

發明專利說明書

(本說明書格式、順序及粗體字，請勿任意更動，※記號部分請勿填寫)

※ 申請案號：94116292

※ 申請日期：94-5-19

※IPC 分類：H04K1/00 (2006.01)

一、發明名稱：(中文/英文)

用以管理異質密碼運算之方法與裝置

METHOD AND APPARATUS TO MANAGE HETEROGENEOUS CRYPTOGRAPHIC OPERATIONS

二、申請人：(共 1 人)

姓名或名稱：(中文/英文)

英特爾公司/ INTEL CORPORATION

代表人：(中文/英文)

塞門 大衛/SIMON, DAVID

住居所或營業所地址：(中文/英文)

美國加州聖塔克萊拉市密遜大學道 2200 號

2200 Mission College Blvd. Santa Clara, CA, USA

國 籍：(中文/英文)

美國/U. S. A.

三、發明人：(共 1 人)

姓 名：(中文/英文)

納歐吉 雷傑/NEOGI, RAJA

國 籍：(中文/英文)

美國/U. S. A.

四、聲明事項：

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

☒ 申請前已向下列國家（地區）申請專利：

【格式請依：受理國家（地區）、申請日、申請案號 順序註記】

☒ 有主張專利法第二十七條第一項國際優先權：

1. 美國;2004, 06, 14; 10/868, 296

☐ 無主張專利法第二十七條第一項國際優先權：

☐ 主張專利法第二十九條第一項國內優先權：

【格式請依：申請日、申請案號 順序註記】

☐ 主張專利法第三十條生物材料：

☐ 須寄存生物材料者：

國內生物材料 【格式請依：寄存機構、日期、號碼 順序註記】

國外生物材料 【格式請依：寄存國家、機構、日期、號碼 順序註記】

☐ 不須寄存生物材料者：

所屬技術領域中具有通常知識者易於獲得時，不須寄存。

九、發明說明：

【發明所屬之技術領域】

本發明係為一種用以管理異質密碼運算之方法與裝置。

5 【先前技術】

發明背景

媒體電腦或機上盒(STB)可對諸如電視系統等娛樂系統提供多項功能。舉例言之，媒體電腦可接收及解碼影音信號供顯示於電視。但媒體電腦可連結至多個媒體源，各個媒體源有其本身的密碼要求。結果，媒體電腦可能需要根據多項密碼技術運算。如此，需要改良來將此等技術配合於裝置或網路。

【發明內容】

本發明係為一種方法，包含下列步驟：接收要對一內文流執行密碼運算之一請求；判定是否接受該請求；若該請求獲接受，則分派該內文流給多個密碼加速器之一；排程該內文流以供用來由該密碼加速器處理；以及根據該排程藉該密碼加速器執行該內文流之該等密碼運算。

圖式簡單說明

20 第1圖顯示系統100之方塊圖。

第2圖顯示系統200之方塊圖。

第3圖顯示系統300之方塊圖。

第4圖顯示一種資料結構400。

第5圖顯示一種資料結構500。

第6圖顯示方塊流程圖600。

第7圖顯示方塊流程圖700。

【實施方式】

較佳實施例之詳細說明

- 5 第1圖顯示系統100之方塊圖。系統100包含通訊系統來於多個節點間通訊資訊。節點可包含於系統100有一個獨特位址之實體或邏輯實體。該獨特位址例如包含諸如網際網路協定(IP)位址之網路位址、諸如媒體存取控制(MAC)位址之裝置位址等。
- 10 若干具體例中，一或多個通訊媒體可連結該等節點。通訊媒體包含任何可承載資訊信號之媒體。通訊媒體例如包括金屬引線、半導體材料、雙絞線、同軸纜線、光纖、射頻(RF)等。「連結」或「互連」及其變化等詞於本內文表示實體連結及/或邏輯連結。
- 15 系統100之節點可配置來通訊不同型別之資訊，諸如媒體資訊及控制資訊。媒體資訊表示對使用者表示內容意義之任何資料，諸如語音資訊、視訊資訊、音訊資訊、文字資訊、文數符號、圖形、影像等。控制資訊表示任何對自動化系統表示命令、指令或控制字眼之資料。舉例言之，
- 20 控制資訊可用來路由媒體資訊通過一系統，或指示一節點來以預定方式處理媒體資訊。

如第1圖所示，系統100包含媒體源1-P、媒體電腦102、及娛樂系統108。媒體電腦102包含密碼內文控制器(CCC)104。媒體電腦102可透過網路110而連結至伺服器112

。雖然第1圖顯示有限數目之節點，但須了解任何數目之節點皆可用於系統100。該等具體例非僅限於本內文。

若干具體例中，系統100包含媒體源1-P。媒體源1-P包含任何可傳輸音訊信號、視訊信號或影音(A/V)信號給一娛樂系統諸如娛樂系統108之任何來源。媒體來源之實例可包括A/V信號如電視信號之來源。媒體來源可配置成供給或傳輸標準類比電視信號、數位電視信號、高傳真電視(HDTV)信號等。電視信號可包括各型資訊，諸如電視音訊資訊、電視視訊資訊及電視控制資訊。電視視訊資訊包括得自視訊節目之內容、電腦產生之影像(CGI)等。電視音訊資訊包括語音、音樂、音效等。電視控制資訊可被嵌置控制信號來顯示電視視訊及/或音訊資訊、商業短片、更新速率、同步信號等。媒體源之另一實例包括音訊信號源。音訊源可配置來供給或傳輸標準音訊資訊，諸如類比音樂或數位音樂。媒體源之另一實例包括視訊信號源，例如由電腦至顯示器之視訊信號源。媒體源1-P之其它實例包括數位相機、影音錄像機、視訊監視系統、視訊會議系統、電話系統、醫療儀器與測量儀器、及其它需要影像及音訊處理運算之來源。具體例非僅限於本內文。

若干具體例中，媒體源1-P可源自多個不同裝置或網路。例如媒體源1-P可包括配置來傳輸以各種格式儲存的預錄媒體之裝置，諸如數位影音光碟(DVD)裝置、視訊家用系統(VHS)裝置、數位VHS裝置、電腦、遊戲機、光碟(CD)播放器等。又另一實例中，媒體源1-P包括多媒體配送系統

來提供廣播式或流線式類比或數位電視信號或音訊信號給媒體電腦102。多媒體配送系統之實例例如包括透過空氣(OTA)廣播系統、地面纜線系統(CATV)、衛星廣播系統等。媒體源1-P之型別及所在位置非僅限於本內文。

- 5 若干具體例中，系統100包含娛樂系統108。娛樂系統108包含任何配置來複製接收自媒體源1-P之一或多個電視信號、音訊信號或視訊信號之任何系統。娛樂系統108之實例包括任何有顯示器及揚聲器之電視系統。娛樂系統108之另一實例包括音訊系統諸如接收器或連結至外部揚聲器之接收器或調諧器。娛樂系統108之又另一實例可包括有顯示器及揚聲器之電腦。該具體例非僅限於本內文。
- 10

- 若干具體例中，系統100可包含媒體電腦102。媒體電腦102可包含一處理系統，如對特定實作所需，該處理系統配置來使用由處理器、硬體電路或結構執行的軟體、或硬體與軟體之組合來實作各項運算。若干具體例中，舉例言之，媒體電腦102可包含個人電腦(PC)或STB配置來對系統100之各個節點管理媒體資訊及控制資訊。媒體電腦102可連結至媒體源1-P及娛樂系統108。媒體電腦可有多個標準輸出入(I/O)裝置，諸如鍵盤、滑鼠、顯示器、印表機等。
- 15
- 20 如對指定實作所需，連結可包括各種有線或無線通訊媒體及適當I/O配接器。具體例非受本內文所限。

若干具體例中，媒體電腦102可透過網路110而連結至伺服器112。網路110之實例包括資料網路，例如根據一或多項網際網路協定，諸如傳輸控制網路(TCP)及網際網路協

定(IP)操作之網路。伺服器112包含電腦或工作站來傳輸內容至媒體電腦102，諸如配置來透過超文字傳輸協定(HTTP)(舉例)來傳輸超文字標記語言(HTML)文件或擴充性標記語言(XML)文件之網路伺服器。該等具體例非囿限於本內文。

值得注意者，雖然媒體電腦102及娛樂系統108顯示於第1圖為分開系統以求清晰，但須了解此二系統可於單一整合系統實作。此種整合系統之實例包含具有處理器及記憶體之數位電視。該等具體例非囿限本內文。

若干具體例中，媒體電腦102可包括CCC 104。CCC 104可配置來對媒體電腦102管理及執行各項密碼運算。多種情況下，媒體電腦102可以加密格式而由媒體源1-P接收各項資訊。加密可根據多種不同密碼技術執行。密碼技術之實例包括資料加密標準(DES)、三重DES、MULTI-2、先進加密系統(AES)、快速資料加密演繹法則(FEAL)、MISTY、ENCRIp等。同理，來自伺服器112之內文可以加密格式諸如IPSec、安全HTTP(SHTTP)、安全套筒層(SSL)等而透過網路110傳輸至媒體電腦102。

若干具體例中，密碼技術可包括多種區塊密文演繹法則。一個區塊密文可為非對稱性或為對稱性。系統區塊密文可使用相同的鑰來加密及解密。對稱性區塊密文可使用不同的鑰來加密及解密。區塊密文可將一區塊之明文加密成為相同尺寸之一區塊密文。區塊可定義為包括任何指定之位元數位。結果，全部區塊密文皆具有自然區塊大小，

包含於單次運算時加密的位元數目。此點係與流密文相反，流密文每次只加密一個位元。任何區塊密文皆可以若干模式之一操作，諸如電子碼書(ECB)模型、密文區塊連鎖(CBC)模型、輸出回授(OFB)模型等。該等具體例非囿限本

5 內文。

多種密碼技術的存在可能要求有一個裝置來執行不同的密碼運算集合。舉例言之，各密碼技術可使用不同型別之鑰、鑰大小、鑰儲存裝置、鑰更新頻率等。此外，各項密碼技術之密碼內文不同，換言之可用於多種不同型別之

10 應用用途與環境。不同密碼內文之實例包括解密流線影音信號、儲存加密/解密、重新加密供於家用網路配送，或於開放匯流排結構通訊內容等。結果，異質密碼技術與異質密碼內文的組合造成密碼運算管理操作的複雜度。

CCC 104可配置來對媒體電腦102之多個客端管理與執行不同的密碼運算，包括媒體源1-P及伺服器112。CCC 104可支援來自多個客端如媒體源1-P之多數密碼內文。CCC 104可基於動態來源配置策略而對來自一客端之各個主動流切換內文、控制及組態。CCC 104可存取至直接記憶體存取(DMA)控制器、可重新組構之密碼引擎、及各個暫存器

20 排組。控制結構可接受無耗損的壓縮來減少動態載入延遲。概略言之媒體電腦102且特別為CCC 104可參照第2圖進一步討論其細節。

第2圖顯示系統200。若干具體例中，系統200為媒體電腦102之系統或次系統之代表例。如第2圖所示，系統200包

含連結至客端1-M之CCC 220、處理器216及記憶體218。

CCC 220包含密碼內文管理器(CCM) 202及密碼處理複合器(CPC) 210。CCM 202包含客端介面模組204、排程模組206及CPC介面模組208。CPC 210包含直接記憶體存取(DMA)

5 212、記憶體214及密碼加速器(CA) 1-N。雖然顯示有限數目的元件作為系統200之一部分，但須了解系統200可包含任何數目之額外元件。具體例非囿限本內文。

若干具體例中，系統200可包含處理器216。處理器216可為任何型別之可提供一具體例之預定速度及功能之處理
10 器。例如處理器216可為英代爾公司(Intel Corporation)等製造之處理器。處理器216也包含數位信號處理器(DSP)及伴隨之架構。處理器216進一步包含專用處理器諸如網路處理器、嵌入式處理器、微控制器、控制器等。該等具體例非囿限本內文。

15 若干具體例中，系統200可有各種型別之記憶體，諸如可存取處理器216之記憶體218及可存取DMA 212之記憶體214。記憶體214及記憶體218可包含任何可儲存程式指令及資料適合藉一處理器執行之機器可讀取媒體。機器可讀取媒體之若干實例包括但非限制性唯讀記憶體(ROM)、隨機
20 存取記憶體(RAM)、動態RAM(DRAM)、雙重DRAM(DDRAM)、靜態RAM(SRAM)、可規劃ROM、可抹除可規劃ROM、可電子抹除可規劃ROM、動態RAM、磁碟(例如軟碟及硬碟機)、光碟(例如CD-ROM)及任何其它可儲存數位資訊之媒體。此外，媒體電腦200可含有可機器讀取

別及持續時間可根據實作而改變，該等實施例非圍限本內文。

若干具體例中，CCC 220可包括CCM 202。CCM 202可連結至CPC 210。CCM 202可為配置來藉密碼處理系統如CPC 210管理多數內文流之執行的系統。多數內文流可源自於單一客端，或可源自於多數客端。若干具體例中，多數內文流可使用不同的密碼技術。例如多數內文流包括欲根據第一密碼運算集合處理之第一內文流，以及欲根據第二密碼運算集合處理之第二內文流。內文流之數目可根據對指定實作之資源數量而改變，該等具體例非圍限本內文。

若干具體例中，CCM 202可包括多個元件，諸如客端介面模組204、排程模組206及CPC介面模組208。模組例如可包含一或多電路、元件、暫存器、處理器、軟體次常式或其任一種組合。雖然CCM 202只包括有限數目之模組，但須了解任何數目之模組皆可用於CCM 202。該等具體例非圍限本內文。

若干具體例中，CCM 202包括客端介面模組204。一或多個客端1-M發送請求密碼服務的請求給CCC 220。客端1-M經由進送一內文參數或客端識別符給客端介面模組204來引發與CCC 220之連結或通訊作業。客端介面模組204可接收請求，可執行認證操作，來證實請求存取CCC 220之密碼服務之客端身分。認證操作例如可對各階段作業執行。

一旦客端經過授權，客端介面模組204可判定CPC 210是否對該客端及/或對該內文流執行密碼運算。客端介面模

組204可取還與客端相關聯之客端資源參數集合。客端介面模組204可取還與CPC 210之密碼加速器1-N相關聯之系統資源參數集合。客端介面模組204可判定是否使用客端資源參數及系統資源參數，來判定是否對客端執行密碼運算。

- 5 若干具體例中，客端資源參數包含可輔助界定服務該項請求所需之資源量的參數。客端資源參數實例包括客端頻寬參數及內文參數。客端頻寬參數表示客端所請求之頻寬量。所請求之頻寬包括位元率，典型係以每秒之位元或位元組表示。內文參數可表示由客端請求之運算型別，如
- 10 加密運算或解密運算。內文參數也表示運算環境如家用網路、辦公室網路、公用網路等。內文參數也表示請求服務之裝置型別，諸如電腦、DVD播放器、遊戲機、CD播放器等。客端資源參數可嵌有客端請求。客端介面模組204也由與各客端相關聯之儲存於記憶體214或218之服務層級吻合
- 15 (SLA)取還客端資源參數。

- 若干具體例中，系統資源參數可包含可輔助界定用來服務該項請求之資源量的參數。系統資源參數實例包括系統頻寬參數、密碼頻寬參數、記憶體頻寬參數、有用之DMA頻道參數、流邏輯參數等。系統資源參數可由CPC 210透過
- 20 CPC介面模組208而取還。

 若干具體例中，客端介面模組204可比較與客端請求相關聯之處理需求與可利用的系統資源。若只能滿足部分客端密碼之需求，則該項服務請求將被拒絕。若客端介面模組204判定CPC 210有足夠可利用的系統資源來服務該項請

求，則客端介面模組204可承認該項請求，且核准該內文流由CPC 210處理。內文流識別符或客端識別符可進送至排程模組206。客端介面模組204可進送與所核准之內文流相關聯之額外資訊，諸如密碼技術用鑰、位元率等。舉例言之，客端介面模組204可對密碼技術進行鑰計算。客端介面模組204可對各邏輯扇區或執行內文來執行鑰計算。各個核准之內文流之位元率例如可用來藉排程模組206來追蹤實時期限。

若干具體例中，CCM 202可包括排程模組206。排程模組206可配置來分派多數內文流之一給一或多個密碼加速器1-N。排程模組206可對各個密碼加速器1-N產生一處理多數內文流之日程表。排程模組206也可操作來確保執行內文邏輯扇區經校準來輔助客端介面模組204執行鑰之計算。

若干具體例中，排程模組206可接收來自客端介面模組204之經過核准的內文流，且將該內文流分派給密碼加速器1-N之一。一旦被分派後，排程模組206可將該內文流加至準備由密碼加速器執行的內文流串列(「就緒串列」)。排程模組206可排程各內文流準備由密碼加速器處理。密碼加速器可對各內文流連續處理資訊區塊，直到內文流達到結束條件為止。結束條件例如包含預定數目之執行週期、內文流逾時、由請求客端所發出之停止指示等。值得注意者為就緒串列初始化密碼加速器的全部活動。一旦內文流開始接收密碼服務，DMA 212可使用DMA岔斷來確保連續操作直到內文流結束為止。

若干具體例中，排程模組206負責排程各內文流來由CPC 210處理。排程模組206可根據動態資源配置策略，基於逐一區塊之基準，對各個主動內文流切換內文、控制、及組態。動態資源配置策略包括一針對來有效使用資源用於CPC 210之規則集合，藉此允許CPC 210來於執行期限內對各個內文流處理多數內文流，同時也縮短DMA 212及密碼加速器1-N之延遲時間及閒置時間。排程模組206可參照第3-6圖討論其進一步細節。

若干具體例中，CCM 202可包括CPC介面模組208。CPC介面模組208配置來介於CCM 202與CPC 210間通訊各型別資訊，諸如媒體資訊、控制資訊、組態資訊等。舉例言之，CPC介面模組208可介於排程模組206與CPC 210間通訊排程資訊。CPC介面模組208也可對CPC 210監視各項系統資源參數，且進送此等參數至客端介面模組204來用於核准新的內文流。

若干具體例中，CCC 220可包括CPC 210。CPC 210可為配置來對多數內文流實際執行密碼運算的系統。CPC 210可包括DMA 212、記憶體214及多數密碼加速器1-N。雖然對CPC 210顯示有限數目之元件，但可了解CPC 210可包含額外元件。該等具體例並非圍限本內文。

若干具體例中，CPC 210包括記憶體214。記憶體214包含CCC 220之專用記憶體，或來自中心系統記憶體218之分隔記憶體節段。記憶體214可儲存各型資訊，來由CPC 210用於處理得自主動內文流之資料區塊，諸如媒體資訊、控

制資訊、密碼加速器之可執行碼、內文資訊、組態資訊等。

若干具體例中，CPC 210包括密碼加速器1-N。密碼加速器1-N可對不同內文流執行不同密碼運算集合。舉例言之

- ，多數密碼加速器可包括第一密碼加速器及第二密碼加速
5 器，第一密碼加速器可執行第一集合之密碼運算以及第二
密碼加速器可執行第二集合之密碼運算。

- 密碼加速器可以多種不同方式實作。例如，密碼加速
器可於硬體(例如接線閘)、軟體(例如微編碼核心)、或硬體
與軟體之某種組合而實作。一具體例之適當軟體結構之實
10 例包括用於處理器或網路處理器之微碼、韌體、或其它對
指定硬體架構為最佳化的低階碼。若密碼加速器係於軟體
實作，則密碼加速器須載入特殊微碼，載入須於執行之初
始化之前完成。CCM 202之排程模組206可鑑於需要介於各
內文間切換所需的載入時間來實作。

- 15 若干具體例中，CPC 210包括DMA 212。DMA 212包含
DMA控制器及隨附之硬體結構諸如一或多暫存器或緩衝器
。DMA 212可根據由排程模組206透過CPC介面模組208所
提供之排程資訊，來安排資訊區塊介於記憶體214與密碼加
速器1-N間的傳輸。密碼加速器1-N可配置來使用該等區塊
20 執行密碼運算。DMA 212之進一步細節將參照第3圖討論。

於一般操作，CCC 220可對媒體電腦102執行對多數內
文流之不同密碼運算集合。CPC 210包括一排組之獨立運算
密碼加速器1-N及一多頻道DMA控制器212來推挽來自共
享記憶體214之所需緩衝器及緩衝器描述器。CCM 202係於

處理器216執行，控制工作負載流之流入密碼加速器1-N。

處理器216之實例可為英代爾公司製造之X規模(Xscale)(XSC)處理器。CCM 202執行各型密碼控制運算，其中一項運算包括執行內文知曉排程，來決定何者內文流需要由密碼加速器執行。如此，CCM 202架設一或多緩衝器描述器於記憶體214，規劃DMA控制器212來進行操作，以及重新組配密碼加速器1-N用於下一個執行期。CCM 202也介面至各個客端1-M來建立通訊階段性通訊作業。

更特別，客端1-M可由CCC 220經由供給內文參數給客端介面模組204來請求服務。客端介面模組204認證客端，基於資源之利用性來接納或拒絕該請求。一旦內文流被接納，排程模組206發出指令給DMA 212來開始由記憶體214挽出區塊，對密碼加速器1-N載入適當輸入資料區塊、可執行碼內文資訊、控制資訊及組態資訊。排程模組206隨後發出開始指令給密碼加速器1-N來處理該輸入資料區塊。加密後或解密後之輸出資料區塊可透過DMA 212而被推至記憶體214。此種基於區塊之處理持續至達到結束條件為止，諸如客端發出中止指示等。

若干具體例中，內文流間之切換係由動態資源配置策略所驅動，其係配置來將主動內文流作優先順位排序，而極少鬆弛。動態資源配置策略試圖根據 $\text{Min}_i\{D_n^i - (T_n + C_k^i)\}$ 來減少主動內文流的鬆弛，此處鬆弛參數係基於CPC 210之目前組態，以一內文流之實時期限與預測完成時間間之差異計算。排程模組206將期限與各回合之密碼運算相關聯

，該排程模組係基於應用於內文流之單調計算之完成百分比。預測完成時間係基於組態側繪，將時間差加至目前時間算出。

如前文說明，CCC 220係服務以區塊為基準之多數內文
 5 流。密碼加速器係組配來使用得自儲存於記憶體214之排程
 模組208之資訊處理一輸入資料區塊，該輸入資料區塊透過
 DMA 212而被傳輸至適當密碼加速器。密碼加速器於各個
 執行週期，可使用不同密碼運算來處理不同區塊。結果，
 連同輸入資料區塊，密碼加速器須被載入內文資訊、可執
 10 行碼、內文資訊、控制資訊及組態資訊。內文資訊包括來
 自前一執行期而需要於階段通訊作業目前執行期進行的檢
 查點資料。例如於CBC模型，得自前一密文區塊的結果可
 能為目前執行所需。同樣地，可能需要初始化向量(IV)來開
 始執行第一密文區塊。組態資訊可包括對一指定之執行週
 15 期所需之組態參數。密碼加速器1-N對一指定之階段性密碼
 作業，可根據效能限制及設計限制來重新組配。於可執行
 目前執行期之前，密碼加速器可以各項組態參數組配，該
 等組態參數諸如表示密碼操作之型別(例如加密/解密)、鑰
 大小(例如56/64/128/192/256)、密碼模型(例如
 20 ECB/CBC/C-CBC/CTR)及密碼演繹法則型別(例如
 AES/C2/DES/3DES/CSS/DVB-CSA)之內文參數。控制空間
 包括對一特定密碼運算集合的演繹法則定義。舉例言之，
 AES之控制空間可表示為 $c_i = E_k(c_{i-1} + m_i)$, $m_i = c_{i-1} + D_k(c_i)$ 。

如第2圖所示，系統200具有系統架構，該系統架構包

括m客端共享由n密碼加速器所提供的服務。有 $2*n$ DMA頻道來服務同時執行n密碼加速器，各個密碼加速器具有一個DMA頻道來由記憶體214挽出輸入資料-結構，以及推出輸出資料結構至記憶體214。若干具體例中，可有單一密碼加速器來服務多數客端1-M。另一具體例中，對各個客端及/或各個型別之服務可有分開之密碼加速器。通常，系統200可實作來於客端與密碼加速器之各項組合滿足 $m \geq n$ 的設計限制。

第3圖顯示一系統300。若干具體例中，系統300例如表示DMA 212以及用於CPC 210之伴隨的結構。如第3圖所示，系統300包含連結至DMA控制器304之記憶體302。DMA控制器304可連結至多個硬體緩衝器，諸如各個先進先出(FIFO)緩衝器。例如DMA控制器304可連結至輸入FIFO(i-FIFO)306、控制FIFO(c-FIFO)308及輸出FIFO(o-FIFO)310。雖然顯示有限數目之元件作為系統300之一部分，但須了解系統300可包含任何數目之額外元件。該等具體例並非圍限本內文。

若干具體例中，系統300包含DMA控制器304。DMA控制器304可支援n項同時運算的內文。內文流之輸入資料區塊可由記憶體214取還，且儲存於i-FIFO 306。與一指定內文流相關之一密碼加速器之可執行碼或可執行區塊可由記憶體214取還且儲存於c-FIFO 308。可執行碼可於該密碼加速器開始執行期之前由c-FIFO 308載入。其次，密文區塊單元可由i-FIFO 306取還，來維持對應之密碼加速器的連續操

可經規劃來使用記憶體214之一鏈結串列資料結構，來存取共同鏈結之分段資料區塊1-L。依據一指定實作而定，輸入資料與輸出資料可為相同鏈結串列或分開鏈結串列之一部分。當資料區塊1-L移動至DMA控制器304之i-FIFO 306時，來自鏈結串列之對應節點或對應鏈路被清除，而剩餘之鏈路經過調整。同樣地，於排程模組206之更新期，輸出資料區塊可由該鏈結串列提取。由DMA控制器304之o-FIFO 310之輸出資料區塊之取還，可與由對應輸入頻道產生的岔斷事件同步。DMA控制器304有設施可於輸入頻道及輸出頻道二者監視各個內文流之位元速率。此項資訊可能凌駕內設之位元速率規格，排程模組206可於評估期期間使用該項資訊來作流量控制決策。排程模組206之各個運算期進一步細節討論如後。

若干具體例中，排程模組206經由連續循環通過三個運算期，包括一更新期、一評估期、以及一排程期，來維持CPC 210之資料流。響應於DMA岔斷事件或非零就緒串列，排程模組206首先找到DMA頻道及密碼加速器的狀態。於更新期期間，排程模組206對各個密碼加速器的就緒串列上的各個內文流更新期限與目前時間偏差值。於評估期期間，排程模組206評估主動內文流來判定需要服務的次一內文流。此可藉運算就緒內文流量的鬆弛度來完成。於排程期，排程模組206於記憶體214設定緩衝器描述器之資料結構，以及規劃DMA控制器304及對應之密碼加速器。

第5圖顯示資料結構500，若干具體例中，資料結構500

例如表示由系統300所使用之資料結構。如第5圖所示，資料結構500包含一鏈結串列，其包含於藉排程模組206初始化期間、以及排程模組206操作期間之一目前節點及一次一節點。雖然顯示一特定資料結構集合來作為資料結構500之一部分，但了解資料結構500可包含任何數目之不同資料結構或額外資料結構設計來支援系統300之運算需求。該等具體例並非囿限於本內文。

如第5圖所示，排程模組206之初始化包括設定目前資料結構及下一個資料結構為零。當客端接合CCC 220或離開CCC 220，各個密碼加速器之就緒串列係據此而更新。期限之計算係由內文流之位元速率所驅使，而預測完成時間係將估計區塊延遲加至目前時間來算出。此種啟發性演繹法則類似退化時間輪，且係基於通知內文流單純滿足其期限要求，需要現在執行，其它事件可等候。於目前佇列之各事件處理後，下一個資料結構變成目前資料結構，同時形成新的下一個資料結構。排程演繹法則可為異步，排程模組206可響應於異步事件來執行排程。當無事件時，排程模組206可維持於等待模型，或進行維持運算，諸如更新統計數據，藉此來減輕處理器216的處理負擔。

前述系統之運算可進一步參照下列附圖及附隨之實施例進一步說明。部分附圖包括規劃邏輯。雖然此等圖式可包括特殊規劃邏輯，但須了解規劃邏輯單純提供此處所述概略功能如何實作之實例。進一步，除非另行指示，否則指定之規劃邏輯無需以所呈現之順序執行。此外，雖然指

定之規劃邏輯可於此處描述為以前述模型實作，但須了解規劃邏輯可於系統內部任何位置實作，而仍然落入具體例之範圍內。

第6圖顯示方塊流程圖600。第6圖顯示方塊流程圖600，其表示由一或多個此處所述系統諸如系統100-300執行的運算。如方塊流程圖600所示，請求對一內文流執行密碼運算可於方塊602接收。判定是否接受該請求可於方塊604判定。若於方塊606接受該請求，則內文流可分配給多數密碼加速器之一。於方塊608，該內文流可被排程用來藉密碼加速器處理。內文流之密碼運算可於方塊610，根據排程，藉密碼加速器執行。

若干具體例中，方塊604之判定係經由對於內文流相關之客端接收客端識別符來執行。客端可使用客端識別符來認證。與客端相關聯之客端資源參數集合、及與密碼加速器相關聯之系統資源參數集合可經取還。可使用該客端資源參數及系統資源參數，來判定是否執行客端之密碼運算。

若干具體例中，於方塊610之執行可經由使用包含輸入資料之資訊區塊、控制資訊、內文資訊及組態資訊之資訊區塊，來產生內文流之一資訊區塊而達成。密碼加速器可根據控制資訊、內文資訊及組態資訊而組配。輸入資料可使用經組配之密碼加速器來處理。

第7圖顯示一方塊流程圖700。第7圖舉例說明一方塊流程圖700，其表示藉一或多個此處所述之系統如系統100-300執行之方塊608之排程運算。如方塊流程圖700所示

，方塊608之排程可經由於方塊702，將內文流加至密碼加速
器之內文流串列來執行。各個內文流及密碼加速器之狀
態資訊可於方塊704更新。方塊704例如係對應於排程演繹
法則之更新期。內文流可於方塊706經選定來由密碼加速器
5 服務。方塊706例如係對應於排程演繹法則之評估期。處理
內文流之時間可於方塊708排程。方塊708例如係對應於排
程演繹法則之排程期。

此處陳述多項特定細節以供徹底了解具體例。但熟諳
技藝人士了解可無此等特定細節來實作具體例。其它情況
10 下，眾所周知之運算、元件及電路並未描述其細節俾不混
淆該等具體例。了解此處揭示之特定結構細節及功能細節
可為代表性，而非必然限制具體例之範圍。

值得注意者，述及「若干具體例」或「一具體例」表
示就該具體例所述之特定特色、結構或特徵係含括於至少
15 若干具體例。於說明書中之各處出現「於若干具體例中」
一詞並非全部皆必然表示同一個具體例。

全部或部分具體例可使用一種架構實作，該架構可根
據以下多項因素之任一項而改變，該等因素諸如預定運算
速率、功率位準、熱忍受性、處理週期預算、輸入資料速
20 率、輸出資料速率、記憶體資源、資料匯流排速度及其它
效能限制。舉例言之，一具體例可藉處理器所執行之軟體
來實作。另一例中，具體例可以專用硬體實作，諸如電路、
特殊應用積體電路(ASIC)、可規劃邏輯裝置(PLD)、DSP
等。又另一例中，具體例可藉規劃後之通用電腦元件與客

I280000

404...DMA設定資料結構

500...資料結構

600...方塊流程圖

602-610...方塊

700...方塊流程圖

702-708...方塊

1-L...資料區塊

1-M...客端

1-N...密碼加速器(CA)

1-P...媒體源

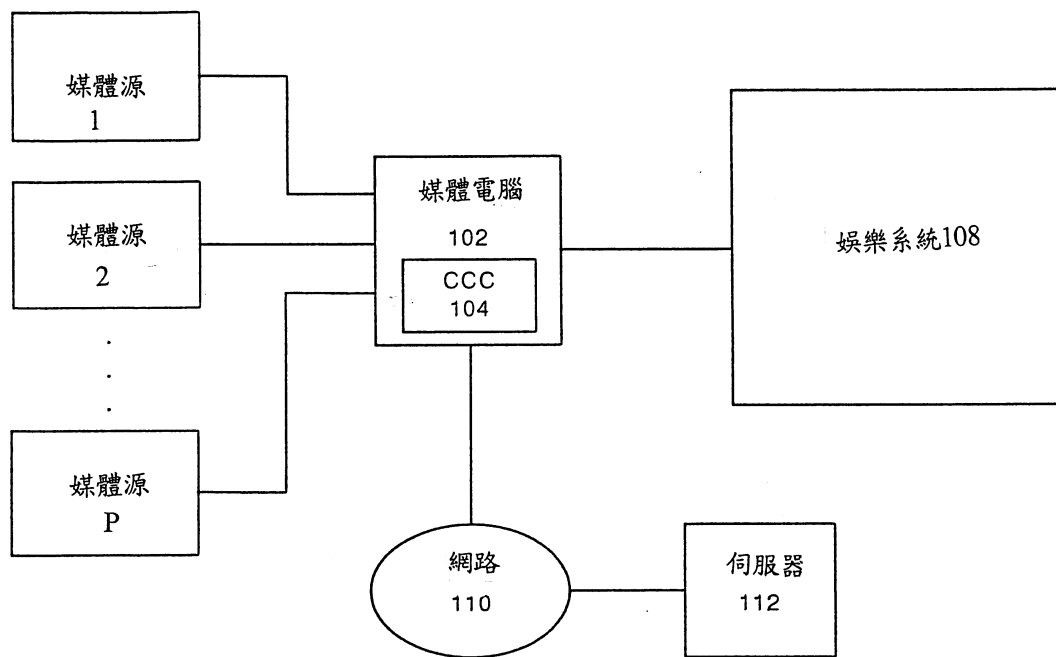
1-Q...描述器

五、中文發明摘要：

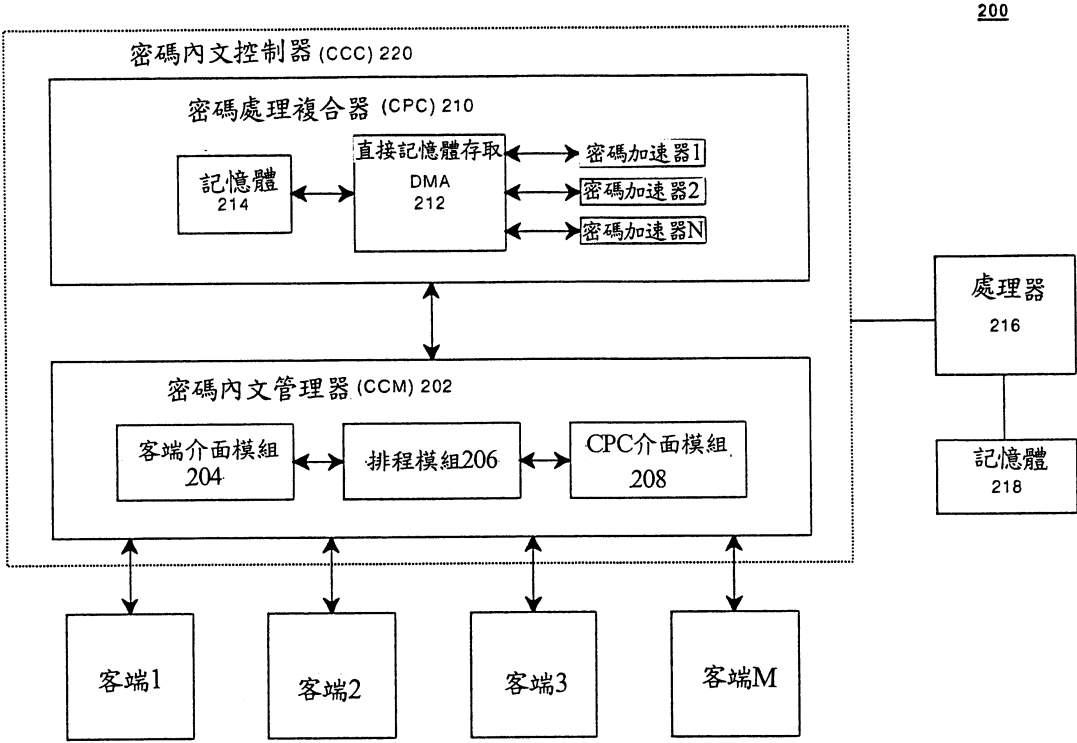
本文說明了供對多個客端執行密碼運算之系統用之方法及裝置。要對一內文流執行密碼運算之一請求可獲接收。可進行一判定來決定是否接受該請求。若該請求獲接受，則內文流可分派給多個密碼加速器之一。內文流可經排程，來接受密碼加速器之處理。內文流之密碼運算可根據該排程而由密碼加速器執行。

六、英文發明摘要：

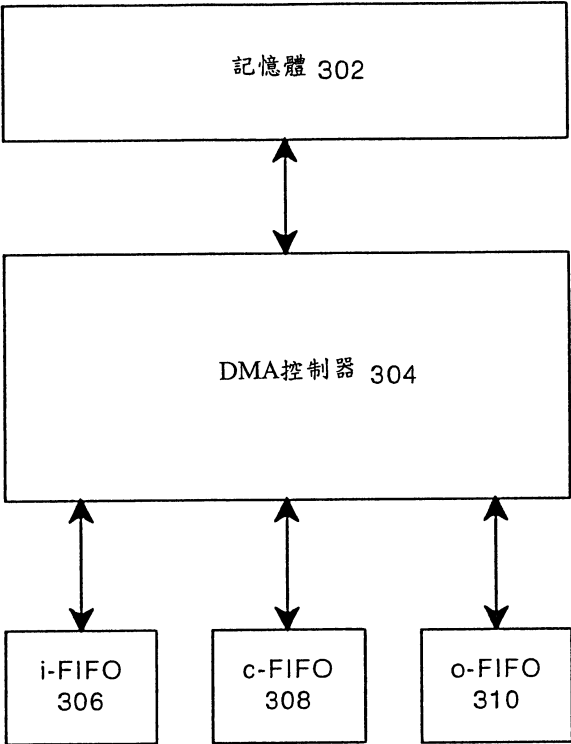
Method and apparatus for a system to perform cryptographic operations for multiple clients are described. A request to perform cryptographic operations for a context flow may be received. A determination may be made as to whether to accept the request. The context flow may be assigned to one of multiple cryptographic accelerators if the request is accepted. The context flow may be scheduled for processing by the cryptographic accelerator. The cryptographic operations for the context flow may be performed by the cryptographic accelerator in accordance with the schedule.



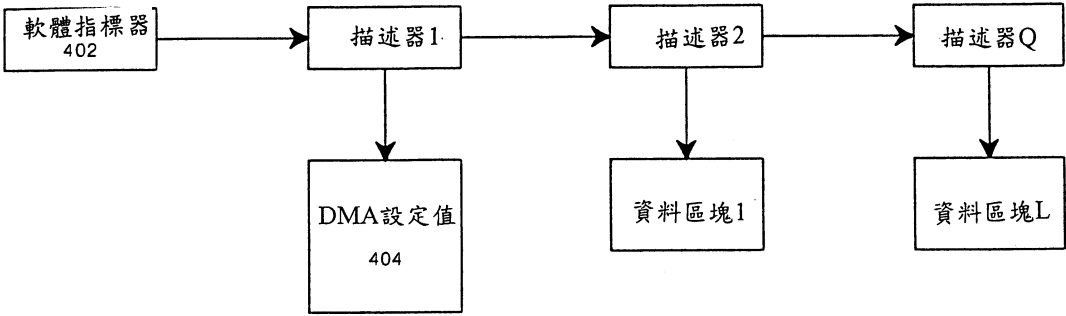
第 1 圖



第 2 圖

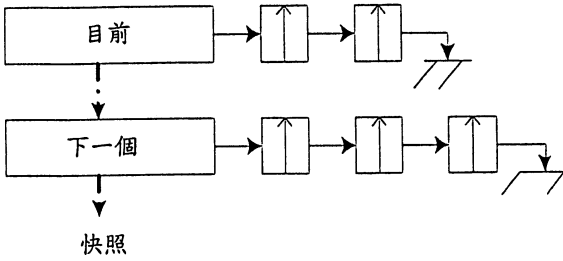
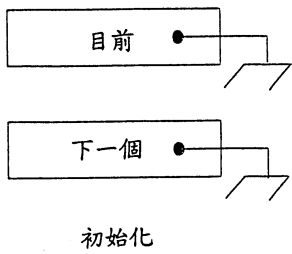


第 3 圖

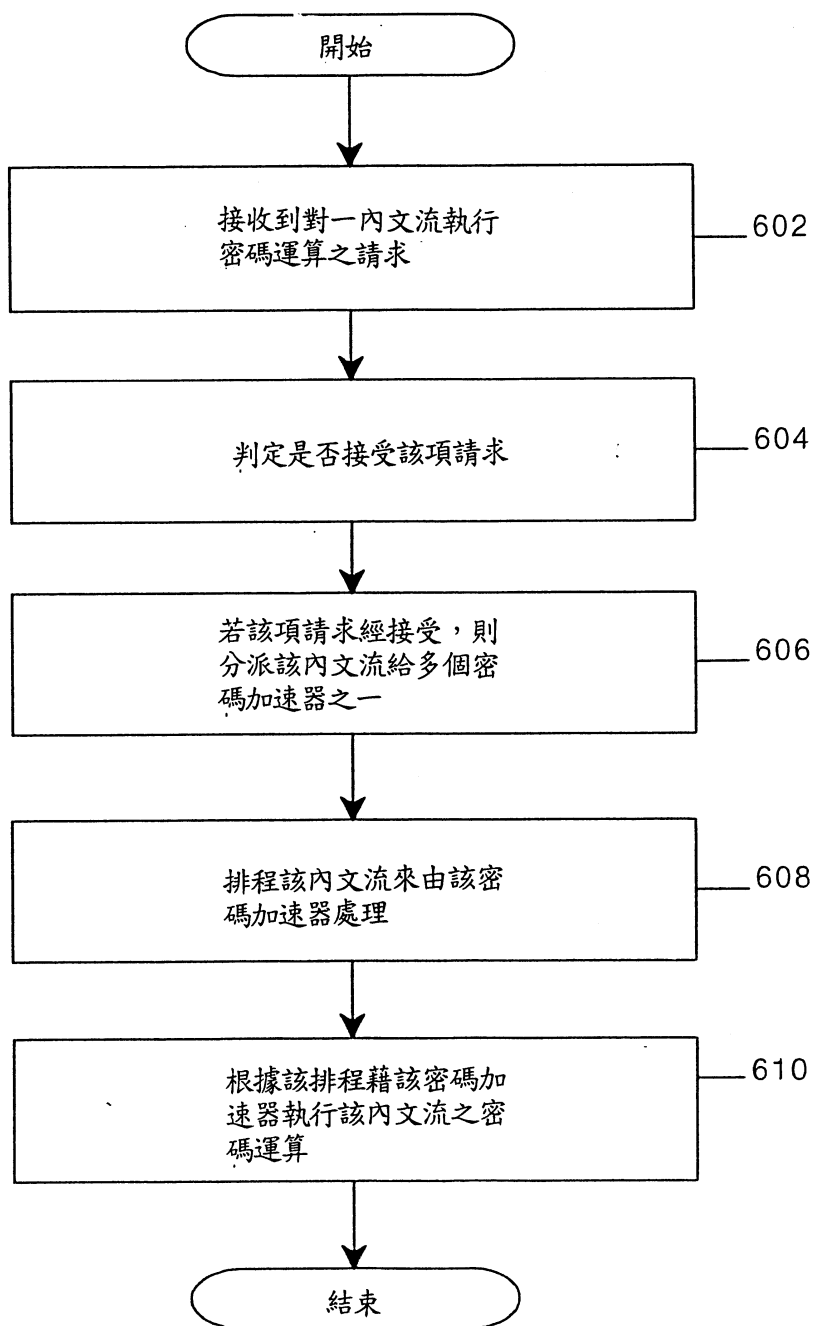


第 4 圖

500



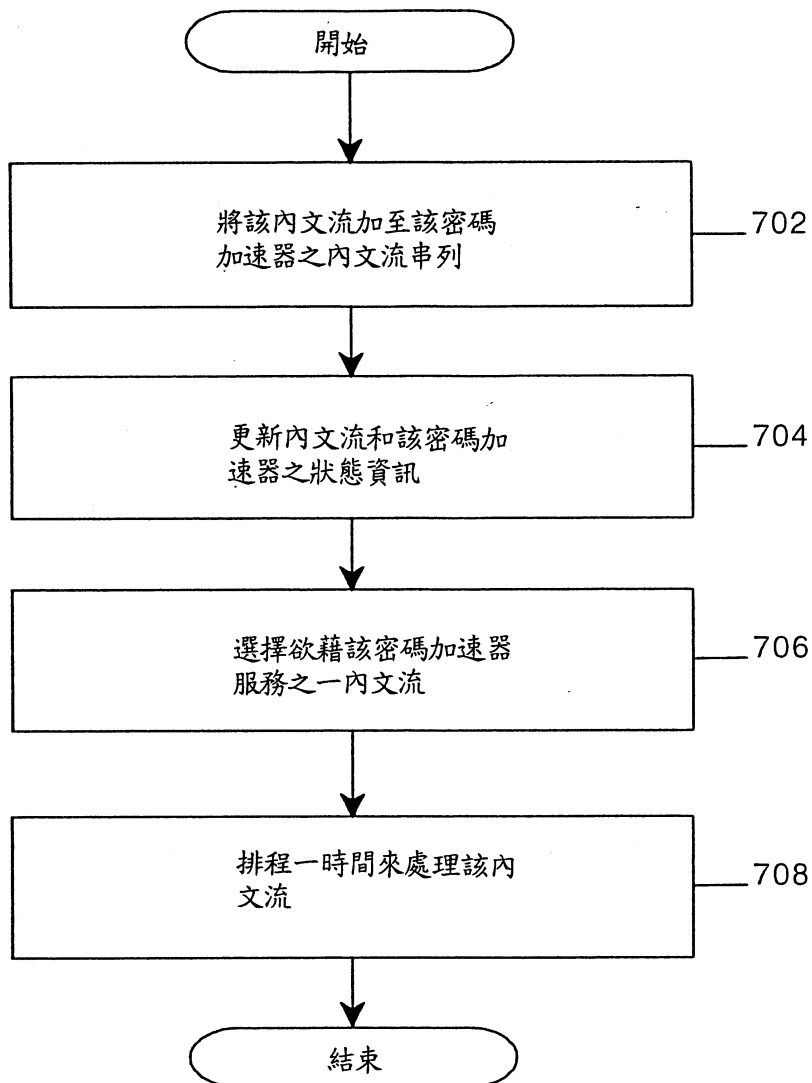
第 5 圖

600

第 6 圖

7/7

700



第 7 圖

七、指定代表圖：

(一)本案指定代表圖為：第 (6) 圖。

(二)本代表圖之元件符號簡單說明：

600…方塊流程圖

606…方塊

602…方塊

608…方塊

604…方塊

610…方塊

八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

之儲存裝置至各種I/O控制器之組合，其可由處理器存取，及其可儲存電腦程式指令與資料的組合。雖然第2圖顯示記憶體214及記憶體218為實體上分開之非連續記憶體，但須了解記憶體214及記憶體218也可使用相同或不同之實體及
5 邏輯定址體系來將實體記憶體連續集合分開成為一或多個邏輯分隔。該等具體例非囿限本內文。

若干具體例中，「程式指令」一詞包括得自預定電腦語言之電腦碼節段包含字、值及符號，其當根據預定方式或預定語法組合放置時，可造成處理器執行某項功能。電腦
10 語言包括C語言、C++語言、爪哇語言、組合語言、網路處理器用之微碼等。指令可以壓縮格式及/或加密格式而儲存於媒體。如此處使用，「適合由處理器執行」一詞表示涵蓋於一壓縮格式及/或加密格式儲存之指令，以及於藉處理器216執行之前必須藉安裝器編譯或安裝的指令。

15 若干具體例中，系統 200包括一或多個客端1-M。一個客端包含任何實體或任何代理器請求的密碼運算，諸如媒體源1-P。客端1-M之實例包括條件存取代理器、數位傳輸控制協定代理器、數位視訊碟片代理器及本地儲存代理器。客端1-M各自使用相同或相異之密碼技術來加密/解密由
20 客端1-M或經由客端1-M所通訊之一或多內文流。內文流之實例包括任何與客端1-M關聯之主動同步或異步資料流、或二客端1-M間之連結。主動資料流表示尚未結束或尚未逾時之任何開放通訊連結或通訊階段作業。內文流可以多種不同方式諸如內文參數、客端識別符等識別。各資訊流之型

作。藉密碼加速器處理之輸出資料區塊可儲存於o-FIFO 310。一旦全部目前執行期之運算皆已經完成，則輸出資料區塊可由o-FIFO 310移動至記憶體214。DMA控制器304可產生DMA岔斷，來通知排程模組206，已經到達i-FIFO 306 5 的水位標誌。水位標誌可經規劃於緩衝器描述器其描述該資料集合，水位標誌可藉DMA控制器304解譯。同樣地，製造商緩衝器位址(用來填充i-FIFO 306)、消費者緩衝器位址(用來填充o-FIFO 310)、及各個DMA頻道相關之控制碼對預定之運算作規劃。

- 10 第4圖顯示資料結構400。若干具體例中，資料結構400例如可表示由系統300使用之資料結構。如第4圖所示，資料結構400包含一鏈結串列，其包含一軟體指標器402、一描述器1-Q集合、一DMA設定值資料結構404及一資料區塊1-L集合。雖然顯示一特殊資料結構集合來作為資料結構 15 400之一部分，但須了解資料結構400可包含任何數目之不同資料結構或額外資料結構設計來支援系統300之運算需求。該等具體例並非囿限於本內文。

- 20 經由假設資料移動器的角色，DMA控制器304允許密碼加速器來將焦點集中在密碼處理。響應於各次DMA岔斷，排程模組206可存取一密碼加速器之目前主動內文流之就緒串列，且對一執行週期識別新的工作負載。由於排程模組206之動態性質，於其操作期間，一內文流可使用不同的密碼加速器。資料結構400舉例說明記憶體214之資料結構，其可用來支援資料流。對各個內文流，DMA控制器304

戶硬體元件之任一種組合來實作。該等具體例並非圍限於本內文。

【圖式簡單說明】

- 第1圖顯示系統100之方塊圖。
- 5 第2圖顯示系統200之方塊圖。
- 第3圖顯示系統300之方塊圖。
- 第4圖顯示一種資料結構400。
- 第5圖顯示一種資料結構500。
- 第6圖顯示方塊流程圖600。
- 10 第7圖顯示方塊流程圖700。

【主要元件符號說明】

100...系統	212...直接記憶體存取(DMA)
102...媒體電腦	214...記憶體
104...密碼內文控制器(CCC)	216...處理器
108...娛樂系統	218...記憶體
110...網路	220...密碼內文控制器(CCC)
112...伺服器	300...系統
200...系統	302...記憶體
202...密碼內文管理器(CCM)	304...DMA控制器
204...客端介面模組	306...輸入FIFO
206...排程模組	308...控制FIFO
208...密碼處理複合器(CPC)介面模組	310...輸出FIFO
210...密碼處理複合器(CPC)	400...資料結構
	402...軟體指標器

十、申請專利範圍：

第94116292號申請案申請專利範圍修正本 95.10.23.

1. 一種用以執行密碼運算之方法，包含下列步驟：

接收要對一內文流執行密碼運算之一請求；

5 判定是否接受該請求；

若該請求獲接受，則分派該內文流給多個密碼加速器之一；

排程該內文流以供用來由該密碼加速器處理；以及

10 根據該排程藉該密碼加速器執行該內文流之該等密碼運算。

2. 如申請專利範圍第1項之方法，其中該判定步驟包含：

接收供與該內文流相關聯之一客端用的一個客端識別符；

使用該客端識別符來認證該客端；

15 取回與該客端相關聯之一組客端資源參數集合、及與該等密碼加速器相關聯之一組系統資源參數集合；以及

使用該等客端資源參數及該等系統資源參數，來判定是否對該客端執行該等密碼運算。

20 3. 如申請專利範圍第1項之方法，其中該排程步驟包含：

將該內文流加至該密碼加速器之一內文流串列；

更新各個內文流及該密碼加速器之狀態資訊；

選擇欲由該密碼加速器服務之一內文流；以及

排程一時間來處理該內文流。

4. 如申請專利範圍第3項之方法，其中該選擇內文流之步驟包含：
- 為各內文流產生一鬆弛參數；以及
- 使用該等鬆弛參數來選擇該內文流。
5. 如申請專利範圍第1項之方法，其中該執行步驟包含：
- 為該內文流產生一資訊區塊，該資訊區塊包含輸入資料、控制資訊、內文資訊、及組態資訊；
- 以該控制資訊、內文資訊、及組態資訊來組配該密碼加速器；以及
- 使用該經組配之密碼加速器來處理該輸入資料。
6. 一種用以執行密碼運算之裝置，包含：
- 一密碼處理複合器，其係配置來對多個內文流執行密碼運算；以及
- 連接至該密碼處理複合器之一密碼內文管理器，該密碼內文管理器可管理該等多個內文流由該密碼處理複合器執行之動作。
7. 如申請專利範圍第6項之裝置，其中該密碼內文管理器包括一客端介面模組，用來接收要為一內文流執行密碼運算而來自一客端之一請求，認證該客端，以及判定該密碼處理複合器是否可對該客端及該內文流執行該等密碼運算。
8. 如申請專利範圍第6項之裝置，其中該密碼處理複合器包括多個密碼加速器；該密碼內文管理器包括一排程模組，用來分派該等多個內文流給一或多個密碼加速器，

以及用來產生各個密碼加速器處理該等多個內文流之一排程表。

- 5 9. 如申請專利範圍第6項之裝置，其中該密碼內文管理器包括一密碼處理複合器介面模組，該密碼處理複合器介面模組可介於該密碼內文管理器與該密碼處理複合器間傳送排程資訊。
- 10 10. 如申請專利範圍第6項之裝置，其中該等多個內文流包括欲根據一第一組密碼運算集合來處理之一第一內文流、以及欲根據一第二組密碼運算集合來處理之一第二內文流。
- 15 11. 如申請專利範圍第10項之裝置，其中該密碼處理複合器包括多個密碼加速器，該等多個密碼加速器包括一第一密碼加速器及一第二密碼加速器，該第一密碼加速器係執行該第一組密碼運算集合，以及該第二密碼加速器係執行該第二組密碼運算集合。
- 20 12. 如申請專利範圍第6項之裝置，其中該密碼處理複合器包括一直接記憶體存取控制器、多個密碼加速器、及記憶體，該直接記憶體存取控制器可於該記憶體與該等密碼加速器間傳輸資訊區塊，以及該等密碼加速器可使用該等區塊來執行密碼運算。
13. 如申請專利範圍第12項之裝置，其中該直接記憶體存取控制器包括一輸入資料緩衝器、一輸入控制緩衝器、及一輸出資料緩衝器，該直接記憶體存取控制器可由該記憶體取回一內文流之輸入資料區塊來儲存於該輸入資

料緩衝器，為欲處理該等輸入資料區塊之一密碼加速器而自該記憶體取回可執行之區塊來儲存於該輸入控制緩衝器，以及由該密碼加速器取回輸出資料區塊來儲存於該輸出資料緩衝器。

5 14. 一種用以執行密碼運算之系統，包含：

至少一客端，用來對多個內文流產生要求密碼運算的多個請求；以及

操作式響應於該客端之一密碼內文控制器，該密碼內文控制器包括：

10 配置來對該等多個內文流執行該等密碼運算之一密碼處理複合器；以及

用以管理由該密碼處理複合器執行該等多個內文流的動作之一密碼內文管理器。

15 15. 如申請專利範圍第14項之系統，其中該客端包含一條件式存取代理器、一數位傳輸控制協定代理器、一數位影碟代理器及一本地儲存代理器中之一者。

16. 如申請專利範圍第14項之系統，其中該系統包含一個客端，該一客端進送該等多個內文流至該密碼內文控制器。

20 17. 如申請專利範圍第14項之系統，其中該系統包含多個客端，而各個客端進送一或多個內文流至該密碼內文控制器。

18. 如申請專利範圍第14項之系統，其中該密碼內文管理器包括一客端介面模組，用來接收來自一客端欲對一內文流執行密碼運算之一請求，認證該客端，以及判定該密

碼處理複合器是否可對該客端及該內文流執行該等密碼運算。

- 5 19. 如申請專利範圍第14項之系統，其中該密碼處理複合器包括多個密碼加速器；該密碼內文管理器包括一排程模組，用來分派該等多個內文流給一或多個密碼加速器，以及用來產生各個密碼加速器處理該等多個內文流之一排程表。
- 10 20. 如申請專利範圍第14項之系統，其中該密碼內文管理器包括一密碼處理複合器介面模組，該密碼處理複合器介面模組可於該密碼內文管理器與該密碼處理複合器間傳送排程資訊。
- 15 21. 如申請專利範圍第14項之系統，其中該等多個內文流包括欲根據一第一組密碼運算集合來處理之一第一內文流、以及欲根據一第二組密碼運算集合來處理之一第二內文流。
- 20 22. 如申請專利範圍第21項之系統，其中該密碼處理複合器包括多個密碼加速器，該等多個密碼加速器包括一第一密碼加速器及一第二密碼加速器，該第一密碼加速器係執行該第一組密碼運算集合，以及該第二密碼加速器係執行該第二組密碼運算集合。
23. 如申請專利範圍第14項之系統，其中該密碼處理複合器包括一直接記憶體存取控制器、多個密碼加速器、及記憶體，該直接記憶體存取控制器可於該記憶體與該等密碼加速器間傳輸資訊區塊，以及該等密碼加速器可使用

該等區塊來執行密碼運算。

24. 一種包含有儲存媒體之物品，其中：

該儲存媒體包括有儲存之指令，該等指令在由一處理器執行時可操作來進行下列動作：

5 判定是否接受要對一內文流執行密碼運算之一請求，

若該請求獲接受，則分派該內文流給多個密碼加速器之一，

 排程該內文流用來由該密碼加速器處理，以及
10 根據該排程由該密碼加速器為該內文流執行該等密碼運算。

25. 如申請專利範圍第24項之物品，其中該等儲存之指令在由一處理器執行時，係使用可操作來執行下列動作的儲存之指令來進行該項判定動作：

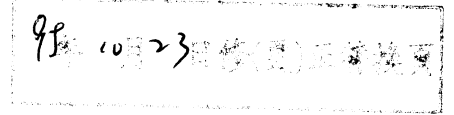
15 接收供與該內文流相關聯之一客端用之一客端識別符，

使用該客端識別符來認證該客端，

 取回與該客端相關聯之一組客端資源參數集合、及與該等密碼加速器相關聯之一組系統資源參數集合，以及
20 及

使用該等客端資源參數及該等系統資源參數，來判定是否對該客端執行該等密碼運算。

26. 如申請專利範圍第24項之物品，其中該等儲存之指令在由一處理器執行時，係使用可操作來執行下列動作的儲



存之指令來進行該項排程動作：

將該內文流加至該密碼加速器之一內文流串列，

更新各個內文流及該密碼加速器之狀態資訊，

選擇欲由該密碼加速器服務之一內文流，以及

5 排程一時間來處理該內文流。

27. 如申請專利範圍第26項之物品，其中該等儲存之指令在
由一處理器執行時，係使用可操作來執行下列動作的儲
存之指令來進行該項選擇動作：

為各內文流產生一鬆弛參數，以及

10 使用該等鬆弛參數來選擇該內文流。

28. 如申請專利範圍第24項之物品，其中該等儲存之指令在
由一處理器執行時，係使用可操作來執行下列動作的儲
存之指令來進行該等密碼運算：

為該內文流產生一資訊區塊，該資訊區塊包含輸入

15 資料、控制資訊、內文資訊、及組態資訊，

以該控制資訊、內文資訊、及組態資訊來組配該密
碼加速器，以及

使用該經組配之密碼加速器來處理該輸入資料。

20