範圍

內；及

修改於該本地記憶體內之該取出之保密結合資料結構。

9．如申請專利範圍第1項之修改於保密結合資料庫中之入口的方法，其係進一步包括下列步驟：儲存該取出之保密結合資料結構之該預定位址位置於一個暫存器之中。

10．一種修改於保密結合資料庫中之入口的方法，該保密結合資料庫係於一個具有複數個保密通道之系統中，該方法係結合每一個頻道，該方法係包含下列步驟：

請求存取於該保密結合資料庫中之一個預定位址位置；

根據相對於由其他保密通道所實施之存取請求之一個序列次序，而對於該請求指定一個加權值；

當無其他保密通道係具有較高之優先權而實施存取該保密結合資料結構時，由該預定位址位置取出該保密結合資料結構；

修改該取出之保密結合資料結構；及

將該修改過之保密結合資料結構寫入至該保密結合資料庫內之該預定位址位置。

11．如申請專利範圍第10項之修改於保密結合資料庫中之入口的方法，其中，該請求存取之步驟係包含於一個控制暫存器內設定一個請求位元。

12．如申請專利範圍第10項之修改於保密結合資

六、申請專利範圍

料庫中之入口的方法，其中，該允許該存取請求之步驟係包含於該控制暫存器內設定一個允許位元。

１３．如申請專利範圍第１０項之修改於保密結合資料庫中之入口的方法，其中，該將該修改過之保密結合資料結構寫入至該預定位址位置之步驟係包括下列步驟：

於將該修改過之保密結合資料結構寫入至該預定位址位置之前，將該修改過之保密結合資料結構寫入至一個寫入緩衝器；及

將該修改過之保密結合資料結構由該寫入緩衝器寫入至該預定位址位置。

１４．如申請專利範圍第１３項之修改於保密結合資料庫中之入口的方法，其中，該請求存取之步驟係包含於一個控制暫存器內設定一個請求位元，且其中，該方法係進一步包括下列步驟：

於將該修改過之保密結合資料結構由該寫入緩衝器寫入至該預定位址位置之前，重置該請求位元。

１５．如申請專利範圍第１３項之修改於保密結合資料庫中之入口的方法，其係進一步包括下列步驟：

於將該修改過之保密結合資料結構寫入至該預定位址位置之前，決定是否該寫入緩衝器係忙碌的。

１６．如申請專利範圍第１０項之修改於保密結合資料庫中之入口的方法，其係進一步包括下列步驟：

儲存該取出之保密結合資料結構於一個本地記憶體之內；及

六、申請專利範圍

修改於該本地記憶體內之該取出之保密結合資料結構。

１７．如申請專利範圍第１０項之修改於保密結合資料庫中之入口的方法，其係進一步包括下列步驟：儲存該取出之保密結合資料結構之該預定位址位置於一個暫存器之中。

１８．一種修改於保密結合資料庫中之入口的方法，該保密結合資料庫係於一個具有複數個保密通道之系統中，該方法係結合每一個頻道，該方法係包含下列步驟：

請求存取於該保密結合資料庫中之一個預定位址位置；

根據相對於由其他保密通道所實施之存取請求之一個序列次序，而對於該請求指定一個加權值；

當無其他保密通道係具有較高之優先權而實施存取該保密結合資料結構時，由該預定位址位置取出該保密結合資料結構；

修改該取出之保密結合資料結構；

決定是否一個寫入緩衝器係忙碌的；

當該寫入緩衝器係忙碌的時，將該修改過之保密結合資料結構寫入至該寫入緩衝器；及

將該修改過之保密結合資料結構由該寫入緩衝器寫入至該保密結合資料庫之該預定位址位置。

１９．一種用於管理對於保密結合資料庫中之入口之存取的控制器，其係於一個具有複數個保密通道之系統中

六、申請專利範圍

，該控制器係包含：

一個暫存器電路，該暫存器電路係包含複數個第一暫存器，該複數個第一暫存器之每一個係個別地與該複數個保密通道之一個作通訊，且該複數個第一暫存器之每一個係可操作於接收由其結合之保密通道而來之一個請求，以取得位於該保密結合資料庫中之一個預定位址處之一個保密結合資料結構；及

一個仲裁器電路，該仲裁器電路係與該暫存器電路作通訊，且係可操作於（i）優先權化由該複數個第一暫存器之每一個所接收而來之該取得的請求爲最高優先權至最低優先權，及（ii）允許該取得之請求傳送至具有最高優先權之保密通道。

２０．如申請專利範圍第１９項之用於管理對於保密結合資料庫中之入口之存取的控制器，其中，該暫存器電路係進一步包含：

複數個第二暫存器，該複數個第二暫存器之每一個係個別地與該複數個保密通道之一個作通訊，且該複數個第二暫存器之每一個係可操作於接收由其結合之保密通道而來之該保密結合資料結構之該預定之位址，取出存取係由其結合之保密通道所請求。

２１．如申請專利範圍第１９項之用於管理對於保密結合資料庫中之入口之存取的控制器，其中，該暫存器電路係進一步包含：

複數個第三暫存器，該複數個第三暫存器之每一個係

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

六、申請專利範圍

個別地與該複數個保密通道之一個作通訊，且該複數個第三暫存器之每一個係可操作於接收由其結合之保密通道而來之一個更新過之保密結合資料結構。

２２．如申請專利範圍第１９項之用於管理對於保密結合資料庫中之入口之存取的控制器，其係進一步包含：

複數個寫入緩衝器電路，該複數個寫入緩衝器電路之每一個係個別地與該複數個保密通道之一個作通訊，且該複數個寫入緩衝器電路之每一個係可操作於（i）接收由其結合之保密通道而來之一個修改過之保密結合資料結構，及（ii）將該修改過之保密結合資料結構寫入至該取出之保密結合資料結構之該位址位置，以回應該仲裁器電路後續允許該複數個保密通道之另一個通道一個取出之請求。

２３．如申請專利範圍第２２項之用於管理對於保密結合資料庫中之入口之存取的控制器，其中，該寫入緩衝器電路之每一個係包含一個先進先出暫存器。

２４．如申請專利範圍第２２項之用於管理對於保密結合資料庫中之入口之存取的控制器，其係進一步包含：

複數個寫入緩衝器電路，該複數個寫入緩衝器電路之每一個係個別地與該複數個保密通道之一個作通訊，且該複數個寫入緩衝器電路之每一個係可操作於（i）決定是否其結合之寫入緩衝器電路係可使用於接收該修改過之保密結合資料結構；及（ii）只有當該寫入緩衝器係可使用時，允許其結合之寫入緩衝器接收該修改過之保密結合資料結構。

六、申請專利範圍

２５．如申請專利範圍第２４項之用於管理對於保密結合資料庫中之入口之存取的控制器，其中，該暫存器電路係進一步包含：

複數個第四暫存器，該複數個第四暫存器之每一個係個別地與該複數個寫入緩衝器之一個及該複數個寫入緩衝器控制器之一個作通訊，

其中，該第四暫存器之每一個係可操作於接收該寫入緩衝器控制器之一個忙碌／不忙碌之狀態位元，且其中，是否該寫入緩衝器控制器電路之每一個係可使用之決定係根據該忙碌／不忙碌之狀態位元而定。

２６．如申請專利範圍第１９項之用於管理對於保密結合資料庫中之入口之存取的控制器，其中，該仲裁器電路係包含：

一個加權控制邏輯電路，該加權控制邏輯電路係可操作於指定一個加權值至該控制器由該複數個第一暫存器之每一個所接收而來之取得的請求之每一個；

一個允許樹邏輯電路，該允許樹邏輯電路係連接至該加權控制邏輯電路，且係可操作於（i）決定該複數個第一暫存器之哪一個係具有一個最高加權值；及（ii）對於該具有該最高加權值之該第一暫存器產生一個允許訊號；及

一個允許邏輯電路，該允許邏輯電路係連接成接收由該允許樹邏輯電路而來之該允許訊號，且回應於該允許訊號，設定一個允許位元於具有該最高加權值之該第一暫存器中。

六、申請專利範圍

２７．一種用於管理對於保密結合資料庫中之入口之存取的控制器，其係於一個具有複數個保密通道之系統中，該控制器係包含：

一個暫存器電路，該暫存器電路係包含複數個第一暫存器，該複數個第一暫存器之每一個係個別地與該複數個保密通道之一個作通訊，且該複數個第一暫存器之每一個係可操作於接收由其結合之保密通道而來之一個請求，以取得位於該保密結合資料庫中之一個預定位址處之一個保密結合資料結構；

一個仲裁器電路，該仲裁器電路係與該暫存器電路作通訊，且係可操作於（i）優先權化由該複數個第一暫存器之每一個所接收而來之該取得的請求爲最高優先權至最低優先權，及（ii）允許該取得之請求傳送至具有最高優先權之保密通道；及

複數個寫入緩衝器電路，該複數個寫入緩衝器電路之每一個係個別地與該複數個保密通道之一個作通訊，且該複數個寫入緩衝器電路之每一個係可操作於（i）接收由其結合之保密通道而來之一個修改過之保密結合資料結構，及（ii）將該修改過之保密結合資料結構寫入至該取出之保密結合資料結構之該位址位置，以回應該仲裁器電路後續允許該複數個保密通道之另一個通道一個取出之請求。

２８．如申請專利範圍第２７項之用於管理對於保密結合資料庫中之入口之存取的控制器，其中，該暫存器電路係進一步包含：

六、申請專利範圍

複數個第二暫存器，該複數個第二暫存器之每一個係個別地與該複數個保密通道之一個作通訊，且該複數個第二暫存器之每一個係可操作於接收由其結合之保密通道而來之該保密結合資料結構之該預定之位址，取出存取係由其結合之保密通道所請求。

２９．如申請專利範圍第２７項之用於管理對於保密結合資料庫中之入口之存取的控制器，其中，該暫存器電路係進一步包含：

複數個第三暫存器，該複數個第三暫存器之每一個係個別地與該複數個保密通道之一個作通訊，且該複數個第三暫存器之每一個係可操作於接收由其結合之保密通道而來之一個更新過之保密結合資料結構。

３０．如申請專利範圍第２７項之用於管理對於保密結合資料庫中之入口之存取的控制器，其係進一步包含：

複數個寫入緩衝器電路，該複數個寫入緩衝器電路之每一個係個別地與該複數個保密通道之一個作通訊，且該複數個寫入緩衝器電路之每一個係可操作於（i）決定是否其結合之寫入緩衝器電路係可使用於接收該修改過之保密結合資料結構；及（ii）只有當該寫入緩衝器係可使用時，允許其結合之寫入緩衝器接收該修改過之保密結合資料結構。

３１．如申請專利範圍第３０項之用於管理對於保密結合資料庫中之入口之存取的控制器，其中，該暫存器電路係進一步包含：

六、申請專利範圍

複數個第四暫存器，該複數個第四暫存器之每一個係個別地與該複數個寫入緩衝器之一個及該複數個寫入緩衝器控制器之一個作通訊，

其中，該第四暫存器之每一個係可操作於接收該寫入緩衝器控制器之一個忙碌／不忙碌之狀態位元，且其中，是否該寫入緩衝器控制器電路之每一個係可使用之決定係根據該忙碌／不忙碌之狀態位元而定。

３２．如申請專利範圍第２７項之用於管理對於保密結合資料庫中之入口之存取的控制器，其中，該控制器係包含：

一個加權控制邏輯電路，該加權控制邏輯電路係可操作於指定一個加權值至該控制器由該複數個第一暫存器之每一個所接收而來之取得的請求之每一個；

一個允許樹邏輯電路，該允許樹邏輯電路係連接至該加權控制邏輯電路，且係可操作於（i）決定該複數個第一暫存器之哪一個係具有一個最高加權值；及（ii）對於該具有該最高加權值之該第一暫存器產生一個允許訊號；及

一個允許邏輯電路，該允許邏輯電路係連接成接收由該允許樹邏輯電路而來之該允許訊號，且回應於該允許訊號，設定一個允許位元於具有該最高加權值之該第一暫存器中。

３３．一種用於管理對於保密結合資料庫中之入口之存取的控制器，其係於一個具有複數個保密通道之系統中，該控制器係包含：

（請先閱讀背面之注意事項再填寫本頁）

訂

線

六、申請專利範圍

一個暫存器電路，該暫存器電路係包含複數個第一暫存器，該複數個第一暫存器之每一個係個別地與該複數個保密通道之一個作通訊，且該複數個第一暫存器之每一個係可操作於接收由其結合之保密通道而來之一個請求，以取得位於該保密結合資料庫中之一個預定位址處之一個保密結合資料結構；及

一個仲裁器電路，該仲裁器電路係與該暫存器電路作通訊，且係可操作於（i）優先權化由該複數個第一暫存器之每一個所接收而來之該取得的請求爲最高優先權至最低優先權，及（ii）允許該取得之請求傳送至具有最高優先權之保密通道，該仲裁器電路係包含：

一個加權控制邏輯電路，該加權控制邏輯電路係可操作於指定一個加權值至該控制器由該複數個第一暫存器之每一個所接收而來之取得的請求之每一個；

一個允許樹邏輯電路，該允許樹邏輯電路係連接至該加權控制邏輯電路，且係可操作於（i）決定該複數個第一暫存器之哪一個係具有一個最高加權值；及（ii）對於該具有該最高加權值之該第一暫存器產生一個允許訊號；及

一個允許邏輯電路，該允許邏輯電路係連接成接收由該允許樹邏輯電路而來之該允許訊號，且回應於該允許訊號，設定一個允許位元於具有該最高加權值之該第一暫存器中；及

複數個寫入緩衝器電路，該複數個寫入緩衝器電路之每一個係個別地與該複數個保密通道之一個作通訊，且該

六、申請專利範圍

複數個寫入緩衝器電路之每一個係可操作於（i）接收由其結合之保密通道而來之一個修改過之保密結合資料結構，及（ii）將該修改過之保密結合資料結構寫入至該取出之保密結合資料結構之該位址位置，以回應該仲裁器電路後續允許該複數個保密通道之另一個通道一個取出之請求。

３４．一種用於管理對於保密結合資料庫中之入口之存取的控制器，其係於一個具有複數個保密通道之系統中，該控制器係包含：

一個加權控制邏輯電路，該加權控制邏輯電路係可操作於指定一個加權值至該控制器由該複數個第一暫存器之每一個所接收而來之取得的請求之每一個；

一個允許樹邏輯電路，該允許樹邏輯電路係連接至該加權控制邏輯電路，且係可操作於（i）決定該複數個第一暫存器之哪一個係具有一個最高加權值；及（ii）對於該具有該最高加權值之該第一暫存器產生一個允許訊號；及

一個允許邏輯電路，該允許邏輯電路係連接成接收由該允許樹邏輯電路而來之該允許訊號，且回應於該允許訊號，設定一個允許位元於具有該最高加權值之該第一暫存器中。

３５．一種電腦可讀取媒體，其係包含用於實施於具有複數個保密通道之電腦系統中之一或多個保密通道修改於一個保密結合資料庫中之入口的指令之電腦可執行碼，該指令係包含下列步驟：

決定是否該複數個保密通道之另一個係具有存取位於

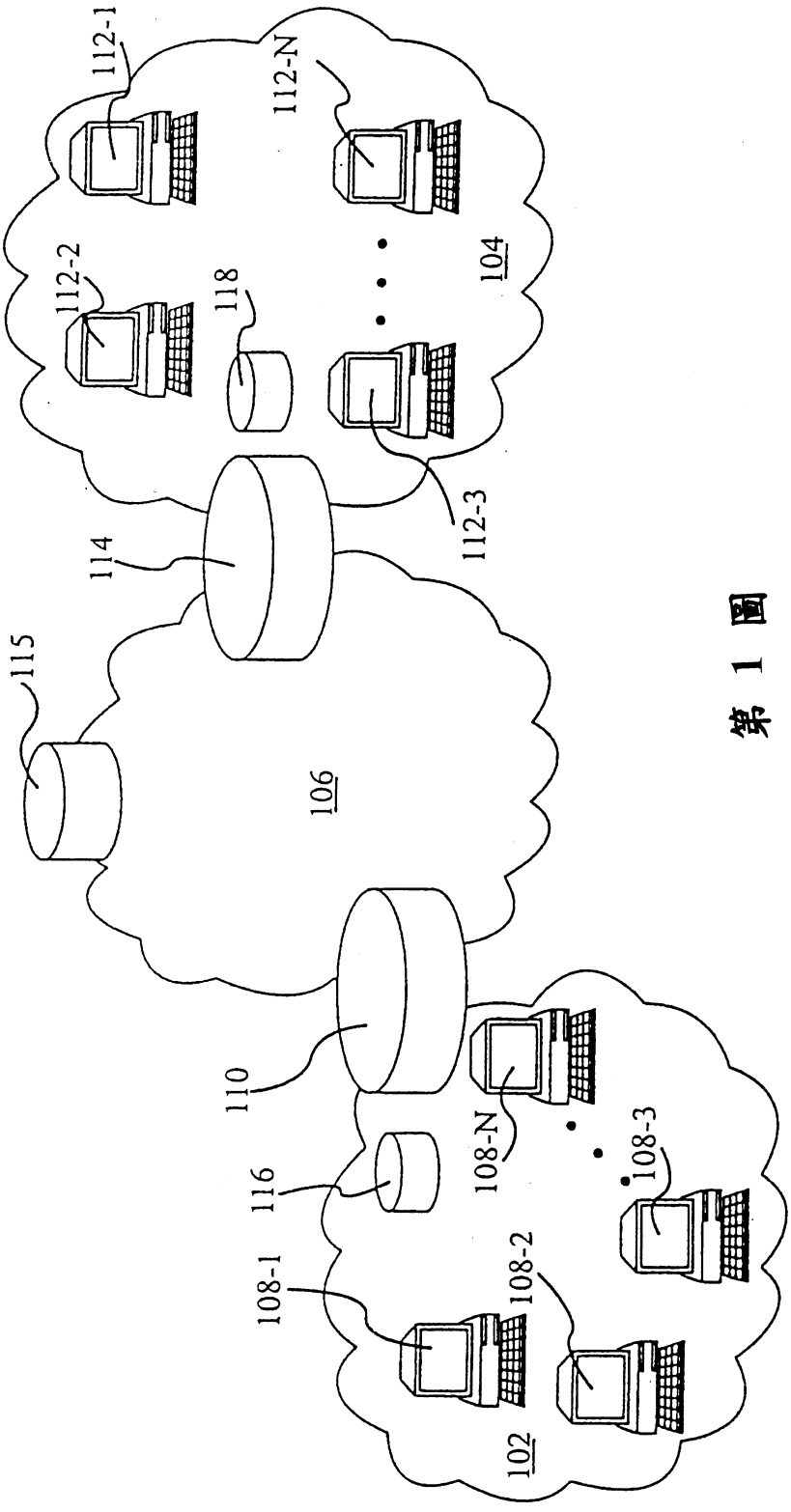
六、申請專利範圍

該保密結合資料庫中之一個預定位址位置之一個保密結合資料結構的較高優先權；

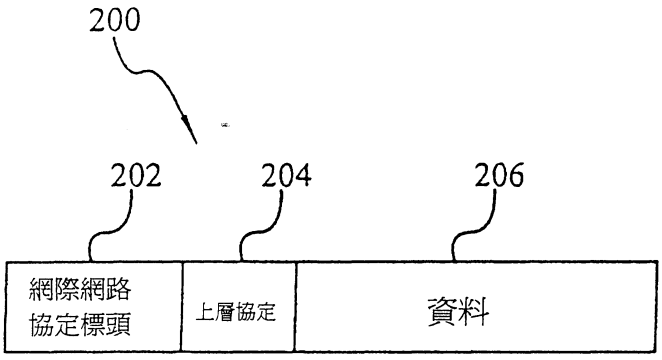
當無其他保密通道係具有較高之優先權而實施存取該保密結合資料結構時，由該預定位址位置取出該保密結合資料結構；

修改該取出之保密結合資料結構；及

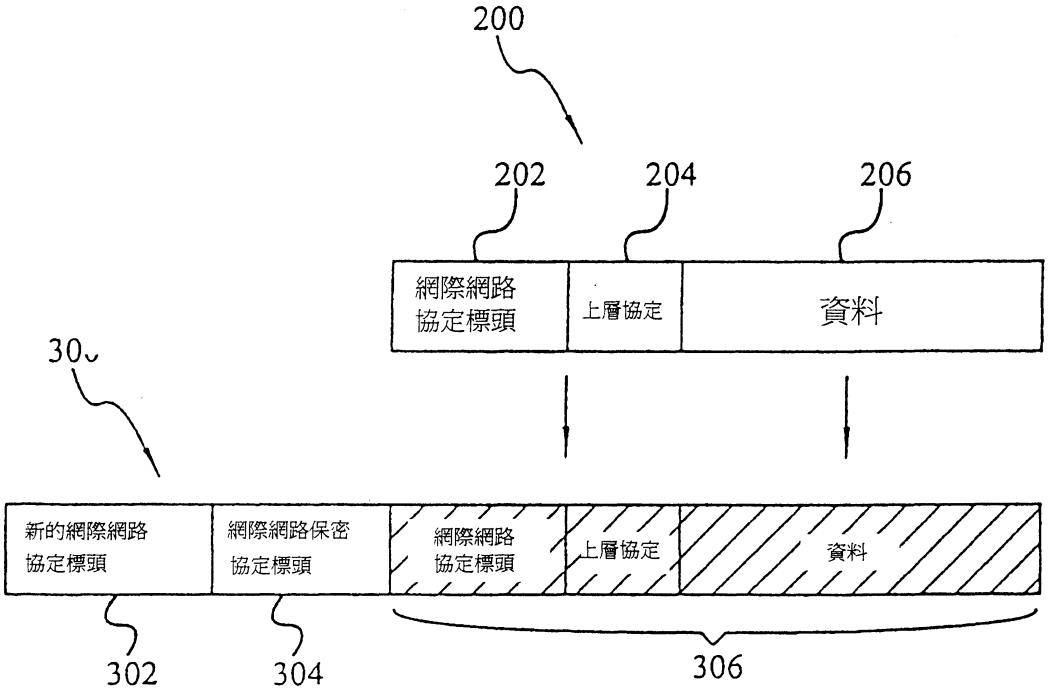
將該修改過之保密結合資料結構寫入至該保密結合資料庫內之該預定位址位置。


112-1
112-N
112-2
118
104
112-3
114
115
106
110
116
108-N
108-3
108-1
108-2
102

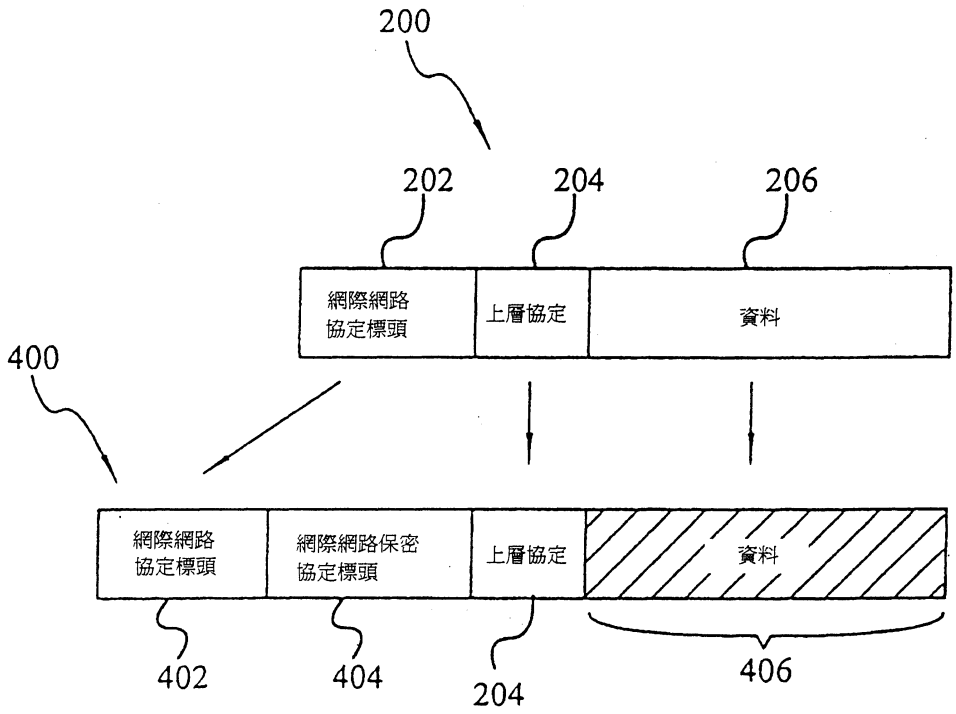
第 1 圖


200
202
204
206
網際網路
協定標頭
上層協定
資料

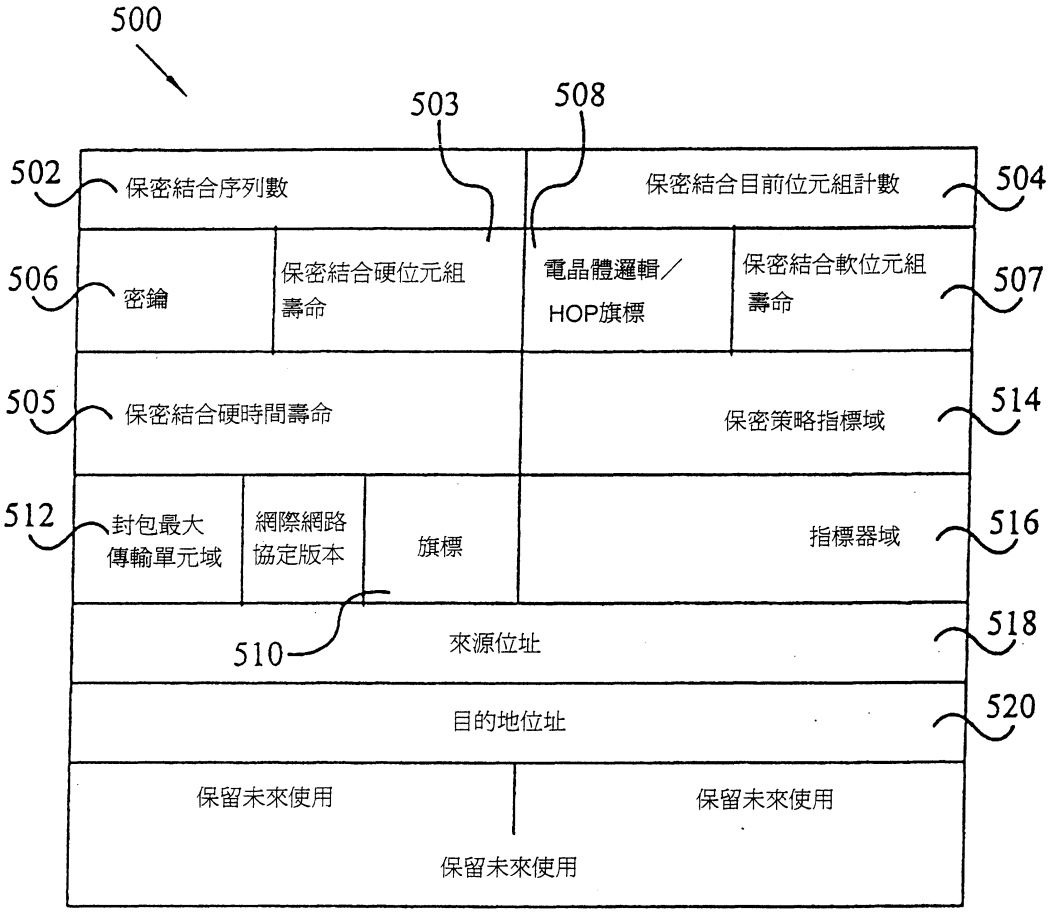
第 2 圖


200
202
204
206
網際網路
協定標頭
上層協定
資料
30
新的網際網路
協定標頭
網際網路保密
協定標頭
網際網路
協定標頭
上層協定
資料
302
304
306

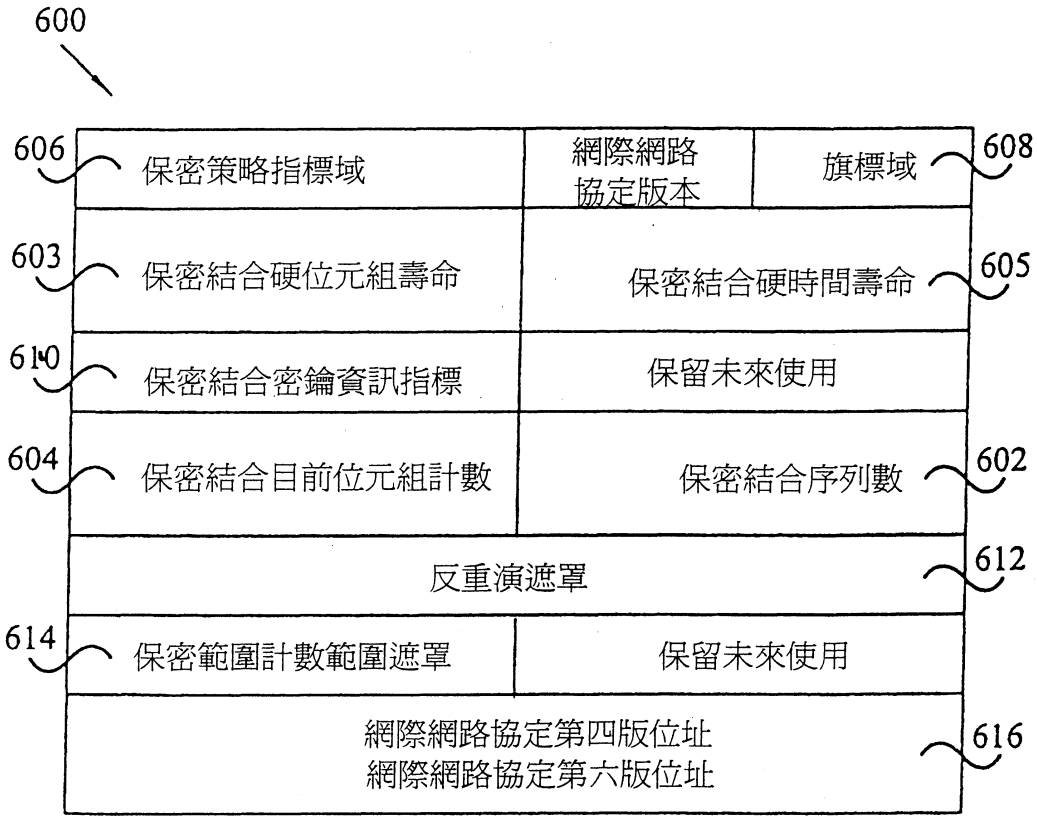
第 3 圖


200
202
204
206
網際網路
協定標頭
上層協定
資料
400
網際網路
協定標頭
網際網路保密
協定標頭
上層協定
資料
402
404
204
406

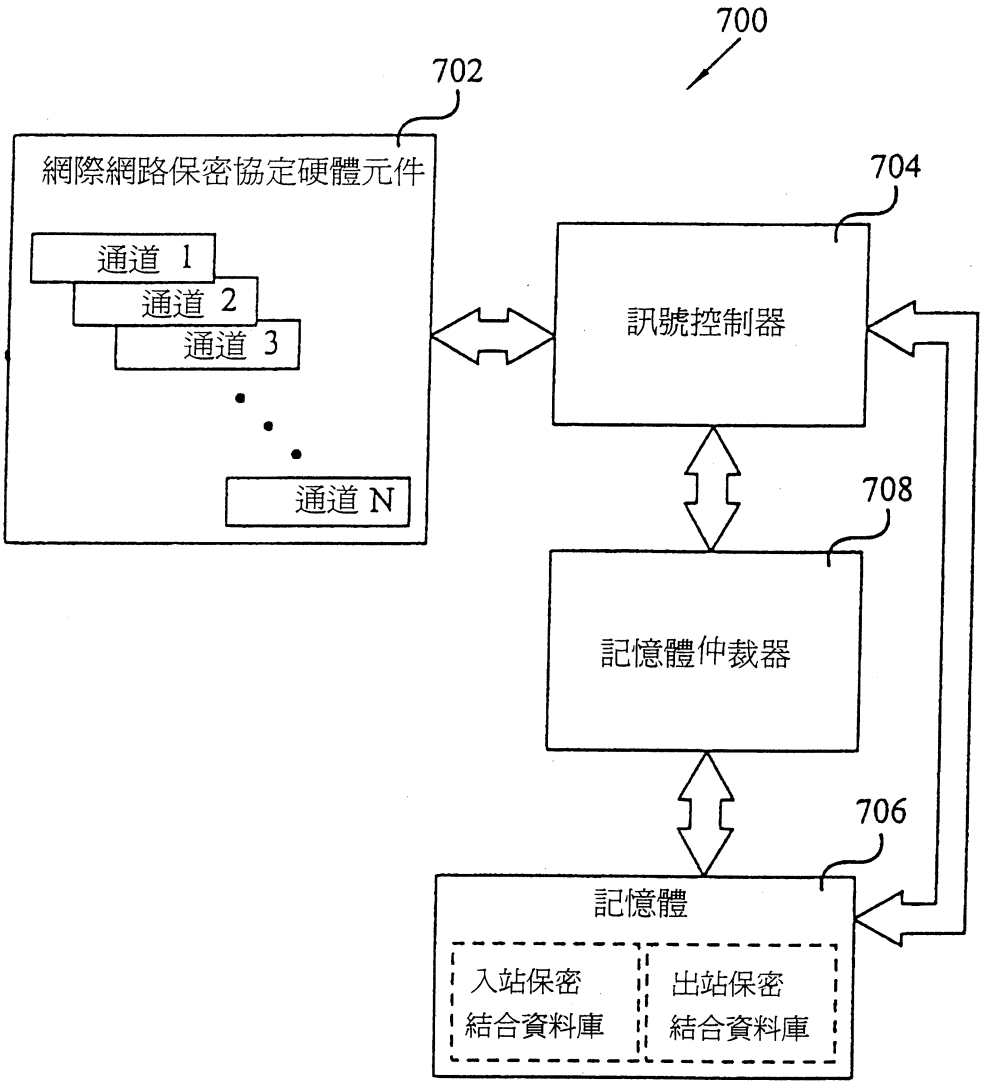
第 4 圖


500
503
508
502
保密結合序列數
保密結合目前位元組計數
504
506
密鑰
保密結合硬位元組壽命
電晶體邏輯／HOP旗標
保密結合軟位元組壽命
507
505
保密結合硬時間壽命
保密策略指標域
514
512
封包最大傳輸單元域
網際網路協定版本
旗標
指標器域
516
510
來源位址
518
目的地位址
520
保留未來使用
保留未來使用
保留未來使用

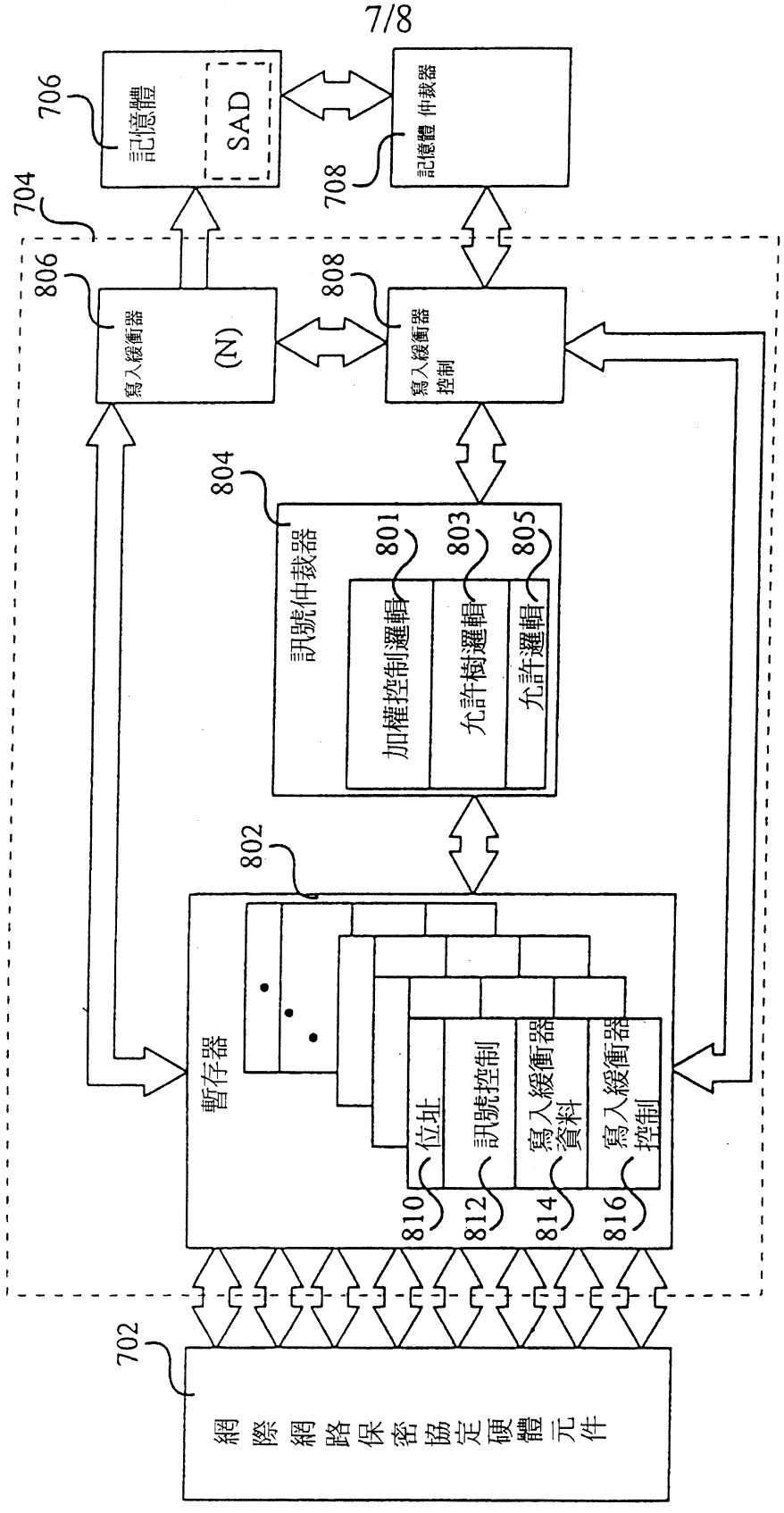
第 5 圖


600
606
保密策略指標域
網際網路
協定版本
旗標域
608
603
保密結合硬位元組壽命
保密結合硬時間壽命
605
610
保密結合密鑰資訊指標
保留未來使用
604
保密結合目前位元組計數
保密結合序列數
602
反重演遮罩
612
614
保密範圍計數範圍遮罩
保留未來使用
網際網路協定第四版位址
網際網路協定第六版位址
616

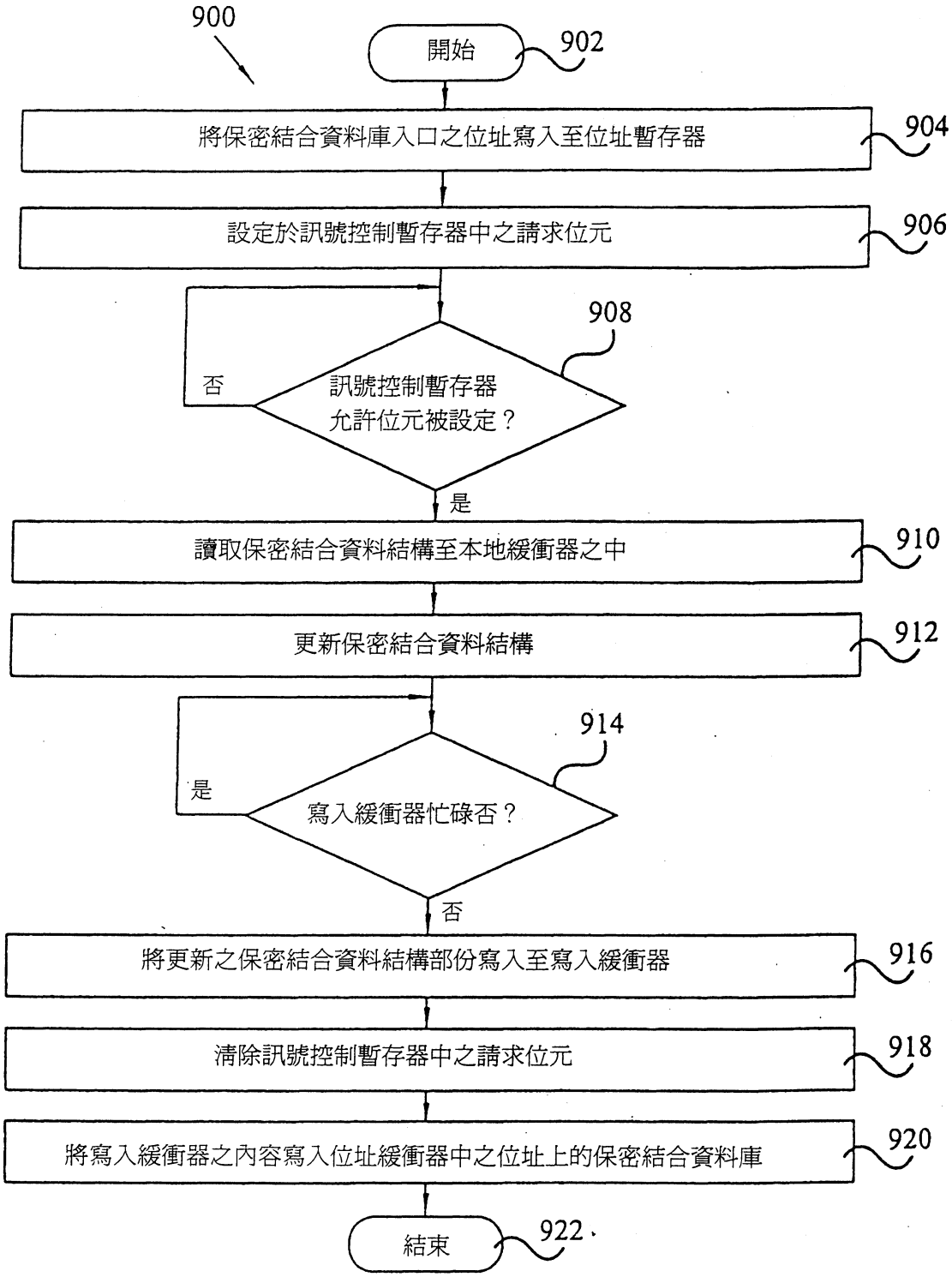
第 6 圖


700
702
網際網路保密協定硬體元件
通道 1
通道 2
通道 3
通道 N
704
訊號控制器
708
記憶體仲裁器
706
記憶體
入站保密
結合資料庫
出站保密
結合資料庫

第 7 圖


706
記憶體
SAD
708
記憶體 仲裁器
704
806
寫入緩衝器
(N)
808
寫入緩衝器
控制
804
訊號仲裁器
801
加權控制邏輯
803
允許樹邏輯
805
允許邏輯
802
暫存器
位址
訊號控制
寫入緩衝器
資料
寫入緩衝器
控制
810
812
814
816
702
網際網路保密協定硬體元件

第 8 圖


900
開始
902
將保密結合資料庫入口之位址寫入至位址暫存器
904
設定於訊號控制暫存器中之請求位元
906
908
否
訊號控制暫存器
允許位元被設定？
是
讀取保密結合資料結構至本地緩衝器之中
910
更新保密結合資料結構
912
914
是
寫入緩衝器忙碌否？
否
將更新之保密結合資料結構部份寫入至寫入緩衝器
916
清除訊號控制暫存器中之請求位元
918
將寫入緩衝器之內容寫入位址緩衝器中之位址上的保密結合資料庫
920
結束
922

第 9 圖