

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：20094115311 (681)

※ 申請日期：94.5.11

※IPC 分類：

G06F 9/30 (2006.01)

一、發明名稱：(中文/英文)

支援密碼運算而具單數暫存器之資料移動器控制器

Data-Mover Controller With Plural Registers For Supporting Ciphering Operations

二、申請人：(共 1 人)

姓名或名稱：(中文/英文)

內數位科技公司/InterDigital Technology Corporation

代表人：(中文/英文) 唐納爾德·伯萊斯/Donald M. Boles

住居所或營業所地址：(中文/英文)

美國德拉威州 19801 威明頓德拉威大道 300 號 527 室

300 Delaware Avenue, Suite 527, Wilmington, DE 19801, U.S.A.

國 籍：(中文/英文) 美國 US

三、發明人：(共 1 人)

1. 姓 名：(中文/英文) 愛德華·赫普勒 / Edward L. HEPLER

國 籍：(中文/英文) 美國 /US

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 US；2004/05/24；No. 60/573,789

2. 美國 US；2004/06/28；No. 10/878,729

☐ 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】

本發明係有關可被用於無線通信應用之資料處理領域。更特別是，本發明係有關使用資料移動器控制器及密碼引擎來密碼運算及轉移資料於兩不同類型記憶體裝置之間。

【先前技術】

許多早期第三代夥伴計劃(3GPP)數據機係以軟體實施層 1 協定。隨著資料速率增加，硬體支援某些功能之需求係被要求。如第三代夥伴計劃，全球行動通信系統(GSM)及通用行動電信系統(UMTS)之無線通信系統中，硬體模組最近已被引進作為某些更計算密集操作之加速器。

一該操作係為密碼運算，藉此加密鑰匙及資料實際加密之操縱係等比被操縱資料量而增加所需處理容量。第三代夥伴計劃系統保全架構內，係具有兩標準化演算法：機密密碼演算法"f8"及完整密碼演算法"f9"。

一種當資料從一記憶體(也就是層)被移至另一記憶體時能有效執行密碼計算之裝置係被期待。

【發明內容】

一種資料處理系統密碼運算及轉移資料於第一記憶體單元及第二記憶體單元，如共享記憶體架構(SMA)靜態隨機存取記憶體(SRAM)及雙倍資料速率(DDR)同步動態隨機存取記憶體(SDRAM)之間。該系統包含一密碼引擎及一資料

移動器控制器。資料移動器控制器包含至少一暫存器，其具有可明定該被轉移資料是否應被密碼引擎作密碼運算之一欄位。

若該欄位明定該被轉移資料應被密碼運算，則該欄位亦明定將被密碼引擎執行之密碼運算類型，如第三代夥伴計劃標準化機密密碼演算法"f8"及完整密碼演算法"f9"。

該暫存器可包含明定被該標準化完整密碼演算法 f9 計算所計算之訊息認證碼(MAC)之另一欄位。

該暫存器可包含明定資料是否從第一記憶體單元被移至第二記憶體單元，或從第二記憶體單元被移至第一記憶體單元之再另一欄位。該第一及第二記憶體單元之處理速度不同。

該暫存器可包含明定被資料移動器控制器轉移之資料塊大小之再另一欄位。該資料塊大小可為四位元組，八位元組，十六位元組或三十二位元組。

該暫存器可包含明定被資料移動器控制器轉移之資料塊數量之再另一欄位。

該暫存器可包含明定當資料轉移完成時岔斷脈衝是否應被產生之再另一欄位。

該暫存器可包含明定被嵌入密碼標頭且被密碼引擎處理之值之再另一欄位。

該暫存器可包含明定加密長度之再另一欄位。

該暫存器可包含明定被嵌入加密標頭且被密碼引擎處理之值之再另一欄位。

該暫存器可包含明定被密碼引擎用來密碼運算被移動資料之鑰匙之再另一欄位。

【實施方式】

較佳實施例將參考附圖作說明，其中遍及全文之相似數字係代表相似元件。

較佳是，載此被揭示之本發明係被併入無線傳輸/接收單元(WTRU)及/或 B 節點。然而，設想只要有關任何無線通信計劃均可從本發明受益。

此後，無線傳輸/接收單元係包含但不限於使用者設備，行動台，固定或行動用戶單元，呼叫器，或可操作於無線環境中之任何其他類型元件。再者，B 節點係包含但不限於基地台，位址控制器，存取點或無線環境中之任何其他接介裝置。

本發明特性可被併入積體電路(IC)，或被併入包含複數互連組件之電路中。

本發明可應用至使用分時雙工(TDD)，分頻雙工(FDD)，分碼多重存取(CDMA)，分碼多重存取 2000(CDMA 2000)，分時同步分碼多重存取(TDSCDMA)，正交分頻多工(OFDM)或類似者之通信系統。

如同許多其他數據機實施，本發明係具有執行資料處理功能之硬體模組(加速器)。本發明係使用共享記憶體來降低既存記憶體例數量。硬體模組及一處理器係存取此記憶體。

相對於許多小型專用記憶體，藉由使用單記憶體，如用於數據機或類似者之電路之特定應用積體電路(ASIC)版本之晶粒尺寸係被降低。此記憶體通常需非常快。快速記憶體(靜態隨機存取記憶體(SRAM))通常非常貴，且從面積觀點並不如其他記憶體型式(也就是動態隨機存取記憶體(DRAM))般密集。例如，見 2003 年 4 月 15 日提出申請之美國專利申請號第 10/414,125 標題為"用於實體層處理之軟體可參數化控制塊"，其被併入參考作為完整說明。

本發明亦具有處理器可用來儲存大量資料之其他記憶體。此記憶體係藉由外部，商用動態隨機存取記憶體或同步動態隨機存取記憶體晶片來執行。被處理來應用之可儲存資料之再排序佇列及其他緩衝器係為此較大，較慢記憶體之使用例。

依據本發明，資料移動器控制器係被配置為快速，硬體可存取記憶體(靜態隨機存取記憶體)及較慢，較密集記憶體(動態隨機存取記憶體)之間資料移動之硬體加速器。不具有硬體加速器係意指處理器必須使用軟體迴路來到處轉移資料，因而耗費每秒百萬指令(MIPS)所測量之大部份處理器計算資源。

通常被移入塊之資料係被稱為協定資料單元(PDUs)及服務資料單元(SDUs)。這些塊可依據第三代夥伴計劃標準來加密。加密及解密處理亦非常需要處理器。其亦需資料被存取，處理且接著被寫回記憶體。

本發明係將直接記憶體存取(DMA)功能及密碼運算及

解密碼運算組合於單硬體加速器中，藉此資料移動器控制器不僅可移動資料，亦可於資料移動處理期間密碼運算及解密碼運算該資料塊。因為有硬體協助且資料已被移動處理，所以此節省時間。因此，所需存取較若獨立硬體加速器被實施為少。

某些實施中，各硬體加速器係具有其自我內部及介面(緩衝器)記憶體。許多記憶體例之擴散係增加這些設計之特定應用積體電路實施大小。

記憶體例數量可藉由組合許多介面(緩衝器)記憶體為單共享記憶體來降低。此記憶體係經由共用記憶體控制器被所有硬體加速器存取。此記憶體通常使用高速同步動態隨機存取記憶體來實施。控制軟體係引導該硬體加速器執行其個別運算，包含共享記憶體中引進資料及共享記憶體中儲存該被處理結果者。本發明係提供加速器給所有層 1 運算。

較高層控制(層 2 及 3)亦可對此共享記憶體存取以與層 1 通信，並提供將被傳送資料及接受已被接收資料。較大，較慢及較不密集記憶體通常係被層 2/3 處理用來固定被預定傳送或收集及組合資料封包以傳遞至應用之來自應用之資料。

當資訊封包被接收或被預定傳送時，資料必須被移動於此較慢，較不密集記憶體及較快，(較貴)記憶體之間。某些例中，這些封包亦必須被加密及/或被解密。

移動資料及協助密碼運算之加速器係被組合來形成資

料移動器控制器。此組合降低必須被執行之存取數量及使處理器免除移動及密碼運算該資料之昂貴處理。

當資料被移動於層 1 及 2 或 3 之間時，附加控制層通常必需被"包覆"於資料封包周圍。此通常以被附著至資料封包之"標頭"型式來表示。資料移動器控制器之定址計劃係藉由允許來源及/或目的地地址包含一偏移來說明此。此允許處理器將資料從一記憶體空間移至另一個，但卻偏移目的地資料如 3 位元組。一旦移動完成，處理器即可將適當標頭資訊經由該偏移寫入針對此被保留之區域。此降低有時發生於層 2 或 3 之格式化資料之資料四處移動。

本發明係為可轉移資料於共享記憶體架構靜態隨機存取記憶體及雙倍資料速率同步動態隨機存取記憶體間之資料處理系統。其亦可將資料從同步動態隨機存取記憶體中之一位置移動至相同同步動態隨機存取記憶體中之另一位置。當若被程式化資料被移除時，其可經由執行密碼計算之邏輯來傳送。

第 1 圖顯示被用來轉移資料於共享記憶體架構靜態隨機存取記憶體 105 及同步動態隨機存取記憶體 110 之間，而同時依據本發明較佳實施例密碼運算及解密碼運算該資料之資料處理系統 100 例方塊圖。共享記憶體架構控制器 115 係當作共享記憶體架構靜態隨機存取記憶體 105 及資料處理系統 100 間之介面。同步動態隨機存取記憶體控制器 120 係當作同步動態隨機存取記憶體 110 及資料處理系統 100 間之介面。處理器 125(也就是控制中央處理單元)係維

持對資料處理系統 100，共享記憶體架構靜態隨機存取記憶體 105，共享記憶體架構控制器 115，同步動態隨機存取記憶體 110 及同步動態隨機存取記憶體控制器 120 之控制。

資料處理系統 100 係包含一資料移動器控制器 128，一密碼引擎 130，輸入資料暫存器 135，140，輸出資料暫存器 145，150，輸入多工器(MUX)155，輸出多工器 160，及一先進先出(FIFO)暫存器 165。

資料移動器控制器 128 係藉由寫入具有被存取之資料起始文字位址之同步動態隨機存取記憶體 110 位址暫存器至同步動態隨機存取記憶體 110 記憶體空間中來設計程式。共享記憶體架構靜態隨機存取記憶體 105 位址暫存器係藉由寫入具有被存取之資料起始文字位址至共享記憶體架構靜態隨機存取記憶體 105 來設計程式。
"Num_blocks_to_move"暫存器係被寫入將移動之資料塊數量。模式暫存器係決定資料移動方向(也就是"0"=從共享記憶體架構靜態隨機存取記憶體 105 至同步動態隨機存取記憶體 110，"1"=從同步動態隨機存取記憶體 110 至共享記憶體架構靜態隨機存取記憶體 105)。各塊大小亦被定義如每塊 32 位元文字數。被轉移之 32 位元文字總數係被指定為 "Num_blocks_to_move*block_size"。資料處理系統 100 之資料移動器控制器 128 內之模式暫存器係標示資料是否應直接被轉移或當資料轉移發生時，資料是否應穿過密碼引擎 130。寫入模式暫存器係使資料移動器控制器 128 啟動資料移動程序。當資料轉移完成時，岔斷係被資料移動器控

制器 128 選擇性設定。

顯示被資料處理系統 100 用來將資料從一記憶體(如共享記憶體架構靜態隨機存取記憶體 105)移至另一記憶體(如同步動態隨機存取記憶體 110)，而經由密碼引擎 130 傳送資料之一步一步例現在將被說明。決定將被儲存於共享記憶體架構靜態隨機存取記憶體 105 中之資料移至同步動態隨機存取記憶體 110 中。處理器 125 接著將控制塊寫入共享記憶體架構靜態隨機存取記憶體 105 中。控制塊係包含針對預期操作配置資料移動器控制器 128 所需之所有參數。處理器 125 係經由被程式設計輸入/輸出(I/O)操作輸出控制信號(也就是起始脈衝)至資料移動器控制器 128 來啟動資料啟動操作。資料移動器控制器 128(有效為狀態機器)係經由一系列狀態接收控制信號及序列從共享記憶體架構靜態隨機存取記憶體 105 檢索控制塊。此係藉由適當主張經由共享記憶體架構控制器 115 來自共享記憶體架構靜態隨機存取記憶體 105 之要求來達成。來自共享記憶體架構靜態隨機存取記憶體 105 之資料係被輸入暫存器 115，且被傳送至資料移動器控制器 128 內之適當配置暫存器。

一旦相關控制參數被接收，則在此被包含之資訊係解釋何類型功能將被執行以進一步引導資料移動器控制器 128。此例中，資料係從共享記憶體架構靜態隨機存取記憶體 105 被移至同步動態隨機存取記憶體 110。若合適，資料移動器控制器 128 係使被包含於相關暫存器中之密碼標頭資訊穿越輸入暫存器 135，輸入多工器 155，先進先出 165，

密碼引擎 130，多工器 160，並經由輸出暫存器 150 及同步動態隨機存取記憶體控制器 120 輸出至同步動態隨機存取記憶體 110。資料移動器控制器 128 繼續經由適當狀態排序轉移來自共享記憶體架構靜態隨機存取記憶體 105 之資料直到適當項數被轉移為止。

若被要求，標示資料移動被完成之岔斷係藉由資料移動器控制器 128 內之暫存器產生。資料移動器控制器 128 接著檢查是否具有被移動之另一控制塊。若是，則另一資料移動器控制器程序係被啟動。

資料移動器控制器 128 係使用叢集存取轉移資料往返雙倍資料速率同步動態隨機存取記憶體 110，及使用單文字存取往返共享記憶體架構靜態隨機存取記憶體 105。直到程式設計師保證塊大小及雙倍資料速率同步動態隨機存取記憶體 110 位址被設定使得並無任何單同步動態隨機存取記憶體叢集存取跨越同步動態隨機存取記憶體頁邊界。

第 2 圖顯示第 1 圖之資料移動器控制器 128 中之暫存器 205-255 配置例。

第 3 圖顯示定義用於來源存取(也就是讀取)同步動態隨機存取記憶體 110 之資料移動器控制器 128 起始位址以啟動資料轉移至共享記憶體架構靜態隨機存取記憶體 105 或至同步動態隨機存取記憶體 110 之暫存器 205。該位址係為一位元組位址且必須被校準至順從被明訂於"模式"暫存器中之塊大小之位址。被寫入暫存器之值係有關同步動態隨機存取記憶體位址空間起始。該位址暫存器僅可被寫入

於資料移動器控制器 128 閒置時。最小顯著位元係於存取期間被忽略，但被使用於密碼運算來明定文字內之資料位移時。

第 4 圖顯示定義用於目的地存取(也就是寫入)同步動態隨機存取記憶體 110 之資料移動器控制器起始位址以啟動資料從共享記憶體架構靜態隨機存取記憶體 105 或從同步動態隨機存取記憶體 110 轉移之暫存器 215。該位址係為一位元組位址且必須被校準至順從被明訂於"模式"暫存器中之塊大小之位址。被寫入暫存器之值係有關同步動態隨機存取記憶體位址空間起始。該位址暫存器僅可被寫入於資料移動器控制器 128 閒置時。最小顯著位元係於存取期間被忽略，但被使用於密碼運算來明定文字內之資料位移時。

第 5 圖顯示定義用於來源存取(也就是讀取)共享記憶體架構靜態隨機存取記憶體 105 起始位址之暫存器 205。被寫入暫存器之值係有關共享記憶體架構位址空間起始。該位址暫存器僅可被寫入於資料移動器控制器 128 閒置時。最小顯著位元係於存取期間被忽略，但被使用於密碼運算來明定文字內之資料位移時。

第 6 圖顯示定義用於目的地存取(也就是寫入)共享記憶體架構靜態隨機存取記憶體 105 起始位址之暫存器 220。資料移動器控制器 128 之位址係被明定給該資料移動器控制器 128 來存取共享記憶體架構靜態隨機存取記憶體 105。被寫入暫存器之值係有關共享記憶體架構位址空間起始。

該位址暫存器僅可被寫入於資料移動器控制器 128 閒置時。最小顯著位元係於存取期間被忽略，但被使用於密碼運算來明定文字內之資料位移時。

第 7 圖顯示定義將被移動於同步動態隨機存取記憶體 110 及共享記憶體架構靜態隨機存取記憶體 105 間之塊數量之暫存器 225。當被啟動時，資料移動器控制器將轉移此暫存器中之值所表示之塊數量。各塊係包含被明定於模式暫存器之"bs"欄位中之 32 位元文字數。

第 8 圖顯示明定資料移動器控制器 128 之模式之模式暫存器 230。操作時，模式暫存器 230 內之各欄位 805, 810, 815, 820, 825 可被寫入來控制資料移動器控制器動作。

"f"欄位 805 係唯讀及指示處理器 195 資料移動操作是否已完成(也就是邏輯 0 用於未完成或邏輯 1 用於已完成)。

"c"欄位 810 可被寫入指示資料是否應被穿越密碼引擎，若是，則何種密碼運算來執行。當"c"欄位 810 為"00"時，並無任何密碼運算被執行，而資料僅從來源位址空間傳送至目的地位址空間。當"c"欄位 810 為"01"時，資料係使用第三代夥伴計劃"f8"密碼演算法從來源位址空間被移至目的地位址空間，但資料移動時係被穿越密碼引擎 145 及被加密及/或被解密。當"c"欄位 810 為"10"時，資料係使用第三代夥伴計劃"f9"密碼演算法從來源位址空間被存取且被穿越密碼引擎 145，但該資料不被儲存。密碼引擎 145 係使用鑰匙及相關控制暫存器值來計算經由暫存器 255 可被處理器 195 獲得之訊息認證編碼值。

當資料移動被完成時，"i"欄位 810 可被程式化來產生岔斷。當"i"欄位 815 為"0"時，並無任何岔斷被產生。當"i"欄位 815 為"1"時，岔斷係被產生於資料移動操作被完成時。

"d"欄位 820 係識別被當作來源及目的地址空間之一個或更多記憶體及明定資料移動方向。例如，當"d"欄位 820 為"00"時，資料係從共享記憶體架構靜態隨機存取記憶體 105 被移至同步動態隨機存取記憶體 110。當"d"欄位 820 為"10"時，資料係從同步動態隨機存取記憶體 110 被移至共享記憶體架構靜態隨機存取記憶體 105。當"d"欄位 820 為"01"時，資料係從同步動態隨機存取記憶體 110 內之一位置被移至另一位置。"d"欄位 820 係被用來決定何記憶體位址指標經由存取要求來引動。

"bs"欄位 825 係決定將被移動之各存取塊大小。"bs"欄位 825 可被設定標示一文字("00"=四位元組)，二文字("01"=八位元組)，四文字("10"=十六位元組)，八文字("11"=三十二位元組)之每塊存取之值。將被移動及/或被密碼運算之文字數係藉由程式化"bs"欄位 825 及移動塊數。總資料移動係以"bs"欄位 825 所表示之值乘積及被明定於暫存器 255 中之塊數量。

第 9 圖顯示定義被嵌入密碼標頭之計數值之暫存器 235。

第 10 圖顯示定義被嵌入密碼標頭之最新值之暫存器 240。

第 11 圖顯示定義必須被放入加密標頭之承載及方向值

及將被加密之位元總數之暫存器 245。暫存器 235，240 及 245 係包含被包含於密碼標頭之第三代夥伴計劃標準所定義之被處理器 195 寫入之值。當密碼運算被包含於資料移動時，這些值係被資料移動器控制器插入適當位置。加密長度欄位係明定有多少位元穿越密碼引擎。塊數量及每塊文字數係被程式設計者預先決定且必須說明此長度。

第 12 圖顯示定義資料移動期間被用於密碼運算之 128 位元鑰匙之暫存器 250。當執行 f8 及 f9 密碼演算法時，鑰匙值於第三代夥伴計劃標準中所說明係被用來加密/解密資料。

第 13 圖顯示提供被計算訊息認證碼值之暫存器 255。f9 密碼演算法係使用該鑰匙值及被呈現至其之資料流值來創造簽章。此簽章係被報告為媒體存取控制給系統使用。

在此被揭示之暫存器說明性質上為例證，藉此其他任意定義可以控制欄位組合來執行相同功能性。

雖然本發明已以較佳實施例型式作說明，但熟練技術人士將了解被描繪於以下申請專利範圍中之本發明範圍內之其他變異。

【圖式簡單說明】

第 1 圖係為依據本發明較佳實施例之密碼運算及轉移資料從一記憶體至另一記憶體之資料處理系統圖示；

第 2 圖顯示被併入資料移動器控制器之暫存器配置例；

第 3 圖顯示定義該資料移動器控制器起始位址從同步動態隨機存取記憶體存取來源之暫存器；

第 4 圖顯示定義該資料移動器控制器起始位址存取目的地至同步動態隨機存取記憶體之暫存器；

第 5 圖顯示定義該資料移動器控制器起始位址存取來源至同步動態隨機存取記憶體之暫存器；

第 6 圖顯示定義該資料移動器控制器起始位址存取目的地至共享記憶體架構記憶體之暫存器；

第 7 圖顯示定義將被移動於同步動態隨機存取記憶體及共享記憶體架構記憶體之間之塊數量之暫存器；

第 8 圖顯示明定該資料移動器控制器模式之暫存器；

第 9 圖顯示定義被嵌入密碼標頭之計數值之暫存器；

第 10 圖顯示定義被嵌入密碼標頭之最新值之暫存器；

第 11 圖顯示定義必須被放入加密標頭之承載及方向值及將被加密之位元總數之暫存器；

第 12 圖顯示定義資料移動期間被用於密碼運算之 128 位元鑰匙之暫存器；及

第 13 圖顯示提供被計算訊息認證碼值之暫存器。

【主要元件符號說明】

100	方塊圖
115、120	控制器
135、145、140、150、165、205、215、210、220、225、230、235、240、245、250、255	暫存器
155、160	多工器
130	密碼引擎
128	資料移動控制器
125	處理器
SMA	共享記憶體架構
SRAM	靜態隨機存取記憶體
SDRAM	同步動態隨機存取記憶體
DM	資料移動器

五、中文發明摘要：

一種資料處理系統，其於第一記憶體單元及第二記憶體單元間進行密碼運算及轉移資料，例如，於一共享記憶體架構(SMA)靜態隨機存取記憶體(SRAM)及雙倍資料速率(DDR)同步動態隨機存取記憶體(SDRAM)間進行。該系統包含一密碼引擎及一資料移動器控制器。資料移動器控制器包含至少一暫存器，其具有明定是否應密碼運算該轉移資料之一欄位。若該欄位明定應密碼運算該轉移資料，則該欄位亦明定由密碼引擎執行之密碼運算類型，如第三代夥伴計劃標準化機密密碼演算法"f8"及完整密碼演算法"f9"。

六、英文發明摘要：

A data processing system ciphers and transfers data between a first memory unit and a second memory unit, such as, for example, between a share memory architecture (SMA) static random access memory (SRAM) and a double data rate (DDR) synchronous dynamic random access memory (SDRAM). The system includes a ciphering engine and a data-mover controller. The data-mover controller includes at least one register having a field that specifies whether or not the transferred data should be ciphered. If the field specifies that the transferred data should be ciphered, the field also specifies the type of ciphering that is to be performed, such as a third generation partnership project (3GPP) standardized confidentially cipher algorithm "f8" or integrity cipher algorithm "f9".

十、申請專利範圍：

1. 用於對一第一記憶體單元及一第二記憶體單元之間的資料進行密碼運算及轉移的無線傳送/接收方法，該方法包括：

一密碼引擎，當資料在該記憶體單元之間轉移時用於對該資料進行密碼運算；

一資料移動器控制器，包括具有一第一欄位的至少一暫存器，該第一欄位明定該轉移的資料是否應由該密碼引擎進行密碼運算；

一處理器，與該第一記憶體單元和該第二記憶體單元電耦合，用於將一控制塊寫入該第一記憶體單元中，該控制塊包括配置該資料移動器控制器所需之控制參數，並用於將一控制信號輸出至該資料移動器控制器以啟動一資料移動操作；

一第一控制器，與該第一記憶體單元、該資料移動器控制器和該處理器電耦合，用以控制該第一記憶體單元；以及

一第二控制器，與該第二記憶體單元、該資料移動器控制器和該處理器電耦合，用於控制該第二記憶體單元，其中該資料移動器控制器回應於從該處理器接收的該控制信號而從該第一記憶體單元擷取該控制塊，且該資料移動器控制器基於該擷取的控制塊中的該控制參數來決定將執行何種類型功能。

2. 如申請專利範圍第 1 項的無線傳送/接收單元，其中，若該第一欄位明定該轉移的資料應被密碼運算，則該第一欄位亦明定將被執行的密碼運算類型。

3. 如申請專利範圍第 2 項的無線傳送/接收單元，其中該無線傳送/接收單元與一第三代夥伴計劃系統（3GPP）連結操作，且

將被執行之該密碼運算類型為一標準化機密密碼演算法 f8。

4. 如申請專利範圍第 2 項的無線傳送/接收單元，其中該無線傳送/接收單元與一第三代夥伴計劃系統（3GPP）連結操作，且將被執行之該密碼運算類型為一標準化完整密碼演算法 f9。

5. 如申請專利範圍第 4 項的無線傳送/接收單元，其中該暫存器包括一第二欄位，該第二欄位明定由該標準化完整密碼演算法 f9 所計算之一訊息認證碼（MAC）值。

6. 如申請專利範圍第 1 項的無線傳送/接收單元，其中該暫存器包括一第二欄位，該第二欄位明定是否將資料從該第一記憶體單元移至該第二記憶體單元或從該第二記憶體單元移至該第一記憶體單元。

7. 如申請專利範圍第 1 項的無線傳送/接收單元，其中該暫存器包括一第二欄位，該第二欄位明定將由該資料移動器控制器所轉移的一資料塊大小。

8. 如申請專利範圍第 7 項之無線傳送/接收單元，其中該資料塊大小為四位元組。

9. 如申請專利範圍第 7 項之無線傳送/接收單元，其中該資料塊大小為八位元組。

10. 如申請專利範圍第 7 項之無線傳送/接收單元，其中該資料塊大小為十六位元組。

11. 如申請專利範圍第 7 項之無線傳送/接收單元，其中該資料塊大小為三十二位元組。

12. 如申請專利範圍第 1 項之無線傳送/接收單元，其中該暫存器包括一第二欄位，該第二欄位明定將由該資料移動器控制器

所轉移的資料塊的數量。

13. 如申請專利範圍第 1 項之無線傳送/接收單元，其中該第一記憶體為一共享記憶體架構（SMA）靜態隨機存取記憶體（SRAM）。

14. 如申請專利範圍第 1 項之無線傳送/接收單元，其中該第二記憶體為一同步動態隨機存取記憶體（SDRAM）。

15. 如申請專利範圍第 1 項之無線傳送/接收單元，其中該第一及該第二記憶體單元之處理速度不同。

16. 如申請專利範圍第 1 項之無線傳送/接收單元，其中該暫存器包括一第二欄位，該第二欄位明定當完成該資料的轉移時是否應產生一岔斷脈衝。

17. 如申請專利範圍第 1 項之無線傳送/接收單元，其中該暫存器包括一第二欄位，該第二欄位明定一嵌入於一密碼標頭且由該密碼引擎處理的值。

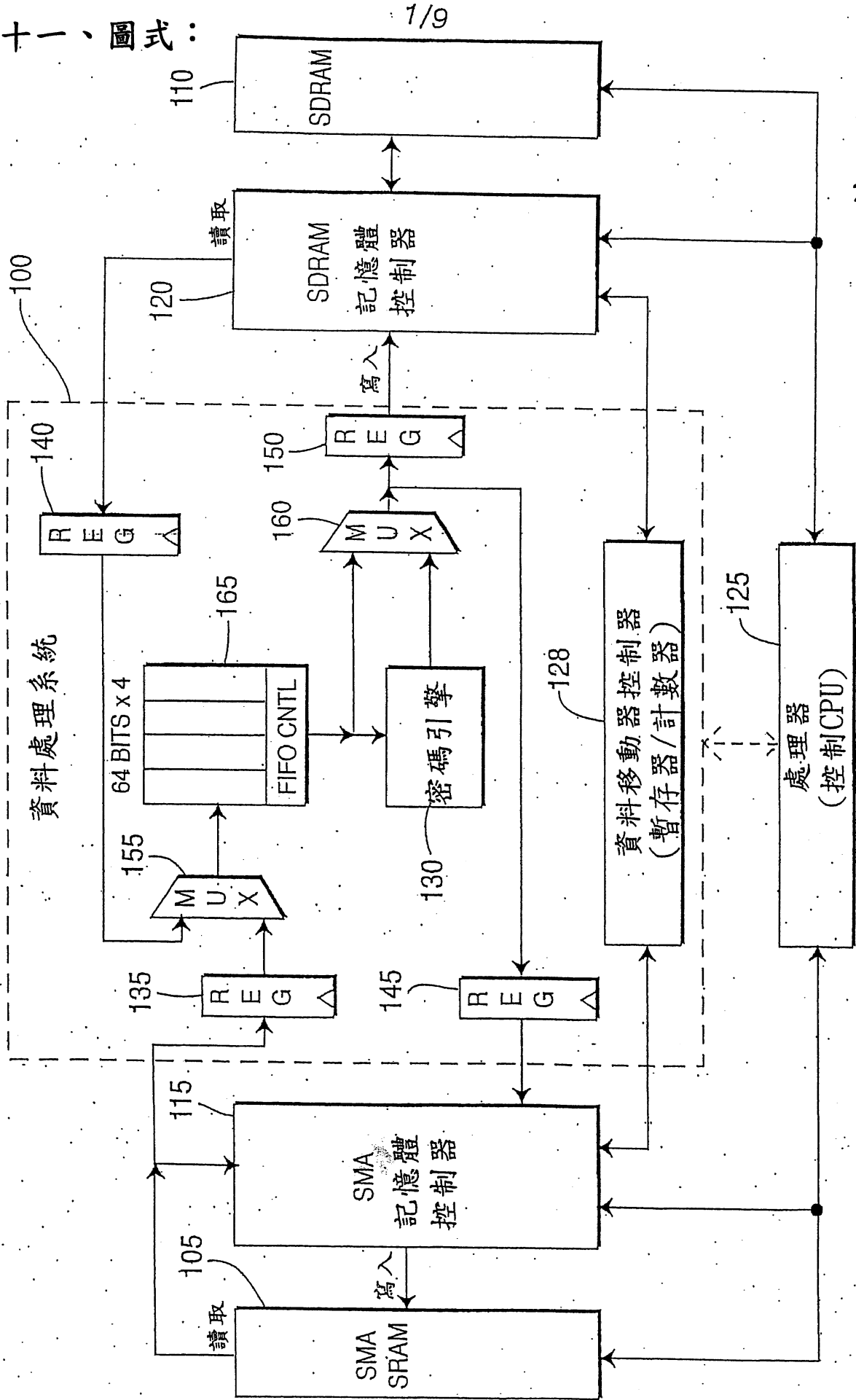
18. 如申請專利範圍第 1 項之無線傳送/接收單元，其中該暫存器包括一第二欄位，該第二欄位明定一加密長度。

19. 如申請專利範圍第 1 項之無線傳送/接收單元，其中該暫存器包括一第二欄位，該第二欄位明定一嵌入於一加密標頭且由該密碼引擎處理的值。

20. 如申請專利範圍第 1 項之無線傳送/接收單元，其中該暫存器包括一第二欄位，該第二欄位明定一由該密碼引擎所使用的一鑰匙以用於密碼運算被移動的資料。

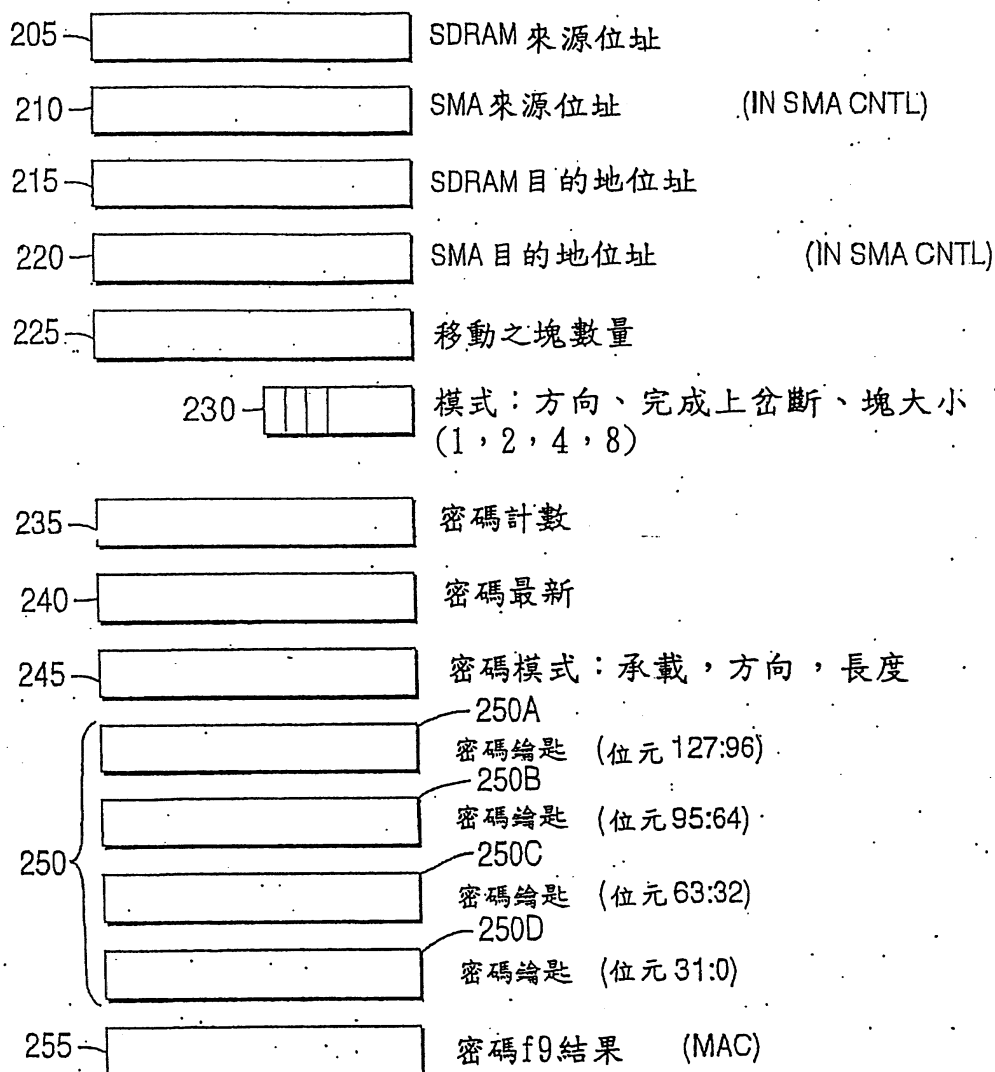
21. 如申請專利範圍第 20 項之無線傳送/接收單元，其中該鑰匙為一 128 位元鑰匙。

十一、圖式：



第 1 圖

2/9



第 2 圖

DM_SDRAM_來源_位址

此暫存器定義資料移動器啟動位址用於來源存取同步動態隨機存取記憶體

名稱：	DM_SDRAM_來源_位址										位址：	0x08e00100										被寫入：	右臂									
位元：	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
資料：	ADDR																															

205

第 3 圖

DM_SDRAM_目的地_位址

此暫存器定義資料移動器啟動位址用於目的地存取同步動態隨機存取記憶體

名稱：	DM_SDRAM_目的地_位址										位址：	0x08e00110										被寫入：	右臂									
位元：	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
資料：	ADDR																															

215

第 4 圖

DM_SMA_來源_位址

此暫存器定義資料移動器啟動位址用於來源存取共享記憶體架構

名稱：	DM_SMA_來源_位址										位址：	SMA 指標										被寫入：	右臂									
位元：	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
資料：	ADDR																															

欄位	列舉	位元指數
ADDR		31:0

210

第 5 圖

DM_SMA_目的地_位址

此暫存器定義資料移動器啟動位址用於目的地存取共享記憶體架構

名稱：	DM_SMA_目的地_位址										位址：	SMA 指標										被寫入：	右臂									
位元：	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
資料：	ADDR																															

220

第 6 圖

欄位	列舉	位元指數
ADDR		31:0

DM_數量_塊

此暫定器係定義將被移動於同步動態隨機存取記憶體及共享記憶體架構間之塊數量。各塊係包含被明定於"模式"暫存器之文字數(達到84位元組文字(32位元))

名稱：	DM_數量_塊																位址：				0x08e00120												被寫入：				右臂											
位元：	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0																
資料：																																			數量													

欄位	列舉												位元指數												說明											
保留													31:16												未來使用											
數量													15:0												明定同步動態隨機存取記憶體及共享記憶體架構記憶體間之移動塊數量											
說明：																									注意寫入此暫存器係啟動資料移動器。 當被寫入時，"模式"暫存器之"f"位元係被清除。 當轉移完成時，"f"位元係被設定而選擇岔斷脈衝係被產生。											

DM_模式

此暫存器係定義資料移動器塊數量

第 8 圖

230

名稱：	DM_模式																位址：				0x08e00130								被寫入：				右臂							
位元：	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0								
資料：	f																											c	i	d		bs								

欄位	列舉	位元指數	說明
f	'0'- 未達成 '1'- 達成	31	完成旗標
保留		30:7	未來使用
c	'00'- 無密碼運算 '01'- 資料係使用 f8 型密碼運算來移除 '10'- 資料係被存取而 f9 密碼運算係被執行	6:5	明定密碼模式
i	'0'- 無岔斷被產生 '1'- 岔斷被產生於移動完成時	4	明定岔斷脈衝是否應被產生於資料移動完成時
d	'00'- 共享記憶體架構至同步動態隨機存取記憶體 '01'- 同步動態隨機存取記憶體至同步動態隨機存取記憶體 '10'- 同步動態隨機存取記憶體至共享記憶體架構	3:2	明定資料移動方向
bs	'00'- 一文字 (4 位元組) '01'- 二文字 (8 位元組) '10'- 四文字 (16 位元組) '11'- 八文字 (32 位元組)	1:0	明定移動塊大小
說明：	模式暫存器決定被資料移動器移動之塊大小，其亦明定移動方向及明定岔斷脈衝是否應被產生於資料移動完成時。 注意同步動態隨機存取記憶體之"叢集"進/出將以塊大小為基礎來達成。		

DM_密碼_計數 235 第 9 圖

此暫定器定義被嵌入密碼標頭之計數值

名稱：	DM_密碼_計數										位址：				0x08e00140				被寫入：				右臂															
位元：	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0						
資料：	COUNT																																					

欄位	列舉	位元指數	說明
計數		31:0	明定被嵌入密碼標頭之計數值
說明：	此暫定器明定被嵌入密碼標頭之計數值。 其必須於資料移動器被啟動之前被寫入(當密碼運算模式被使用時)		

DM_密碼_最新 240 第 10 圖

此暫定器定義被嵌入密碼標頭之最新值

名稱：	DM_ 密碼 _ 最新										位 址：				0x08e00150				被 寫 入：				右 臂															
位 元：	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0						
資 料：	計 數																																					

欄位	列舉	位元指數	說明
計數		31:0	明定被嵌入密碼標頭之最新值
說明：	此暫定器明定被嵌入密碼標頭之最新值。此值僅被使用於"f9"密碼模式。 其必須於資料移動器被啟動之前被寫入(當密碼運算模式被使用時)		

DM_ 密碼 _ 模式

此暫存器報告何FIRQ岔斷來源目前主動。主動FIRQ岔斷位元係被清除。

名稱：	DM_ 密碼 _ 模式										位址：				0x08e00130										被寫入：				右臂									
位元：	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0						
資料：	承載										d																								長度			

欄位	列舉	位元指數	說明
承載		31:27	明定被嵌入加密標頭之承載值
d		26	明定被嵌入加密標頭之方向值
保留		25:18	未來使用
長度		17:0	明定加密長度(位元)
說明：	此暫定值包含被嵌入密碼標頭之承載及方向值。長度欄位係明定被密碼運算之資料位元數		

DM_密碼_鑰匙_n 第 12 圖

這些暫存器定義資料移動期間被用於密碼運算之128位元鑰匙

名稱：	DM_密碼_鑰匙_n																位址：				0x08e001n0								被寫入：				右臂							
位元：	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0								
資料：																																	鑰匙							

欄位	列舉	位元指數	說明
鑰匙	鑰匙_0 保持位元 127:96;	31:0	說明資料被移動被用於密碼運算之128位元鑰匙
	鑰匙_1 保持位元 93:64;		
	鑰匙_2 保持位元 63:32;		
	鑰匙_3 保持位元 31:0.		
說明：	當資料被資料移動器移動時，這些暫存器保持被用於密碼運算之128位元鑰匙。其必須於資料移動器被啟動之前被寫入(當密碼運算模式被使用時)		

DM_密碼_MAC 第 13 圖

此暫存器提供被計算媒體存取控制值

名稱：	DM_密碼_MAC																位址：				0x08e00200								被寫入：				右臂							
位元：	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0								
資料：	MAC																																							

欄位	列舉	位元指數	說明
MAC		31:0	f9密碼計算之後明定被計算媒體存取控制值
說明：	此暫存器包含執行f9密碼計算之後之結果		

七、指定代表圖：

(一)本案指定代表圖為：第 (1) 圖。

(二)本代表圖之元件符號簡單說明：

100 方塊圖

115、120 控制器

135、145、140、150、165 暫存器

155、160 多工器

130 密碼引擎

128 資料移動控制器

125 處理器

SMA 共享記憶體架構

SRAM 靜態隨機存取記憶體

SDRAM 同步動態隨機存取記憶體

八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：