

發明專利說明書 200423669

(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：92135835

※申請日期：92/2/17

※IPC 分類：H04L9/00

壹、發明名稱：(中文/英文)

於一複數頻道串列通信介面上之專屬加密虛擬頻道

DEDICATED ENCRYPTED VIRTUAL CHANNEL IN A
MULTI-CHANNEL SERIAL COMMUNICATIONS INTERFACE

貳、申請人：(共 1 人)

姓名或名稱：(中文/英文)

荷蘭商皇家飛利浦電子股份有限公司

KONINKLIJKE PHILIPS ELECTRONICS N.V.

代表人：(中文/英文)

JL 凡 德 渥

VAN DER VEER, J. L.

住居所或營業所地址：(中文/英文)

荷蘭愛因和文市格羅尼渥街1號

GROENEWOUDSEWEG 1, 5621 BA EINDHOVEN, THE
NETHERLANDS

國 籍：(中文/英文)

荷蘭 THE NETHERLANDS

參、發明人：(共 1 人)

姓 名：(中文/英文)

大衛 R 依佛

EVOY, DAVID R.

住居所地址：(中文/英文)

美國加州聖瓊斯市麥凱大道1109號

1109 MCKAY DRIVE, M/S-41SJ, SAN JOSE, CALIFORNIA 95131,
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12月18日；60/434,796

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12月18日；60/434,796

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】

本發明一般係關於資料通信與資料加密。本發明尤其有關於在一複數頻道串列通信介面上傳達之資料的加密。

【先前技術】

為了保護數位資料免於未經授權的存取，安全管理變得越來越重要。在許多實例中，可利用安全管理來維護安全通信的機密特性，致使只有特定的接收者才可以檢視資訊。此外，為了限制諸如電影、音樂、電視廣播等數位內容的存取，有關數位版權管理的安全管理也變得格外重要。

目前存在著各種安全管理方案。許多方案所利用的加密演算法可在傳達至接收者之前有效拌碼數位資料，因此只有接收者可以解密資料並從中取得資訊。通常，加密的利用與數位認證、公開金鑰基礎建設(Public Key Infrastructure, PKI)及其類似物有關，以確保只有獲得授權的接收者可以解密拌碼的資料。

各種不同類型的通信介面通常都需要安全管理。例如，最好可以在串列通信介面中採用安全管理，因為在傳送與接收模式之間或耦合至串列互連的端點之間，以點對點方式使用串列通信介面的高效能與高頻寬通信資料的應用越來越多。為了不同的運算應用，已經發展諸如通用串列匯流排(Universal Serial Bus, USB)、IEEE-1394及PCI-Express等不同的通信協定。

除了其他特性之外，上述許多串列通信介面標準都支援

將多個頻道的資料流多工處理至單一串列介面的概念，一般可支援如音訊及視訊資料流之時間相依資料的等時傳輸。例如，PCI-Express標準明確支援虛擬頻道的概念，亦即允許此類頻道建立於端點之間，以允許多個資料流可在單一互連上接受多工處理。

PCI-Express標準的期望是找到取代PCI標準的技術應用性；傳統上係在電腦中使用PCI標準將週邊元件連接至中央處理複合。此外，PCI-Express標準最後還可以用來取代電腦及諸如機上盒、DVD播放機等資料處理系統中的一些其他互連技術。

和所有的通信介面一樣，PCI-Express-相容串列互連能夠傳送加密資料。但是，對於資料加密的標準卻沒有明確的支援。一般反而依軟體指示加密資料，致使資料傳送到PCI-Express-相容介面後，已由作業系統或應用軟體進行加密。

然而，使用軟體在串列互連上加密通信用的資料有一些缺點。最明顯的是，軟體式加密與解密會消耗實質的系統資源。此外，當使用多個積體電路或晶片實施任何電腦或資料處理系統時，有一個可能是解密資料可能會沿著晶片邊界受到暴露，亦即沿著將兩個積體電路或晶片一起互連在封裝或電路板中的路徑。

與保障串列互連上傳達之資料安全關連的難題最好的例子可能是在數位版權管理的背景中。例如，媒體與娛樂工業花費大量資源嘗試保護內容，以免駭客找到未經內容提

供者的授權而存取內容的方法。複製保護已成為內容提供者與經銷商為防止未經授權的內容複製所利用的重要工具。此外，隨著諸如電影、電視節目、音樂等內容已轉變成數位格式，更增加了未經授權的複製風險，因為數位複製在品質上通常與其原始內容一樣。因此，極為需要保護數位內容免於未經授權的存取。

為了確保只有獲得授權的使用者可以觀看內容，許多用來播放數位內容的電子裝置都必須採用存取控制的技術。例如，直播衛星(Direct Broadcast Satellite, DBS)機上盒與接收器一般會採用存取控制技術，以確保只有獲得授權的用戶才受允許觀看DBS衛星的內容廣播。同樣的，DVD播放機、遊戲系統及其類似物一般會採用存取控制技術，以確保DVD光碟上的壓縮資料流無法用來複製其中儲存的數位內容。此外，許多DVD採用區域編碼，允許某些地理區域販售的DVD播放機可播放只能在這些地理區域使用的DVD光碟。

機上盒、DVD播放機及其類似物通常會利用嵌埋式電子包裝，其中包括多個積體電路或晶片。此外，在這些應用中必須處理的資料量通常都很大，因此需要相當高的頻寬資料通信能力。由於減少這些裝置成本的必要性，處理資源通常會受到限制，因此，最好可以減少與執行數位資料流加密與/或解密相關的間接費用。此外，此類裝置中所用的積體電路或晶片還提供了未經授權存取數位內容的可能途徑，只要沿著延伸於這些晶片之間的導體信號路徑，監

控晶片間的資料流即可。

由於積體電路的製造方式，使得偵測積體電路內部資料流極為困難，至少與偵測積體電路及其他裝置間的資料流相比是如此。因此，通常最好避免在多個晶片之間進行未加密的數位內容通信。

禁止晶片間未加密的數位內容通信的一個方式是，在相同晶片上採用如解碼及解壓縮數位資料流所用的存取控制功能。例如，DBS衛星廣播與DVD媒體上儲存的數位內容通常利用稱為MPEG的標準來編碼。使用MPEG標準編碼的數位內容為高壓縮，以減少儲存與頻寬上的需求。但是，要在電視上播放之前，必須先將MPEG資料流解碼及解壓縮。然而，形成的解壓縮資料一般因為量太大而無法複製，而且完全需要使用MPEG編碼器進行解壓縮，因而降低了品質並使形成的複製比原始內容差。

DBS衛星傳達與DVD媒體上儲存的MPEG資料流一般藉由存取控制來加密與保護，以允許只有獲得授權的裝置才能解碼MPEG資料以對消費者顯示。

因此，將廣播MPEG資料流轉換至電視或其他顯示裝置的過程，一般涉及兩個獨立步驟。第一，決定授權可觀看內容的機上盒或DVD播放機後，要解密MPEG資料流，必須使用存取控制功能。此解密操作的結果即為解密的MPEG資料流。第二個操作是MPEG解碼，在取得解密的MPEG資料流後將資料流解碼及解壓縮，以產生輸出至電視或其他顯示裝置的音訊與/或視訊資料。

在這兩個操作中間的解密資料流一般可代表原始內容的壓縮與完美複製。因此，為了防止存取此解密資料流，系統設計師的習用策略是在相同的積體電路上採用存取控制邏輯與MPEG解碼器邏輯。

儘管在相同的積體電路上採用存取控制與MPEG解碼可提供一些安全上的優點，但從企業觀點來看仍有一些缺點。首先，MPEG標準的利用與各種的不同技術有關，其中包括上述的DVD與DBS技術。在所有這些不同的技術中，都需要各種不同的存取控制機制。例如，就DBS技術而言，個別用戶(亦即機上盒的持有人)必須受到鑑認。但就DVD技術而言，一般需要區域存取控制。因此，不同應用所用的存取控制邏輯實質上有所不同。

儘管要整合相同積體電路上的存取控制電路與MPEG解碼電路在技術上有點微不足道，但從成本觀點看來，這麼做過於昂貴。由於與開發製造中使用的合適遮罩關連的成本，高效能積體電路設計的啟用成本會非常高昂。半導體工業一般依賴大量製造來收回每個晶片設計相當高昂的啟用成本。因此，即使調適現有的電路設計以採用替代性存取控制電路，也會是一種極為昂貴的做法。

從經濟觀點來看，將存取控制邏輯與解碼邏輯分開，並利用多個晶片來執行分開功能，實質上會更符合成本效益。尤其存取控制電路通常可使用相當簡單的電路來實施。此外，由於串列互連及其類似物相當高的頻寬能力，因此可以使用諸如PCI-Express-相容互連的高速串列互連，在存取

控制與解碼晶片之間傳達資料流。

在許多實例中，最好使用可以與多個類型的存取控制晶片接合的共用MPEG解碼器晶片，以允許MPEG解碼器晶片可以在各種應用中使用。但是，由於駭客攔截解密資料流所造成的合理憂慮，複數晶片實施也不能算是理想的選擇方案。

因此，在本技術中，極為需要在高速通信介面上提供更符合成本效益的安全管理方式，其中包括有關積體電路及其類似物之間的數位資料通信中所用的串列與其他互連。此外，在本技術中，在實施有關保護數位內容的存取控制上，也極為需要更符合成本效益的方式。

【發明內容】

本發明可以解決與先前技術關連的這些及其他問題，其係藉由提供一種在一複數頻道串列通信介面上傳達資料的資料處理系統、電路配置及方法，該複數頻道串列通信介面係使用該通信介面所支援之多個虛擬頻道中之一專屬加密虛擬頻道。用於該專屬加密虛擬頻道的加密係由一耦合至該介面的硬體加密電路提供，致使可按一相當低的位準執行加密，且具有免於洩露的實質保護，尤其在沿著晶片邊界。附加的虛擬頻道一般可支援未加密資料(與/或經由其他機制，例如經由軟體加密的資料)，因而允許加密與未加密資料都可以相當有效、符合成本效益及安全的方式共享一共用介面。

儘管一些替代性具體實施例的設想與本發明一致，但本

發明之一特定應用與提供數位資料流的存取控制有關，如在直播衛星(DBS)接收器、DVD播放機及其類似物等資料處理系統中，支援區域與/或用戶式數位內容的存取控制。與習用之單晶片存取控制方案相比，與本發明一致的具體實施例可利用一複數晶片存取控制方案，該方案係依賴一晶片在一接收的數位資料流上提供存取控制，並在獲得授權後利用另一晶片處理該數位資料流。在該多個晶片間之一安全的複數頻道串列通信介面會：重新加密一已在該存取控制晶片上加密的數位資料流，該存取控制晶片係使用配置在其上的硬體加密邏輯；在一由該複數頻道串列通信介面支援之專屬加密虛擬頻道上傳達該重新加密的數位資料流；以及解密該重新加密的數位資料流，該重新加密的數位資料流係使用配置在該其他晶片上的硬體解密邏輯。

因此，存取控制功能實際上可與最後利用數位資料流的功能分開，同時該數位資料流可保持安全保障，免於橫跨晶片邊界之未經授權的存取。除了其他好處之外，本文所述架構就開發與製造複數晶片設計中所用的個別晶片而言，還可以節省實質成本。

描繪本發明特徵的這些與其他優點與特色，將在本文隨附的申請專利範圍中說明並在本文中形成另一個部分。但是，為了更加瞭解本發明及透過其使用所得到的優點與目的，應該參考圖式與隨附的說明內容，其中說明了本發明的示範性具體實施例。

【實施方式】

以下所述具體實施例在如PCI-Express-相容互連之複數頻道串列通信介面中採用專屬加密虛擬頻道。與本發明一致之複數頻道串列通信介面一般採用共享一共用串列通信路徑之多個「虛擬」頻道的概念。在許多通信協定中，會在共用串列通信路徑上多工處理虛擬頻道，如使用時間式多工處理。例如，在PCI-Express-相容通信介面中，會支援稱為「等時」頻道的多個虛擬頻道，且這些多個頻道能個別透過明確定義的通信協定來建立與配置。

串列通信介面的一或多個與本發明一致之虛擬頻道可配置成「專屬」加密虛擬頻道。與本發明一致之專屬加密虛擬頻道一般利用配置在相同積體電路或晶片上的硬體式加密與/或解密邏輯，如用來在複數頻道串列通信介面上傳達的介面電路。此外，此硬體式邏輯耦合至介面電路的方式，致使在專屬加密虛擬頻道上傳達的所有資料(例如)經由介面電路與加密/解密邏輯間的直接信號路徑來加密。因此，在許多具體實施例中，最好在專屬加密虛擬頻道上傳達資料的加密，以便無法略過或停用加密資料。

應明白，在複數頻道串列通信介面中的其他虛擬頻道可以加密或不加密，且如果有任何加密的話，也可以在硬體與/或軟體中實施加密。此外，儘管在專屬加密虛擬頻道上傳達的資料一直會加密，但其他與專屬加密虛擬頻道的建立相關的資料，如設定資料、控制資料、授權資料、公開金鑰等，可以在另外的虛擬頻道上以加密或不加密的方式來傳達。

還應明白，本發明的利用可與PCI-Express-相容介面以外的複數頻道串列通信介面有關。因此，儘管以下說明的具體實施例的重點會是本發明有關PCI-Express介面的一項特定應用，但本發明並不因此受限。

一般而言，應明白，以下討論的任何硬體式功能一般可在一或多個積體電路或晶片以及視需要加入之附加支援電子元件採用的電路配置中實施。此外，如本技術中所熟知的，一般使用一或多個電腦資料檔案設計與製造的積體電路，本文稱為硬體定義程式碼，其可定義裝置上電路配置的布局。程式碼一般係由設計工具產生，隨後並在製造期間使用以建立定義用於半導體晶圓之電路配置的布局遮罩。一般可以使用諸如VHDL、verilog、EDIF等硬體定義語言(hardware definition language, HDL)的預定格式來提供程式碼。儘管本發明已經且將在下文說明，在完全作用之積體電路與利用該積體電路的資料處理系統中實施的電路配置背景，但熟悉本技術者應明白，與本發明一致之電路配置也可以像程式產品以各種形式分布，且無論實際執行分布所用之信號載送媒體的特定類型，本發明均同樣適用。信號載送媒體的範例包括，但不限於：諸如揮發與非揮發性記憶體裝置、軟式磁碟與其他可移磁碟、硬碟驅動機、磁帶、光碟(如CD-ROM、DVD等)等可錄類型媒體及諸如數位與類比通信鏈路的傳輸類型媒體。在一些與本發明一致之具體實施例中，其他積體電路技術，如FPGA技術及其類似物也可用來實施本文所述的部分硬體式功能。

現在請看圖式，其中相同的號碼代表圖式中相同的零件，圖1顯示示範性資料處理系統10，該系統採用具有與本發明一致之專屬加密虛擬頻道的複數頻道串列通信介面。資料處理系統10包括經由複數頻道串列互連14耦合至週邊裝置16的主機裝置12。在不同的具體實施例中，裝置12、裝置16可配置在相同或不同的積體電路上，甚至可以配置在分開的電路板、封裝、外殼上等。此外，應明白，其他裝置可耦合至與本發明一致之複數頻道串列互連。在顯示的具體實施例中，互連14係為PCI-Express-相容互連。因此，裝置12、裝置16可藉由點對點連接來耦合，或也可在裝置12、裝置16之間利用中間裝置，如橋接器或切換器。

在此說明設計中，將主機裝置12顯示為包括處理器18與記憶體20，而將週邊裝置16顯示為包括複數個邏輯方塊，22、24、26、28，該等方塊代表存在週邊裝置上的不同邏輯電路。與業界專門用語一致，這些邏輯方塊可稱為智慧財產(Intellectual Property, IP)方塊，代表可與積體電路上其他電路組合的自含設計。然而，應明白，幾乎任何邏輯電路均可配置在與本發明一致之主機裝置12或週邊裝置16的任一個裝置上。

在此說明資料處理系統中，還顯示一適合用來將安全資料從週邊裝置16傳達至主機裝置12的示範性配置。各裝置12、裝置16包括複數頻道串列端點電路30、複數頻道串列端點電路32，其係配置成用以多工處理複數頻道串列互連14上的複數個虛擬頻道(頻道0-2顯示於圖1用來示範)。由於

使用 PCI-Express 通信協定實施資料處理系統 10，因此電路 30、電路 32 各可包含標準 PCI-Express-相容 IP 方塊。不過，在其他的設計中，可在選擇方案中使用自訂端點電路。

資料處理系統 10 支援專屬加密虛擬頻道 (此處為虛擬頻道 1) 的概念，以便使用安全的方式將資料從週邊裝置 16 傳達至主機裝置 12。在此考量下，週邊裝置 16 包括配置成用以耦合至頻道 1 互連或輸入至端點 32 的硬體加密邏輯 34。加密邏輯 34 一般經由直接信號路徑耦合至端點 32 的頻道 1 互連，且是頻道 1 互連唯一的連接，因此確保只有加密資料可在複數頻道串列互連的頻道 1 上傳達。

對應的硬體式解密邏輯電路 36 配置在裝置 12 中，且耦合至頻道 1 互連或端點 30 的輸出。因此，解密邏輯 36 可解密在複數頻道串列互連的虛擬頻道 1 上傳送的任何加密資料。此外，為了提供共用路徑至記憶體 20 中，提供多工器 38 以耦合解密邏輯 36 的輸出以及任何其他至記憶體 20 的虛擬頻道。

為了實施與本發明一致之專屬加密虛擬頻道，可設計加密邏輯 34 與解密邏輯 36 以支援幾乎任何加密/解密演算法，包括，例如 PKI、RSA DES 與 Triple DES 等。應明白，可在專屬加密虛擬頻道上，或在選擇方案中的另外頻道上，將附加資料，例如存取或控制資料與/或公開金鑰資訊傳達至方塊 34、方塊 36 之一。

例如，虛擬頻道 0 係為可在其上傳達控制與存取資訊的預設頻道。因此，最好是將各 IP 方塊 22、方塊 24、方塊 26 及

方塊28耦合至頻道0以支援這些方塊的各個功能，以由主機裝置(例如，經由處理器18在虛擬頻道0上發出的指令)進行適當配置。此外，最好進一步將頻道0耦合至加密邏輯34(例如經由圖1所示的唯寫路徑)，以允許藉由，例如，將解密邏輯36的公開金鑰轉接至加密邏輯34來建立專屬加密虛擬頻道。

在此說明範例中，將會顯示一些變化。例如，如上所述，可將虛擬頻道0建立為預設頻道，而將虛擬頻道1建立為其上只傳達加密資料的專屬加密虛擬頻道。另一方面，頻道2可以是習用之虛擬頻道，可視需要運載加密與/或未加密資料。

此外，可從IP方塊22、方塊24、方塊26及方塊28看出，可將裝置16中的邏輯方塊耦合至不同的頻道以支援不同的功能。例如，可將IP方塊22視為正常最佳工作量裝置，其上通信則限於預設頻道0。另一方面，IP方塊24只耦合至加密邏輯34，因此，方塊24與裝置12之間的唯一通信係在加密虛擬頻道上。圖中也顯示方塊24耦合至虛擬頻道0；不過，在許多具體實施例中，最好能限制此類存取以建立存取控制，例如，以交換公開金鑰或允許主機裝置能選擇性啟用方塊。因此，在部分具體實施例中，最好只提供從虛擬頻道0至IP方塊24的單向路徑，致使IP方塊24無法在虛擬頻道0上傳達資料。

方塊26顯示可選擇性經由專屬加密虛擬頻道1或虛擬頻道2傳達的邏輯電路。同樣的，方塊28顯示只在虛擬頻道2

上傳送資料的邏輯方塊，而且不使用經由加密邏輯34的加密。為了支援多個邏輯方塊可利用虛擬頻道2，在選擇方案中可以使用40處所示的多工器或其他選路邏輯。

應明白，在圖1所示的配置中，以及利用習用PCI-Express IP方塊的各介面電路30、介面電路32，所有實施專屬加密虛擬頻道所需的有效負載修改可於電路30、電路32外部實施。因此，不用對PCI-Express標準進行任何修改，即可實施專屬加密虛擬頻道。

為了建立專屬加密虛擬頻道，必須根據建立虛擬頻道的PCI-Express通信協定初始化虛擬頻道。應明白，為了初始化合適數量的虛擬頻道及為了在專屬加密虛擬頻道上對加密資料流進行初始化加密與授權解密所實施的合適邏輯，係在從實例揭示受益之一般熟悉本技術者的能力範圍內。還應明白，只要是對任何特定應用是最好的，與本發明一致之複數頻道串列互連可利用任何數量的虛擬頻道及任何數量的專屬加密虛擬頻道。

在與本發明一致之專屬加密虛擬頻道中，所有在虛擬頻道上傳達的資料均已加密。應明白，在公開金鑰的利用與存取控制關連的實施中，可不時更新這些公開金鑰，且在部分具體實施例中可選擇不同的加密方案。但是，在許多具體實施例中，最好採用無法在特定專屬頻道上略過的預設加密方案。藉由這麼做，且另外藉由提供傳達非加密資料(或已經由軟體加密的資料)的附加頻道，即可讓多項使用共享共用的匯流排資源，通常可降低成本並增加要將哪個

部分的資料加密的彈性。此外，隨著下文將會更加明白，當複數頻道串列互連的端點配置在分開的積體電路上時，可實質上增進加密資料的安全。

還應明白，對複數頻道串列互連上傳達的資料進行編碼或修改的其他方式，專屬加密虛擬頻道的加密可做為補助。例如，PCI-Express通信協定可拌碼鏈路上傳達的所有資料，主要目的是為了展開橫跨更廣頻率範圍所產生的電子雜訊頻譜，並藉此降低峰值發射。儘管此拌碼形式可視為加密形式，但此拌碼目的並非保護數位版權，事實上，由於解碼演算法已眾所皆知，因此要解碼相當容易。因此，本文所述方式中指定頻道的加密實質上在PCI-Express環境中，比標準以其他方式所提供的提供更大安全性。

各種替代性設計的使用可與本發明一致。例如，如圖2至5所示，在一些替代性方式中，IP方塊可耦合至複數頻道串列端點。例如，如圖2所示，積體電路50可包括含有多個虛擬頻道54、虛擬頻道56、虛擬頻道58及虛擬頻道60的複數頻道串列端點52。虛擬頻道56與虛擬頻道58可配置成專屬加密虛擬頻道。IP方塊62可經由加密邏輯64耦合至虛擬頻道56，以按上述方式在虛擬頻道56上傳達加密資料。同樣的，在解密邏輯68提供加密資料流的解密之下，加密虛擬頻道58可從串列互連接收加密資料以由IP方塊66消耗。因此，可以看出，相同的積體電路上可同時支援加密與解密。

儘管將虛擬頻道56、虛擬頻道58的特性顯示為單向，但

應明白，與本發明一致之虛擬頻道的特性也可以是雙向。如圖3所示，例如，積體電路70可包括支援複數個虛擬頻道74、虛擬頻道76及虛擬頻道78的複數頻道串列端點72。虛擬頻道76可配置成具有雙向特性的專屬加密虛擬頻道。因此，IP方塊80既可以製作也可以消耗加密資料。為了支援此類功能，加密邏輯82可配置在方塊80與端點72的中間，以加密預定送往串列互連的送出資料。同樣的，對於傳入的加密資料，解密邏輯84可以耦合在IP方塊80與端點72的中間。

同樣如上所述且如圖4進一步所示，配置在積體電路上的IP方塊能在多個虛擬頻道上進行傳達。圖4的積體電路90，例如，包括支援複數個虛擬頻道94、虛擬頻道96及虛擬頻道98的複數頻道串列端點92，其中虛擬頻道94為未加密頻道，及虛擬頻道96為專屬加密虛擬頻道。IP方塊100可在頻道94、頻道96之一上傳達，其中含介於IP方塊100與端點92之間的102所代表的加密與/或解密邏輯，以支援在專屬加密虛擬頻道上傳達的加密資料的加密與/或解密。

此外，如圖5所示，多個IP方塊可以共享給定的專屬虛擬頻道。圖5的積體電路110，例如，顯示了支援複數個虛擬頻道114、虛擬頻道116及虛擬頻道118的複數頻道串列端點112。虛擬頻道116配置為專屬加密虛擬頻道，及多個IP方塊120、方塊122經由加密與/或解密邏輯124耦合至虛擬頻道116以促進此類方塊之資料的安全通信。選擇性多工器126或其他交換邏輯可用來接合多個IP方塊及與本發明一

致之加密虛擬頻道。

圖6接著顯示本文所述之複數頻道串列互連的特定應用，以用於如DBS機上盒或接收器130之資料處理系統中提供存取控制。如習用的DBS機上盒，可在機上盒中提供調諧器/解調器邏輯132，以從衛星接收器(一般以134表示)，一般從LNB降頻器，解調變所接收的衛星信號。DBS廣播信號可解調變至加密的數位資料流，以提供存取控制及防止數位資料流未經授權的存取。此加密資料流可提供至機上盒的控制器，此處以處理器晶片組136表示。晶片組136進一步耦合至記憶體138及用來驅動視訊顯示與/或外部音訊電路的音訊/視訊輸出電路140。此外，藉由使用者輸入電路，一般以142表示，使用者輸入，例如，經由前方面板按鈕與/或遙控器，可提供至處理器晶片組136。此外，可經由存取或智慧卡144的使用來支援存取控制功能，其係利用146表示的存取卡連接器耦合至處理器晶片組。

如本技術所熟知，DBS機上盒傳統上可由智慧卡連接器提供，以使個別單元可根據特定用戶的訂閱設定分開授權。存取卡一般與特定用戶帳號關連，致使授權可受到嚴密監控與控制。

如上所述，習用之DBS機上盒設計一般會在相同的積體電路中，同時採用DBS衛星信號的存取控制與解碼。相反的，機上盒130，尤其是處理器晶片組136，則利用一對積體電路148與積體電路150，其中積體電路148可提供存取控制邏輯，及積體電路150可提供解碼器邏輯，還有附加的處

理與控制邏輯可管理機上盒的整體操作。採用與本發明一致之專屬加密虛擬頻道的複數頻道串列互連152將積體電路148與積體電路150互相耦合。如下文將會說明的，為了在積體電路148、積體電路150之間保護沿著晶片邊界的數位資料流，可在晶片之間按加密方式傳達代表DBS廣播信號的數位資料流。

具體而言，如圖7中比較詳細的顯示，可將複數頻道串列互連152配置為PCI-Express互連，並具有為了說明而概略顯示的四個虛擬頻道。為了控制積體電路148與積體電路150之間的各種操作，例如建立任何專屬加密虛擬頻道的存取控制，虛擬頻道0可以是傳達明確資料所需的預設固定頻道。可將虛擬頻道1顯示為固定與專屬加密虛擬頻道，而將虛擬頻道2與虛擬頻道3顯示為不同應用中最好配置能傳達加密或未加密資料的彈性頻道。為了支援多個頻道，積體電路150包括具有至少四個頻道互連支援的PCI-Express串列介面電路154、PCI-Express串列介面電路156，以便在各個晶片上傳達其他邏輯電路的虛擬頻道資料。

為了支援安全接收授權的DBS程式設計，積體電路148包括可實施機上盒所需存取控制功能之指定用戶的解密邏輯方塊158。同樣的，為了支援將壓縮資料流解碼為未壓縮的音訊與/或視訊資料，積體電路150包括MPEG解碼器邏輯方塊160。

為了確保積體電路148與積體電路150之間的晶片邊界安全，會在專屬加密虛擬頻道1上傳達資料流(此處為壓縮但

解密之MPEG資料的資料流)，在此考量下，指定平台的加密與解密邏輯162、加密與解密邏輯164分別配置在各積體電路148、150之上。為了建立合適的存取控制，以及為了在積體電路148、150之間建立安全連線，積體電路包括耦合至虛擬頻道0且配置成用以傳達由積體電路148所消耗之控制、狀態、存取及金鑰產生資料的邏輯方塊166。

同樣如圖7所示，在部分具體實施例中，壓縮資料流可包括未加密或未受限的資料。在此類實例中，最好也能提供壓縮資料流至虛擬頻道2及直接至MPEG解碼器方塊160。應明白，此類資料在串列互連152上傳達時，不會受到存取控制方式的影響，也不會受到加密。

還應明白，附加的IP邏輯，一般以方塊168與方塊170表示，也可以配置在各積體電路上以在如虛擬頻道3之附加虛擬頻道上傳達。附加邏輯，包括機上盒許多的處理與控制邏輯，也可以在積體電路148與積體電路150之一或二者中採用，或是在處理器晶片組中配置的附加積體電路中採用。此類附加功能為熟悉本技術者所充分瞭解，因此從圖7中省略。

如所配置的，壓縮的存取控制資料流可由代表加密資料流的方塊158接收。在由方塊158視需要授權及解密後，形成的解密資料流可提供至方塊162以執行指定平台的加密。然後可在專屬加密虛擬頻道上提供此加密資料流由方塊164進行解密。在積體電路148與積體電路150之間的晶片邊界，應明白，在晶片邊界上傳達的資料會加密，因此不

會遭到洩露。方塊164接著會以補充的方式解密方塊162所提供的加密資料流，及將此現在已解密但仍壓縮的資料流提供至MPEG解碼器方塊160。方塊160接著會以習用之方式解壓縮及解碼資料流，因而產生可從機上盒輸出之未壓縮的音訊與/或視訊資料。

此配置可以得到一些優點。首先，可將存取控制與解碼功能分成兩個分開的積體電路，以允許不同的解碼演算法可視需要透過結合不同的晶片設計來利用不同的存取控制演算法。

此外，由於存取控制功能通常可以在相當簡單的邏輯電路中實施，因此在部分具體實施例中，可以實施使用如FPGA之場可程式化邏輯的積體電路148。因此，積體電路的存取控制邏輯可以極為符合成本效益與高度可自訂的方式來建立，而不用對業已存在的晶片設計進行昂貴的修改。

應明白，根據給定設計中所用的串列通信協定與加密演算法，虛擬頻道的初始化與專屬加密虛擬頻道的建立也會有所變化。例如，圖8顯示可對圖7電路執行的示範性常式，以初始化複數頻道串列互連，且建立與其有關的合適專屬加密虛擬頻道。

特別的是，圖8顯示可依作為複數頻道串列互連(如PCI-Express)主機的裝置指示而執行的初始化互連常式172。常式172可以藉由，例如，資料處理系統的電源開啟來啟動。此時係假設所有互連暫存器一般已重設。

常式172始於方塊174，其係藉由初始化匯流排架構，包

括建立預設虛擬頻道(虛擬頻道0)，一般係根據已知的PCI-Express通信協定。在此初始化過程中，可經由硬體建立鏈路通信，且一般不用主機處理器介入，以允許第一通信能橫跨頻道來產生。在此階段結尾，只支援主機處理器的配置週期。所有端點間的鏈路，亦即主機、週邊設備、切換器、橋接器等之間個別的點對點連接，一般不用主機處理器的協助即可達到此狀態。

建立鏈路通信後，可由主機處理器執行配置週期以配置所有切換器與端點，以設定整體匯流排架構，同樣根據PCI-Express通信協定。藉由這麼做，可視需要啟用記憶體與I/O空間。此時，已可進行記憶體操作，因此週邊裝置中個別的IP方塊可以讀取與寫入主機裝置中的記憶體空間。主機裝置中個別的IP方塊也可以讀取與寫入週邊裝置中的記憶體空間。然而，此時，在配置過程中，預設頻道0以外的虛擬頻道並未啟用，因此部分週邊裝置與/或IP方塊無法使用。此外，專屬加密虛擬頻道也尚未建立。

接著，如方塊176所示，為特定複數頻道串列互連所需之各附加虛擬頻道配置了頻寬。特別的是，在主機處理器上執行的軟體一般可用來根據PCI-Express通信協定設定所需的虛擬頻道，並使用預設頻道0設定所有其他虛擬頻道的頻寬配置。此時，可以進行等時操作，及任何週邊裝置中的個別IP方塊一般可以使用等時傳送的保證頻寬來讀取與寫入主機裝置中的記憶體，並可在所有頻道上執行最佳工作量傳送。

不過，此時，專屬加密虛擬頻道還是無法使用。特別的是，在專屬加密虛擬頻道上接收的任何資料，一般將以初始化該頻道的硬體加密邏輯以在電源重設 (Power On Reset, POR) 後使用的任何金鑰來加密。此金鑰並非對應之硬體解密邏輯在專屬加密虛擬頻道所用的公開金鑰，因此在該頻道上傳送的任何資料無法由硬體解密邏輯破解。

因此，方塊 178 可為各專屬加密虛擬頻道初始化設定密碼的迴路，以授權安全的通信。對各個此類頻道而言，方塊 180 可取得該頻道之硬體解密邏輯的金鑰。此即公開金鑰，一般不需要保護。根據系統需求，如何取得此金鑰以及金鑰的數量、各個金鑰的長度及所用的加密演算法也會不一樣。一個可行的方法是讓主機處理器上執行的軟體從解密邏輯中的暫存器讀取此金鑰。或是，可將金鑰編碼為軟體中的常數。例如，解密邏輯的加密與解密金鑰可以軟體產生，其中將解密單元的私有金鑰載入解密邏輯，及以某種方式，例如，經由軟體可存取之專屬暫存器中的儲存裝置，讓軟體可以使用與此私人金鑰配對的公開金鑰。

接下來，如方塊 182 與方塊 184 所示，在預設虛擬頻道 0 上傳達公開金鑰並將其儲存在專屬加密虛擬頻道的加密邏輯中。特別的是，使用頻道 0 配置週期，解密邏輯的公開金鑰可寫入週邊裝置的硬體加密邏輯，因此提供必要的金鑰以允許硬體加密邏輯可以使用只有該專屬加密虛擬頻道的硬體解密邏輯能正確解密資料的方式將資料解碼。

在使用對應之硬體解密邏輯的公開金鑰更新硬體加密邏

輯後，在專屬加密虛擬頻道上之後的資料通信可使用該金鑰來加密。因此，如方塊186所示，接著可以啟用任何依賴專屬加密虛擬頻道的IP方塊，藉此將由解密邏輯解密專屬加密虛擬頻道上之該等方塊所進行的通信。

完成方塊186後，控制將返回方塊178以建立任何附加專屬加密虛擬頻道上的安全通信。所有此類頻道都已建立後，常式172既已完成。

請注意，常式172可在不同的應用中變化。例如，在部分具體實施例中，由於允許部分IP方塊可在多個虛擬頻道上傳達，因此最好只在所有專屬加密虛擬頻道均已建立後才啟用IP方塊。適合其他安全通信協定與/或串列互連架構的其他初始化常式的使用可以與本發明一致。

現在請稍微回到圖6，應明白，DBS接收器130中的晶片148、晶片150一般配置在相同的電路板上或可能在相同的複數晶片封裝或模組中，藉此複數頻道串列互連152一般可配置在電路板上。在選擇方案中，最好可以採用在多個電路板之間延伸的複數頻道串列通信介面。例如，如圖9所示，最好可以藉由專屬加密虛擬頻道的複數頻道串列互連，在採用耦合至中央控制器之內建邏輯晶片的「智慧」存取卡中，採用存取控制功能。

圖9特別顯示可從衛星接收器202接收衛星廣播信號並使用調諧器/解調器邏輯204解調變該廣播信號的DBS接收器200。DBS廣播信號可解調變至加密的數位資料流，以提供存取控制及防止數位資料流未經授權的存取。此加密資料

流可提供至機上盒的控制器，此處以處理器晶片組206表示。晶片組206可進一步耦合至記憶體208及音訊/視訊輸出電路210與使用者輸入電路212。

處理器/解碼器晶片214係配置在處理器晶片組206之中。不過，並不在處理器晶片組206中採用內建存取控制晶片，而是將存取卡連接器216配置成用以接受智慧存取卡218，該智慧存取卡可提供存取控制功能並經由複數頻道串列互連220耦合至處理器晶片組206。

配置在存取卡218上的是複數頻道串列介面電路222，例如PCI-Express介面電路。配置方式與圖7中方塊158與方塊162相似之指定用戶的解密方塊224與指定平台的加密方塊226，也配置在該存取卡上。

在此具體實施例中，互連220的配置包括三個虛擬頻道，其中頻道0為預設控制頻道，頻道1為專屬加密虛擬頻道，及頻道2為未加密頻道。在此具體實施例中，由解調器204輸出的壓縮加密資料流可經由互連220的頻道2提供至方塊222，其中由方塊224產生之重新加密的資料流會返回專屬加密虛擬頻道1上的處理器晶片組。請注意，在機上盒200與存取卡218之間傳達的資料，一直會由內容提供者(在用戶式解密之前)或由DBS接收器(藉由方塊224)進行加密。因此，可有效保障數位資料流的安全並保護免於未經授權的竄改。

除了其他優點之外，在存取卡中採用存取控制功能還可允許內容提供者以相當符合成本效益的方式，不時更新與

修改存取控制與數位版權管理演算法。因此，要是駭客洩露設定的存取控制方案，將不用更換或修改個別的DBS機上盒，即可用另一種控制方案取代。

接著，如上所述，上述存取控制功能的使用可與DBS接收器及其類似物以外的資料處理系統有關。例如，圖10顯示DVD播放機230，其中包括配置成用以讀取DVD媒體234之資料流及提供解調變、壓縮及加密資料流至處理器晶片組236(依序耦合至記憶體238、音訊/視訊輸出電路240及使用者輸入電路242)的光學驅動機電路232。晶片組236包括藉由採用專屬加密虛擬頻道的複數頻道串列互連248耦合至處理器/解碼器晶片246的區域存取晶片244。

應明白，DVD播放機230可利用如圖6之DBS機上盒130與圖9之DBS機上盒200之一的相同處理器/解碼器積體電路。藉由利用適當的區域存取晶片244、採用區域存取邏輯與本文所述之硬體加密邏輯和複數頻道串列介面邏輯，DBS機上盒中所用之相同基礎的處理器/解碼器設計可隨時調適用於DVD播放機中。

本文所述具體實施例提供一些勝於習用設計的優點。例如，藉由使用專屬加密虛擬頻道，加密與非加密資料通常都能共享單一的通信資訊，因而可以節省成本。此外，如上所示，專屬加密虛擬頻道可以促進加密資料的安全，尤其在橫跨晶片邊界上。

從實例揭示受益之一般熟悉本技術者應明白各種附加的修改。因此，本發明在於下文隨附的申請專利範圍。

【圖式簡單說明】

圖1為資料處理系統的方塊圖，該系統採用具有與本發明一致之專屬加密虛擬頻道的複數頻道串列通信介面。

圖2至5的方塊圖顯示與本發明一致之複數頻道串列通信介面中，邏輯方塊、硬體加密邏輯及硬體解密邏輯的示範性替代性配置。

圖6為採用處理器晶片組之直播衛星接收器的方塊圖，該晶片組利用與本發明一致之複數頻道串列通信介面。

圖7為圖6之處理器晶片組的方塊圖。

圖8為顯示示範性互連初始化常式的流程圖，該常式可用來在圖6與圖7中所示的複數頻道串列通信介面上建立安全通信。

圖9為圖6直播衛星接收器之替代性直播衛星接收器的方塊圖，且採用的存取卡係利用與本發明一致之複數頻道串列通信介面。

圖10為採用處理器晶片組之DVD播放機的方塊圖，該晶片組利用與本發明一致之複數頻道串列通信介面。

【圖式代表符號說明】

0, 1, 2, 3	虛擬頻道
10	資料處理系統
12	主機裝置
14, 152, 220, 248	複數頻道串列互連
16	週邊裝置

18	處理器
20, 138, 208, 238	記憶體
22, 24, 26, 28, 166	邏輯方塊
30, 32	複數頻道串列端點電路
34	硬體加密邏輯
36	解密邏輯電路
38, 40, 126	多工器
50, 70, 90, 110, 148, 150	積體電路
52, 72, 92, 112	複數頻道串列端點
54, 56, 58, 60,	虛擬頻道
62, 66, 80	IP方塊
64, 82, 102, 124	加密邏輯
68, 84, 102, 124	解密邏輯
74, 76, 78, 94, 96, 98,	虛擬頻道
100, 120, 122, 168, 170	IP方塊
114, 116, 118	虛擬頻道
130	接收器
132, 204	調諧器/解調器邏輯
134, 202	衛星接收器
136, 206	處理器晶片組
140, 210, 240	音訊/視訊輸出電路
142, 212, 242	輸入電路

144	存取或智慧卡
146, 216	存取卡連接器
154, 156	PCI-Express 串列介面電路
158	解密邏輯方塊
160	解碼器邏輯方塊
162, 164	加密與解密邏輯
172	初始化互連常式
174, 176, 178, 180, 182, 184, 186	方塊
200	DBS接收器
214, 246	處理器/解碼器晶片
218	智慧存取卡
222	複數頻道串列介面電路
224	解密方塊
226	加密方塊
230	DVD播放機
232	光學驅動機電路
234	DVD媒體
236	晶片組
244	區域存取晶片

伍、中文發明摘要：

本發明係揭示一種在一複數頻道串列通信介面(14)上傳達資料的資料處理系統、電路配置與方法，該複數頻道串列通信介面係使用該通信介面(14)所支援之多個虛擬頻道中之一專屬加密虛擬頻道。用於該專屬加密虛擬頻道的加密係由一耦合至該介面的硬體加密電路(34)來提供，致使可按一相當低的位準執行加密，且具有免於洩露的實質保護，尤其在沿著晶片邊界。在一特定的應用中，可將存取控制提供給使用一複數晶片存取控制方案的數位資料流，該方案係依賴一晶片(148)在一接收的數位資料流上提供存取控制，並在獲得授權後利用另一晶片(150)處理該數位資料流。在該多個晶片間之一安全的複數頻道串列通信介面會：重新加密一已在該存取控制晶片(148)上加密的數位資料流，該存取控制晶片(148)係使用配置在其上的硬體加密邏輯(162)；在一由該複數頻道串列通信介面支援之專屬加密虛擬頻道上傳達該重新加密的數位資料流；以及解密該重新加密的數位資料流，該重新加密的數位資料流係使用配置在該其他晶片(150)上的硬體解密邏輯(164)。

陸、英文發明摘要：

A data processing system, circuit arrangement, and method communicate data over a multi-channel serial communications interface (14) using a dedicated encrypted virtual channel from among multiple virtual channels supported by the communications interface (14). Encryption for the dedicated encrypted virtual channel is provided by a hardware encryption circuit (34) that is coupled to the interface, such that encryption may be performed at a relatively low level, and with substantial protection from compromise, particularly along chip boundaries. In one particular application, access control may be provided for a digital data stream using a multi-chip access control scheme that relies on one chip (148) to provide access control over a received digital data stream, with another chip (150) utilized to process the digital data stream once authorized to do so. A secure, multi-channel serial communications interface between the multiple chips re-encrypts a digital data stream that has been decrypted on the access control chip (148) using hardware encryption logic (162) disposed on the access control chip (148), communicates the re-encrypted digital data stream over a dedicated encryption virtual channel supported by the multi-channel serial communications interface, and decrypts the re-encrypted digital data stream using hardware decryption logic (164) disposed on the other chip (150).

拾、申請專利範圍：

1. 一種資料處理系統，其包括：

一第一積體電路，該第一積體電路包括：一配置成用以產生一資料流之第一邏輯方塊；一耦合至該第一邏輯方塊且配置成用以加密該資料流以產生一加密資料流之硬體加密電路；及一配置成用以在複數個PCI-Express虛擬頻道上支援資料通信之第一PCI-Express-相容介面電路，其中該複數個PCI-Express虛擬頻道包括一未加密的預設虛擬頻道與一配置成用以專門傳達加密資料之專屬加密虛擬頻道，其中該第一PCI-Express-相容介面電路包括複數個頻道互連，各頻道互連與該複數個虛擬頻道中之一虛擬頻道關連，其中該複數個虛擬頻道中之一第一頻道互連耦合至該硬體加密電路以接收該加密資料流，及其中該第一PCI-Express-相容介面電路係配置成用以在該專屬加密虛擬頻道上從該硬體加密電路傳達該加密資料流；

一第二積體電路其藉由一PCI-Express-相容互連耦合至該第一積體電路，該第二積體電路包括：一耦合至該PCI-Express-相容互連以在該專屬加密虛擬頻道上接收該加密資料流之第二PCI-Express-相容介面電路，該第二PCI-Express-相容包括複數個頻道互連，各頻道互連與該複數個虛擬頻道中之一虛擬頻道關連；一耦合至該第二PCI-Express-相容介面電路之該複數個頻道互連中一第一頻道互連且配置成用以解密該加密資料流的硬體解密

電路；及一耦合至該硬體解密電路且配置成用以使用該解密資料流之第二邏輯方塊；以及

控制邏輯其耦合至該第一PCI-Express-相容介面電路與第二PCI-Express-相容介面電路至少其中之一，且配置成用以在該預設的虛擬頻道上傳達授權資料以在該專屬加密虛擬頻道上授權該第一積體電路與第二積體電路之間的安全通信。

2. 一種電路配置，其包含：一配置成用以在使用複數個虛擬頻道之一串列互連上傳達資料之複數頻道串列介面電路；及一耦合至該複數頻道串列介面電路且配置成用以加密在該複數個虛擬頻道中之一專屬加密虛擬頻道上傳達的所有資料之硬體加密電路。
3. 如申請專利範圍第2項之電路配置，其中該複數頻道串列介面電路包含耦合至該硬體加密電路且配置成用以在一PCI-Express-相容互連上傳達由該硬體加密電路輸出之加密資料的PCI-Express-相容介面邏輯。
4. 如申請專利範圍第2項之電路配置，進一步包含一耦合至該硬體加密電路且配置成用以在該串列互連上將用於通信的資料輸出至該硬體加密電路，致使由該邏輯方塊輸出的資料在該串列互連上的通信前受到加密的邏輯方塊。
5. 如申請專利範圍第4項之電路配置，其中該邏輯方塊係附加配置成用以在該複數個虛擬頻道中之一未加密的虛擬頻道上輸出用於通信的附加資料。
6. 如申請專利範圍第4項之電路配置，其中該邏輯方塊係配

置成用以輸出只在該專屬加密虛擬頻道上之該串列互連上的資料。

7. 如申請專利範圍第4項之電路配置，進一步包含一耦合至該複數頻道串列介面電路且配置成用以在該複數個虛擬頻道中之一未加密的虛擬頻道上輸出用於通信的資料之第二邏輯方塊。
8. 如申請專利範圍第4項之電路配置，進一步包含一耦合至該硬體加密電路且配置成用以在該專屬加密虛擬頻道上輸出用於通信的資料之第二邏輯方塊。
9. 如申請專利範圍第4項之電路配置，進一步包含一在該複數頻道串列介面電路與該邏輯方塊中間耦合之硬體解密電路，該硬體解密電路配置成用以解密藉由該複數頻道串列介面電路從該串列互連接收且在該專屬加密虛擬頻道上傳達的加密資料。
10. 如申請專利範圍第4項之電路配置，其中該複數個虛擬頻道包括一配置成用以傳達授權資料以在該專屬加密虛擬頻道上授權安全通信的預設虛擬頻道。
11. 一種包含如申請專利範圍第2項之複數頻道串列介面電路與硬體加密電路之積體電路。
12. 一種資料處理系統，其包含如申請專利範圍第11項之積體電路，及一包含一配置成用以由該第一複數頻道串列介面電路接收在該串列互連上傳達之該加密資料的第二複數頻道串列介面電路之第二積體電路，該第二積體電路進一步包含一配置成用以解密在該串列互連上接收之

加密資料的硬體解密電路。

13. 一種包含定義如申請專利範圍第2項之電路配置的硬體定義程式碼之程式產品，及一載送該硬體定義程式碼之信號載送媒體，其中該信號載送媒體包括一傳輸媒體與一可錄媒體至少其中之一。
14. 一種電路配置，其包含：一配置成用以在使用複數個虛擬頻道之串列互連上傳達資料之複數頻道串列介面電路；及一耦合至該複數頻道串列介面電路，且配置成用以藉由已在該複數個虛擬頻道中之一專屬加密虛擬頻道上之該串列互連上傳達之該複數頻道串列介面解密，而從該串列互連接收之所有資料的硬體解密電路。
15. 一種在一串列互連上傳達資料之方法，該方法包含：使用一配置在一積體電路上的硬體加密電路加密資料流；及使用一配置在該積體電路上之複數頻道串列介面電路傳達在一串列互連上的該加密資料流，其中傳達該加密資料流包括從該複數頻道串列介面電路支援之複數個虛擬頻道中之一專屬加密虛擬頻道上傳達該加密資料流，其中該專屬加密虛擬頻道專用於該加密資料的通信。
16. 如申請專利範圍第15項之方法，其中該複數頻道串列介面電路包含耦合至該硬體加密電路的PCI-Express-相容介面邏輯，其中在該串列互連上傳達該加密資料流包含在一PCI-Express-相容互連上傳達該加密資料。
17. 如申請專利範圍第15項之方法，進一步包含從一配置在該積體電路上的邏輯方塊產生資料流。

18. 如申請專利範圍第17項之方法，其中該邏輯方塊係配置成用以輸出只在該加密虛擬頻道上之該串列互連上的資料。
19. 如申請專利範圍第17項之方法，進一步包含從一配置在該積體電路上的第二邏輯方塊產生一第二資料流，及在使用由該複數頻道串列介面電路支援之該複數個虛擬頻道中之一未加密的虛擬頻道之該串列互連上傳達該第二資料流。
20. 如申請專利範圍第17項之方法，其進一步包含：解密一由該複數頻道串列介面電路，從該串列互連接收及在使用配置在該積體電路上之一硬體解密電路之專屬加密虛擬頻道上傳達之第二加密資料流；以及將該解密資料流傳達至該邏輯方塊。
21. 如申請專利範圍第17項之方法，其中該複數個虛擬頻道包括一預設虛擬頻道，該方法進一步包含在該預設虛擬頻道上傳達授權資料以在該專屬加密虛擬頻道上授權安全通信。
22. 如申請專利範圍第17項之方法，其進一步包含：從使用一配置在一第二積體電路上之第二複數頻道串列介面電路之該串列互連接收該加密資料流；及解密使用一配置在該第二積體電路上之硬體解密電路的該加密資料流。
23. 一種用於提供一數位資料流之存取控制之方法，該方法包含：解密一第一積體電路中的一第一加密資料流以產生一第一解密資料流；重新加密該第一積體電路中的該

第一解密資料流以產生一第二加密資料流；在藉由傳達該複數頻道串列互連支援之複數個虛擬頻道中一專屬加密虛擬頻道上的該第二加密資料流以連接的該第一積體電路與第二積體電路之一複數頻道串列互連上，從該第一積體電路將該第二加密資料流傳達至一第二積體電路；及解密該第二積體電路中的該第二加密資料流以產生一第二解密資料流。

24. 如申請專利範圍第23項之方法，進一步包含解調變一調變的輸入信號以產生該第一加密資料流。
25. 如申請專利範圍第24項之方法，進一步包含解碼該第二積體電路中的該第二解密資料流以產生一解碼資料流。
26. 如申請專利範圍第24項之方法，其中該調變的輸入信號包含一衛星廣播信號，其中該第一加密資料流包含一加密MPEG資料流，及其中解碼該第二積體電路中的該第二解密資料流包含執行在該第二解密資料流上的MPEG解碼。
27. 如申請專利範圍第23項之方法，其中解密該第一加密資料流包括執行在該第一加密資料流上的區域存取控制。
28. 如申請專利範圍第23項之方法，其中解密該第一加密資料流包括執行在該第一加密資料流上的用戶存取控制。
29. 如申請專利範圍第23項之方法，其中該第一積體電路與第二積體電路係配置在一機上盒之中。
30. 如申請專利範圍第23項之方法，其中該第一積體電路係配置在經由一連接器耦合至該第二積體電路之一存取卡

上。

31. 如申請專利範圍第23項之方法，其中重新加密該第一解密資料流係由配置在該第一積體電路上的硬體加密邏輯來執行。
32. 一種電路配置，其包含：配置成用以解密一第一加密資料流及從中產生一第一解密資料流的解密邏輯；配置成用以重新加密該第一解密資料流及從中產生一第二加密資料流的加密邏輯；以及一配置成用以藉由傳達該複數頻道串列互連支援之複數個虛擬頻道中一專屬加密虛擬頻道上的該第二加密資料流，而在一複數頻道串列互連上傳達該第二加密資料流的複數頻道串列介面電路。
33. 如申請專利範圍第32項之電路配置，進一步包含配置成用以解密該第二加密資料流及從中產生一第二解密資料流的第二解密邏輯。
34. 如申請專利範圍第33項之電路配置，進一步包含配置成用以從一調變的輸入信號產生該第一加密資料流的調變邏輯。
35. 如申請專利範圍第34項之電路配置，進一步包含配置成用以解碼該第二解密資料流的解碼器邏輯。
36. 如申請專利範圍第35項之電路配置，其中該調變的輸入信號包含一衛星廣播信號，其中該第一加密資料流包含一加密MPEG資料流，及其中解碼該第二積體電路中的該第二解密資料流包含執行在該第二解密資料流上的MPEG解碼。

37. 如申請專利範圍第35項之電路配置，其中該調變邏輯、該第一解密邏輯、該加密邏輯及該複數頻道串列介面電路係配置在一第一積體電路上，其中該第二解密邏輯與解碼器邏輯係配置在一第二積體電路上，及其中該第二積體電路包括一耦合至該複數頻道串列互連以從中接收該第二加密資料流之第二複數頻道串列介面電路。
38. 如申請專利範圍第32項之電路配置，其中該解密邏輯係配置成用以執行在該第一加密資料流上之區域存取控制。
39. 如申請專利範圍第32項之電路配置，其中該解密邏輯係配置成用以執行在該第一加密資料流上之用戶存取控制。
40. 如申請專利範圍第32項之電路配置，其中該複數頻道串列介面電路包含耦合至該加密邏輯，且配置成用以在一PCI-Express-相容互連上傳達該第一加密資料流的PCI-Express-相容介面邏輯。
41. 一種包含如申請專利範圍第32項之解密邏輯、加密邏輯及複數頻道串列介面電路的積體電路。
42. 一種資料處理系統，其包含如申請專利範圍第41項之積體電路，及一包含一配置成用以從該複數頻道串列互連接收該第二加密資料流之第二複數頻道串列介面電路與配置成用以解密該第二加密資料流並從中產生一第二解密資料流之第二解密邏輯的第二積體電路。
43. 如申請專利範圍第42項之資料處理系統，進一步包含一其上配置該第一積體電路之存取卡。
44. 一種包含如申請專利範圍第32項之解密邏輯、加密邏輯

及複數頻道串列介面電路之存取卡。

45. 一種包含定義如申請專利範圍第32項之電路配置的硬體定義程式碼之程式產品，及一載送該硬體定義程式碼之信號載送媒體，其中該信號載送媒體包括一傳輸媒體與一可錄媒體至少其中之一。

拾壹、圖式：

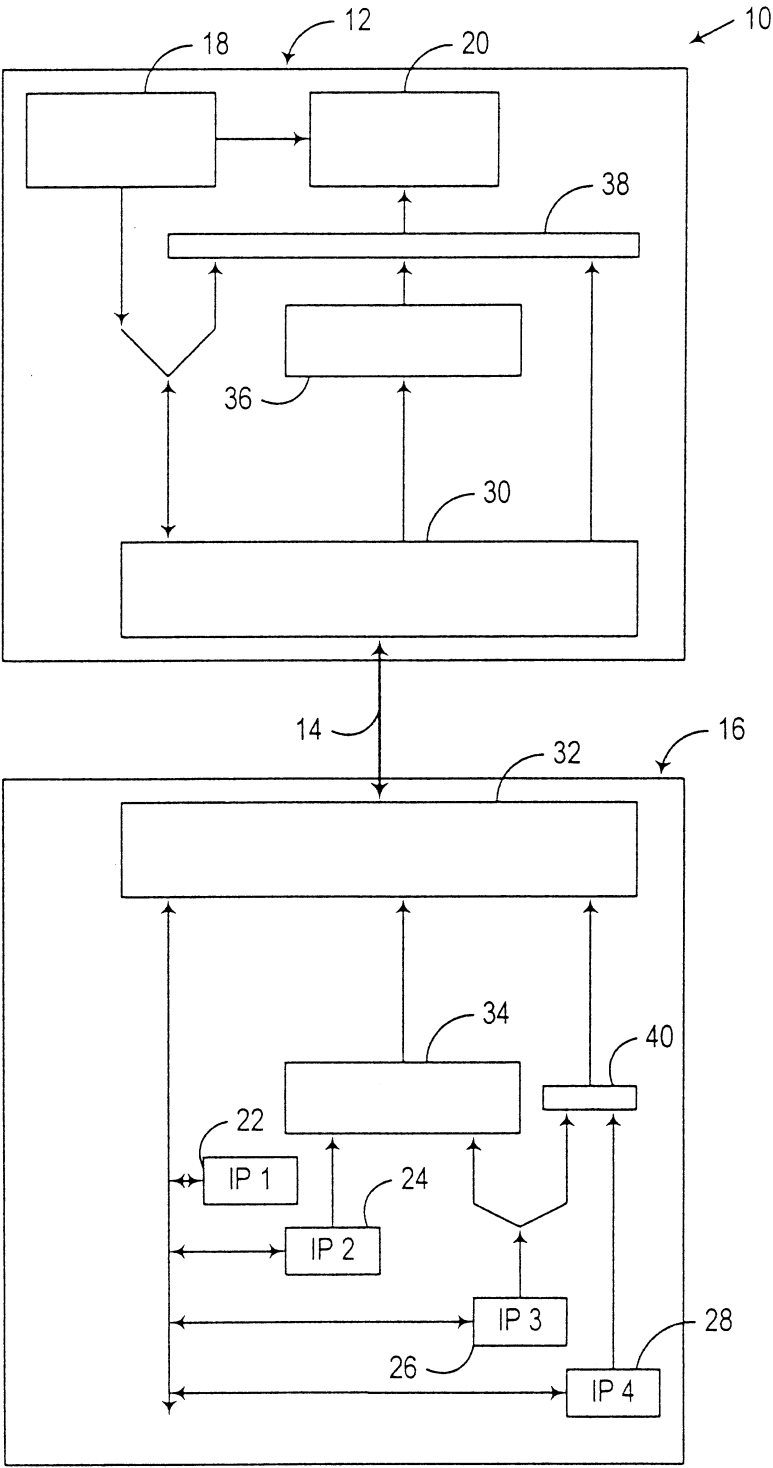


圖 1

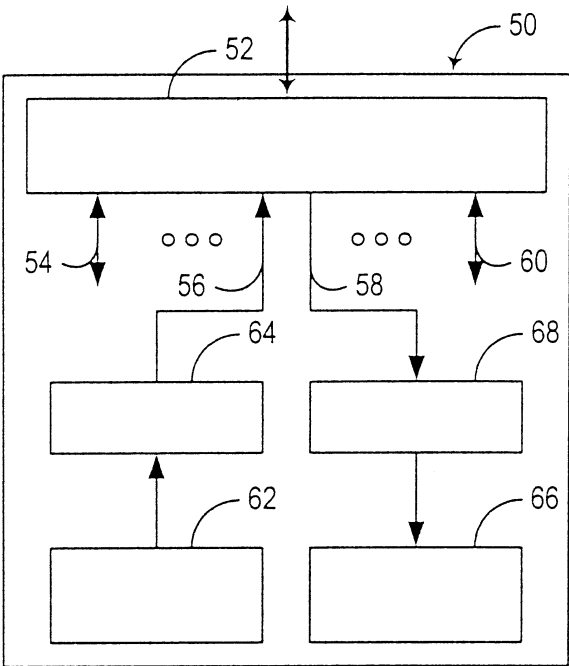


圖 2

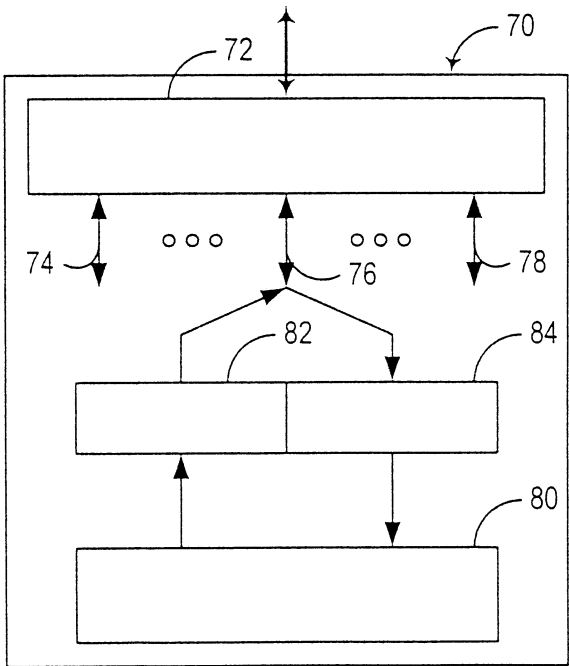


圖 3

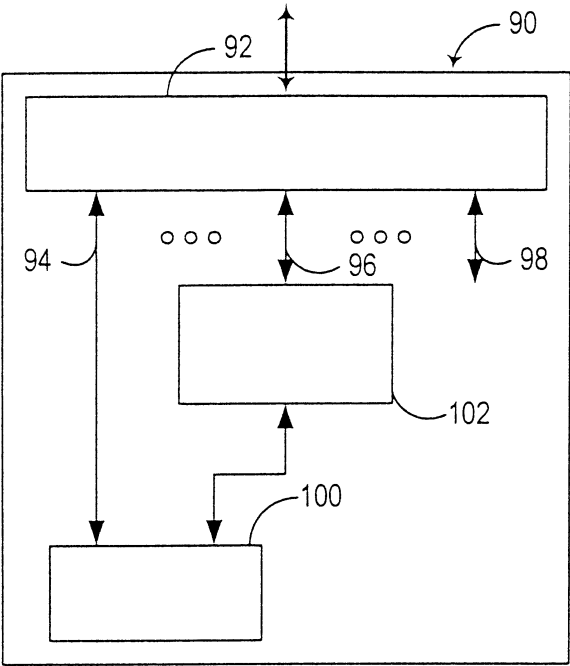


圖 4

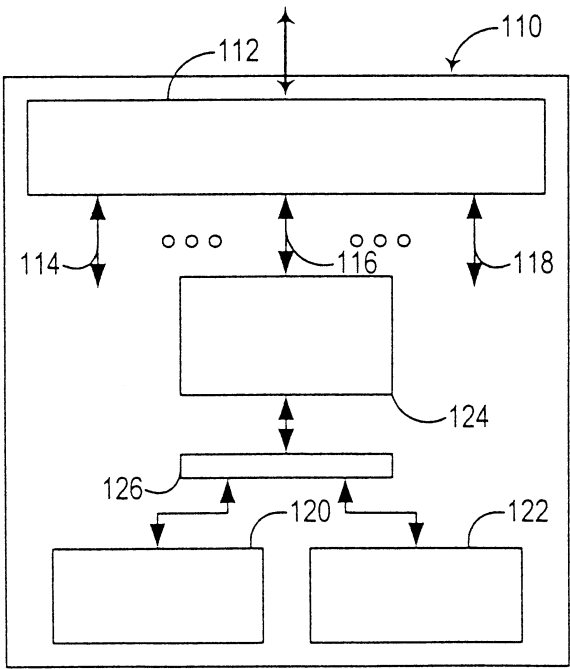


圖 5

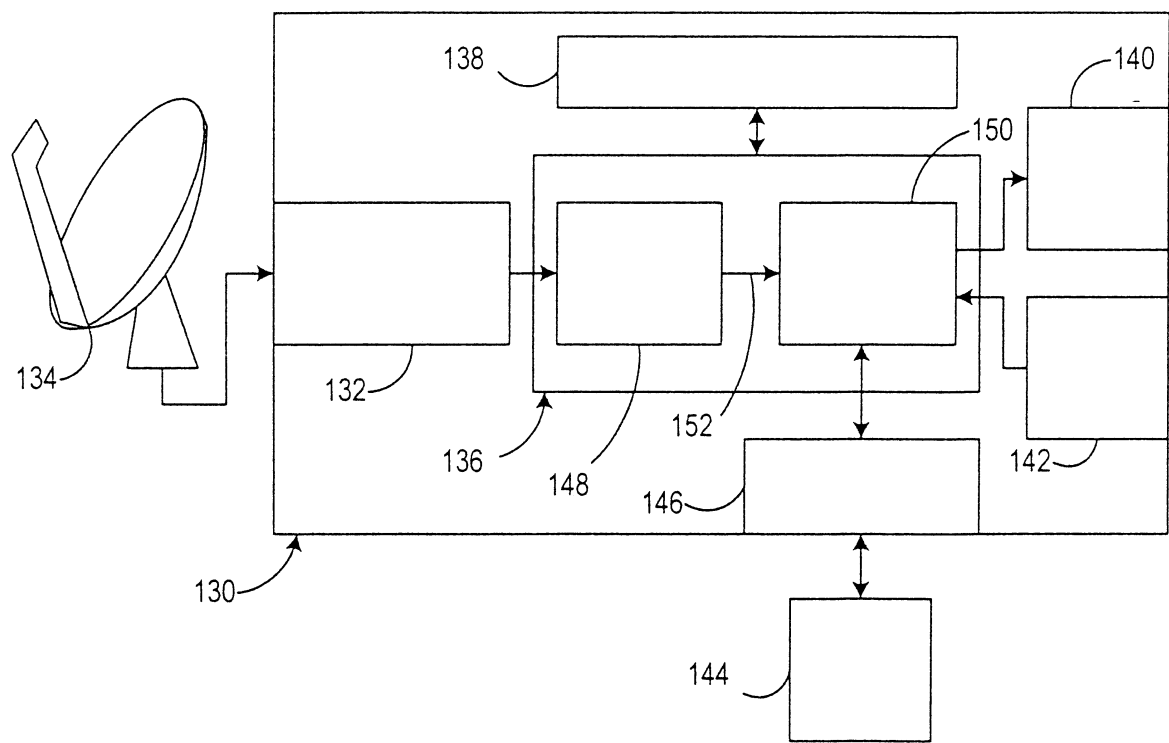


圖 6

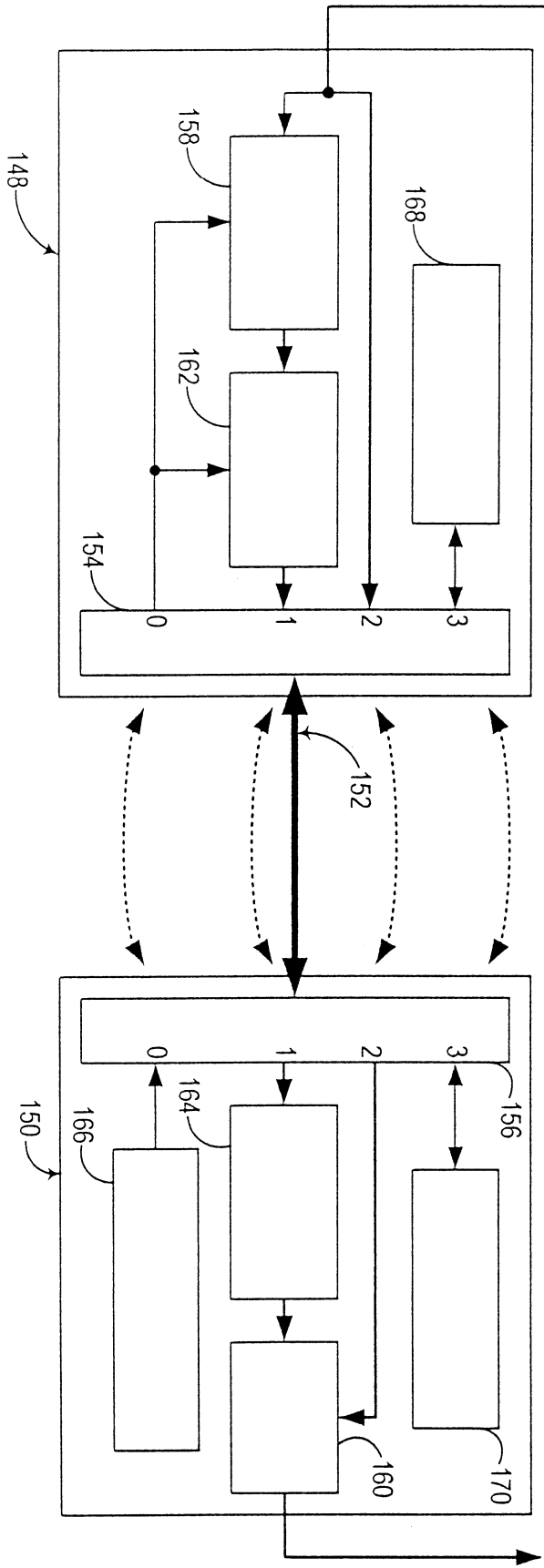


圖 7

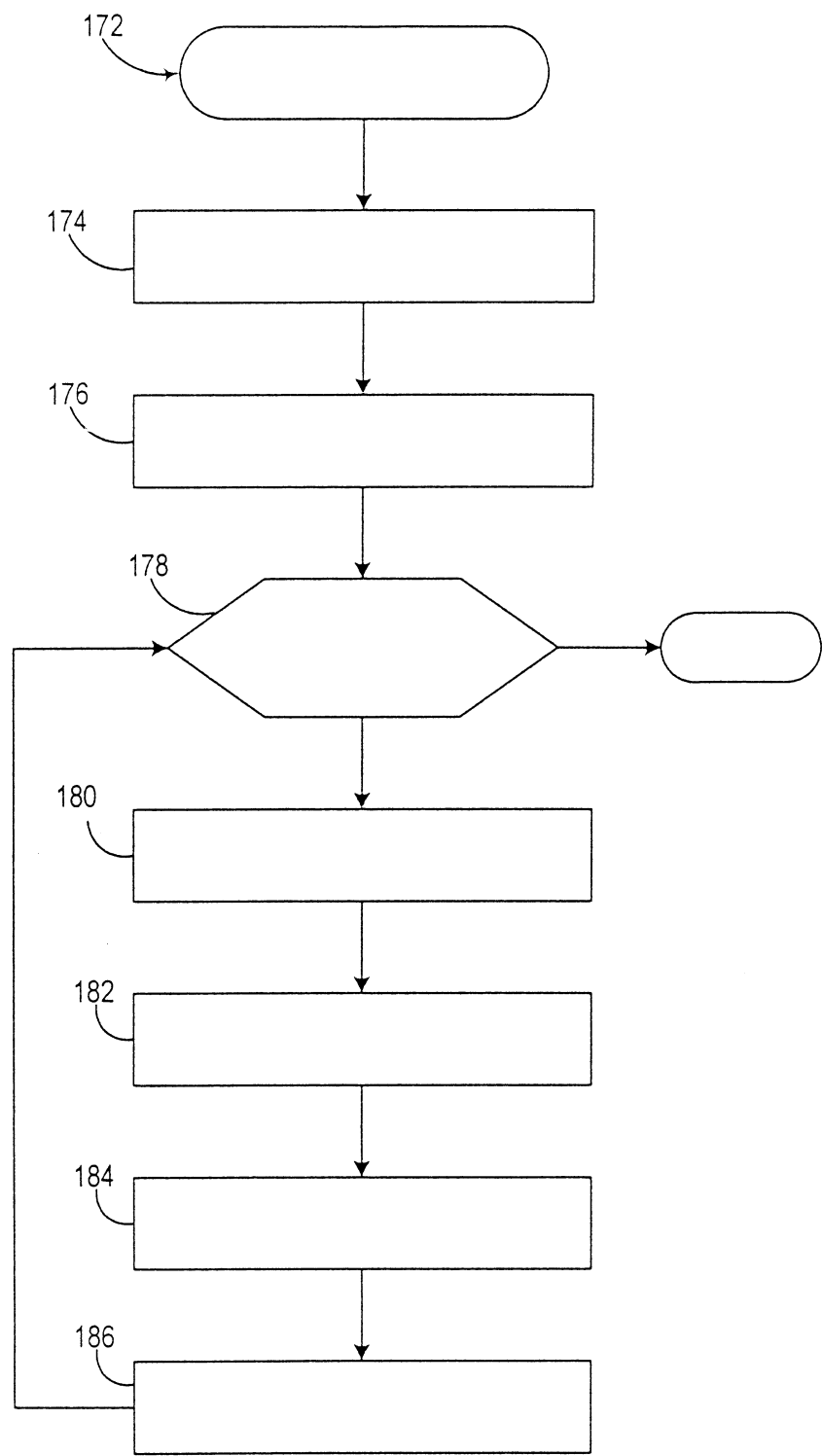


圖 8

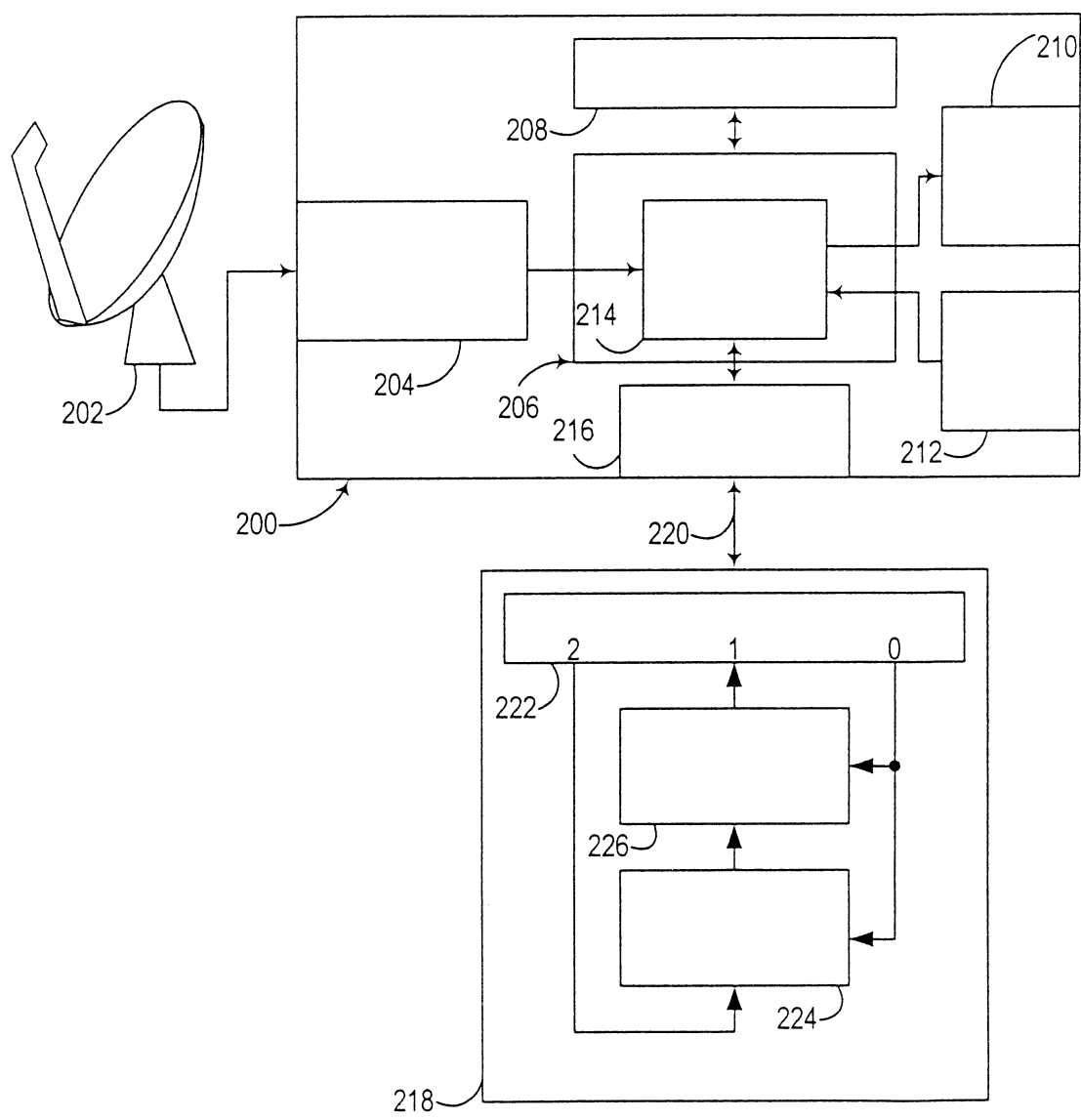


圖 9

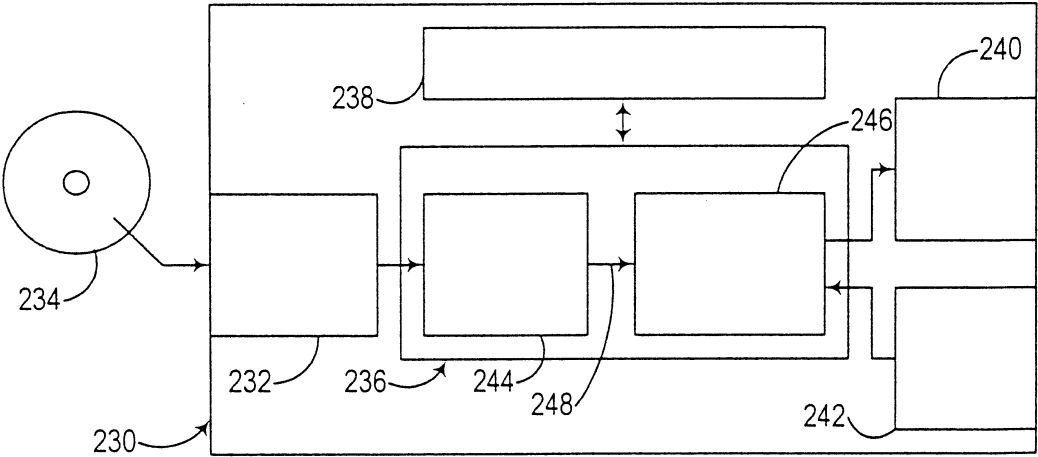


圖 10

柒、指定代表圖：

(一)本案指定代表圖為：第（ 1 ）圖。

(二)本代表圖之元件代表符號簡單說明：

10	資料處理系統
12	主機裝置
14	複數頻道串列互連
16	週邊裝置
18	處理器
20	記憶體
22, 24, 26, 28	邏輯方塊
30, 32	複數頻道串列端點電路
34	硬體加密邏輯
36	解密邏輯電路
38, 40	多工器

捌、本案若有化學式時，請揭示最能顯示發明特徵的化學式：