申請日期：	P2-9-4	IPC分類	G06F 12/14
申請案號：	P2124489		

(以上各欄由本局填註)

發明專利說明書 200405164

一、發明名稱	中文	擁有加密部的半導體裝置、擁有外部介面的半導體裝置及內容再生方法
	英文	SEMICONDUCTOR DEVICE INCLUDING ENCRYPTION SECTION, SEMICONDUCTOR DEVICE INCLUDING EXTERNAL INTERFACE, AND CONTENT REPRODUCTION METHOD
二、發明人(共7人)	姓名(中文)	1.藤原 睦 2.根本 祐輔 3.安井 純一
	姓名(英文)	1.Fujiwara, Makoto 2.Nemoto, Yusuke 3.Yasui, Junichi
	國籍(中英文)	1.日本 JP 2.日本 JP 3.日本 JP
	住居所(中文)	1.日本國京都府京都市西京區山田平尾町51-50-507 2.日本國兵庫縣神戶市東灘區住吉東町2-1-14 3.日本國大阪府高槻市東五百住町3-23-26
	住居所(英文)	1.51-50-507, Yamada-hirao-cho, Nishikyo-ku, Kyoto-shi, Kyoto JAPAN 2.2-1-14, Sumiyoshi-higashimachi, Higashinada-ku, Kobe-shi, Hyogo JAPAN
三、申請人(共1人)	名稱或姓名(中文)	1.松下電器產業股份有限公司
	名稱或姓名(英文)	1.Matsushita Electric Industrial Co., Ltd.
	國籍(中英文)	1.日本 JP
	住居所(營業所)(中文)	1.〒571-8501日本國大阪府門真市大字門真1006番地 (本地址與前向貴局申請者相同)
	住居所(營業所)(英文)	1.1006, Oaza Kadoma, Kadoma-shi, Osaka 571-8501, Japan
	代表人(中文)	1.中村 邦夫
	代表人(英文)	1.Nakamura, Kunio

027

申請日期：	IPC分類
申請案號：	

（以上各欄由本局填註）

發明專利說明書

一、發明名稱	中 文	
	英 文	
二、發明人（共7人）	姓 名（中文）	4.前田 卓治 5.伊藤 孝幸 6.山田 泰司
	姓 名（英文）	4.Maeda, Takuji 5.Ito, Takayuki 6.Yamada, Yasushi
	國 籍（中英文）	4.日本 JP 5.日本 JP 6.日本 JP
	住居所（中 文）	4.日本國大阪府寢屋川市上神田2-20-1-501 5.日本國大阪府門真市御堂町25-3-213 6.日本國愛知縣稻澤市橫野町590
	住居所（英 文）	4.2-20-1-501, Kamikamida, Neyagawa-shi, Osaka JAPAN 5.25-3-213, Mido-cho, Kadoma-shi, Osaka JAPAN 6.590, Yokono-cho, Inazawa-shi, Aichi JAPAN
三、申請人（共1人）	名稱或姓 名（中文）	
	名稱或姓 名（英文）	
	國 籍（中英文）	
	住居所（營業所）（中 文）	
	住居所（營業所）（英 文）	
	代表人（中文）	
	代表人（英文）	

申請日期：	IPC分類
申請案號：	

(以上各欄由本局填註)

發明專利說明書

一、發明名稱	中 文	
	英 文	
二、發明人(共7人)	姓 名(中文)	7.井上 信治
	姓 名(英文)	7.Inoue, Shinji
	國 籍(中英文)	7.日本 JP
	住居所(中 文)	7.日本國大阪府寢屋川市東香里園町9-13-306
	住居所(英 文)	7.9-13-306, Higashikorien-cho, Neyagawa-shi, Osaka JAPAN
三、申請人(共1人)	名稱或姓 名(中文)	
	名稱或姓 名(英文)	
	國 籍(中英文)	
	住居所(營業所)(中 文)	
	住居所(營業所)(英 文)	
	代表人(中文)	
	代表人(英文)	

一、本案已向

國家(地區)申請專利	申請日期	案號	主張專利法第二十四條第一項優先權
日本 JP	2002/09/04	特願2002-258481	有

二、□主張專利法第二十五條之一第一項優先權:

申請案號:

無

日期:

三、主張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

日期:

四、□有關微生物已寄存於國外:

寄存國家:

寄存機構: 無

寄存日期:

寄存號碼:

□有關微生物已寄存於國內(本局所指定之寄存機構):

寄存機構:

寄存日期: 無

寄存號碼:

□熟習該項技術者易於獲得,不須寄存。

五、發明說明（1）

一、【發明所屬之技術領域】

本發明係屬於提高用於鑰匙（key）安裝系統如LSI之半導體裝置之安全性的技術。

二、【先前技術】

與本案申請人相同的申請人，係在日本國特願（專利申請）2001－286881中，揭露了使鑰匙安裝系統中之鑰匙的機密性和隱匿性較習知技術為高之技術。

但因為所述先前技術係非公開之發明，所述此處無本應記載之習知技術文獻資訊。

三、【發明內容】

發明欲解決之課題

本發明之目的，係在於：提供一種安全性位準很高的半導體裝置，提供一種安全性位準很高的內容再生方法。

解決課題之手段

為解決上述問題，本發明係提供一種半導體裝置，其包括：執行對程式加密及對程式解密中之至少一個的加密部。所述加密部，係擁有加密運算部及加密控制部，加密運算部，其能執行含有對程式進行加密處理及解密處理的複數個順序；加密控制部，其係判斷是否允許執行所述加密運算部能執行的每一個順序，對係判斷為不允許執行的順序，其便禁止所述加密運算部的操作。

五、發明說明（2）

依據本發明，在加密部，對判斷出加密運算部可執行的每一個順序中的不允許執行的順序，便由加密控制部禁止加密運算部的操作。換言之，加密運算部僅執行由加密控制部判斷之允許執行的順序。故可防止順序的不正當執行於未然，提高安全性位準。

於本發明所關係之半導體裝置中，較佳者，係所述複數個順序中含有鑰匙的加密處理及解密處理。

於本發明所關係之半導體裝置中，較佳者，係加密控制部擁有用以儲存模式ID的模式ID儲存暫存器，而且，依據所述模式ID儲存暫存器中所儲存的模式ID的值判斷是否允許執行每一個順序。

於本發明所關係之半導體裝置中，較佳者，係所述加密控制部，擁有對應於所述每一個順序而設且用以儲存其發行次數的暫存器，所述加密控制部除依據所述模式ID的值以外，亦依據儲存於所述暫存器之所述每一個順序的發行次數判斷是否允許執行每一個順序。

再者，較佳者，係本發明所關係之半導體裝置，擁有有不可改寫區域的機密記憶體，所述不可改寫區域中儲存著所述模式ID，所述模式ID儲存暫存器僅在起動該半導體裝置時可寫入，而且起動時，係寫入從所述機密記憶體的所述不可改寫區域讀出的所述模式ID。再者，較佳者，係本發明所關係之半導體裝置擁有儲存引導程式（boot program）的引導ROM，由儲存於所述引導ROM中的引導程式執行將所述模式ID向所述模式ID儲存暫存器中之寫入。

五、發明說明 (3)

再者，較佳者，係擁有儲存表示該半導體裝置是否係第一次起動之安裝模式旗標的機密記憶體，所述加密控制部除依據所述模式ID值以外，亦依據所述安裝模式旗標來判斷是否允許執行每一個順序。

再者，較佳者，係本發明所關係之半導體裝置，擁有儲存與所述複數個順序中之至少一個相對應的引導程式的引導ROM，所述加密運算部，係藉由執行儲存於所述引導ROM中的引導程式執行順序。

再者，較佳者，係本發明所關係之半導體裝置擁有控制手段，藉由其控制使得：不能從該半導體裝置外部存取所述加密運算部及加密控制部所擁有之暫存器。

本發明係關係之另一種半導體裝置，係擁有用以於其和外部記憶體之間進行程式、資料之輸出入的外部介面，所述外部介面，係擁有輸出入程式的程式處理部及輸出入資料的資料處理部；所述程式處理部和資料處理部係構成為相互獨立。

依據本發明，於外部介面，程式處理部和資料處理部係構成為相互獨立。因此，程式遭遇不正當執行之風險便分散了，安全性位準提高。

於本發明所關係之半導體裝置，較佳者，係程式處理部，擁有通過部及程式解密用密碼引擎。該通過部，其係將程式原樣輸出入。該程式解密用密碼引擎，其係接收儲存於所述外部記憶體中之加密程式，將其解密為原始程式（raw(binary)program），再將其供至該半導體裝置內

五、發明說明（4）

部。

再者，較佳者，係所述通過部擁有：執行用通過部和加密用通過部。經由所述執行用通過部所輸入的程式於該半導體裝置中執行，另一方面，經由所述加密用通過部輸入的程式係供向加密部並被加密。

再者，較佳者，係擁有儲存表示所述外部記憶體之各個區域和位址間之對應關係的位址管理資訊的位址段儲存暫存器（address segment storage register），當存取所述外部記憶體而讀入程式之時，參考所述位址管理資訊，決定使所述加密用通過部、所述執行用通過部及所述程式解密用密碼引擎中之哪一個有效。

再者，較佳者，係所述位址段儲存暫存器僅於該半導體裝置起動時可以寫入。

再者，較佳者，係擁有有不可改寫區域的機密記憶體，所述不可改寫區域中儲存著所述位址管理資訊，起動該半導體裝置時，所述位址段儲存暫存器中寫入從所述機密記憶體的所述不可改寫區域讀出的所述位址管理資訊。

再者，較佳者，係擁有含有用以儲存模式ID的模式ID儲存暫存器的模式定序器，亦依據儲存於所述模式ID儲存暫存器之模式ID的值決定使所述加密用通過部、所述執行用通過部及所述程式解密用密碼引擎中之哪一個有效。

再者，較佳者，係所述模式定序器擁有跳線值判斷部，亦依據由所述跳線值判斷部判斷出的跳線值，決定使所述加密用通過部、所述執行用通過部及所述程式解密用

五、發明說明 (5)

密碼引擎中之哪一個有效。

再者，於本發明所關係之半導體裝置，較佳者，係資料處理部擁有：將資料原樣輸出入的通過部及在輸出入資料時進行加密或者解密的資料加密解密用密碼引擎。

為達到上述目的，本發明提供一種內容再生方法，其係包括：將儲存於外部記憶體的不可再生區域之原內容取至LSI的步驟；於所述LSI，使用儲存於內部記憶體之固有ID生成資料固有鑰匙的步驟；於所述LSI，使用所述資料固有鑰匙對所述原內容加密的步驟；將已加密之內容儲存至所述外部記憶體的可再生區域的步驟；將儲存於所述可再生區域之所述已加密之內容取至所述LSI中，利用所述資料固有鑰匙將該已加密之內容解密並再生該已加密之內容的步驟。

依據本發明，儲存於外部記憶體的不可再生區域中的原內容加密，係於LSI中以利用儲存於內部記憶體中的固有ID生成的資料固有鑰匙加密。已加密之內容，係儲存至外部記憶體的可再生區域，再生之時使用資料固有鑰匙將該加密之內容解密。是以，因為以自固有ID生成的資料固有鑰匙加密之內容係儲存於外部記憶體的可再生區域，故再生係不能由無相同的資料固有鑰匙的其他LSI來進行。結果是，可防止內容之不正當執行，提高安全性位準。

於本發明所關係之內容再生方法中，較佳者，係所述原內容為一由資料共有鑰匙加密的內容，在使用所述資料固有鑰匙將所述原內容加密之前，使用儲存於內部記憶體

五、發明說明（6）

之所述資料共有鑰匙將所述原內容解密。

發明之效果

綜上所述，依據本發明，加密運算部僅執行由加密控制部判斷出係為允許執行的順序。因此，可防止順序的不正當執行於未然。在外部介面，程式處理部和資料處理部係構成為相互獨立者。因此，程式遭遇不正當執行的風險便分散了。再者，因為在外部記憶體的可再生區域，儲存著利用由固有ID生成的資料固有鑰匙加密的內容，故不可能由不具有同一個資料固有鑰匙的其他LSI再生此內容。因此，內容的不正當執行係得以防止。結果是安全性位準提高。

四、【實施方式】

發明之實施例

下面，參考附圖，說明本發明的實施例。

圖1為表示本實施例所關係之作為半導體裝置的機密LSI的內部結構的方塊圖。於圖1，機密LSI1係構成為可藉由外部匯流排120與外部記憶體100（快閃記憶體101及RAM102）等連接。而且，係可藉由施加模式ID設定其操作模式。

對本實施例所關係之主要結構要素加以簡單的說明。

首先，機密LSI1，係包括：含不可改寫區域11的機密記憶體（機密Flash）10。該不可改寫區域11中設有不可

五、發明說明（7）

改寫區域寫入旗標12。一旦模式ID寫至機密記憶體10，不可改寫區域寫入旗標12的旗標值便會從"可寫入"變成"已經寫完"，之後便不能向不可改寫區域11寫入了。值得注意的是，於本實施例，機密記憶體10，係由快閃記憶體構成，當然並不限於此，只要係非揮發性記憶體即可。

再者，加密部2，係對程式進行加密、解密的部份，係擁有：作為加密運算部的秘密鑰匙運算處理部20、作為加密控制部的鑰匙生成／更新定序器30、儲存程式加密種（program encryption seed）的儲存部35。秘密鑰匙運算處理部20，其係擁有儲存各種鑰匙等的暫存器，能執行包括程式的加密處理或者解密處理的複數個順序（sequences）。鑰匙生成／更新定序器30，其係判斷是否允許執行秘密鑰匙運算處理部20可執行的各種順序，針對已經判斷出為不允許執行的順序，便令秘密鑰匙運算處理部20停止操作。鑰匙生成／更新定序器30，其係擁有模式ID儲存暫存器31，依據儲存於該模式ID儲存暫存器31之模式ID的值，判斷是否允許執行每一個順序。鑰匙生成／更新定序器30，其係亦擁有：儲存表示鑰匙或者程式由何種算法、鑰匙長加密之加密種類識別符（encryption type identifier）的加密種類識別符儲存暫存器32。加密部2的結構和操作之詳情後述。

模式定序器40，其係亦擁有模式ID儲存暫存器41。該模式定序器40，係依據儲存於模式ID儲存暫存器41之模式ID和跳線器43的值控制外部主介面（I／F）50的操作，換

五、發明說明 (8)

言之，係控制藉由哪一個主介面以將儲存於外部記憶體100之程式、資料讀入。由此可控制是否可執行儲存於外部記憶體100之原始程式。模式定序器40還擁有：儲存了表示用什麼方法將鑰匙加密的加密種類識別符的加密種類識別符儲存暫存器42。

外部主介面50，在模式定序器40的控制下，藉由程式處理部51所擁有的通過部52和程式解密用密碼引擎53、資料處理部55所擁有的通過部56及資料加密／解密用密碼引擎58中之任一個，在它和外部記憶體100之間進行程式、資料的輸出入。

此處，除後述的管理模式及應用程式開發模式以外，經由通過部52輸入的程式係不於機密LSI1內部執行。換言之，通過部52，係在原始程式的加密、或者用其他的鑰匙對已經加密之程式再次加密時有效。機密LSI1係構成為，除了後述的管理模式及應用程式開發模式以外，不使操作移向經由通過部52輸入的程式。因此，即使例如已經成為商品的機密LSI1經由通過部52取入了原始程式，亦不能執行該原始程式。

引導ROM60，係儲存控制機密LSI1的起動操作的引導程式。HASH運算部70，係為驗證讀至機密LSI1之程式的正當性而計算HASH值。

再者，在外部記憶體100，程式係儲存於快閃記憶體101中；資料（內容）係儲存於RAM102中。外部工具110中儲存著一開始起動機密LSI1時儲存於機密記憶體10的各種

五、發明說明（9）

初始值。該初始值的種類隨著所設定的操作模式而異。

圖2係為顯示使用了圖1中的機密LSI1的開發及產品化的整個流程的圖。如圖2所示，機密LSI1，係在管理模式（模式ID: 00）、鑰匙生成模式（模式ID: 01）、開發模式（模式ID: 10）及商品操作模式（模式ID: 11）這4種操作模式下操作。

首先，被設定為管理模式的機密LSI1，係作為管理者用LSI操作。在管理者用LSI，係開發鑰匙生成程式（PA1），而且，係使用任意的鑰匙生成鑰匙對該鑰匙生成程式加密（PA2）。

被設定為鑰匙生成模式的機密LSI1，係作為鑰匙生成用LSI操作，在鑰匙生成用LSI，係安裝在管理者用LSI中生成、加密的鑰匙生成程式（PB1）。藉由執行該鑰匙生成程式，便生成了各種鑰匙（PB2）。

被設定為開發模式的機密LSI1，係作為開發用LSI操作，在開發用LSI，係開發在實際的產品中執行的應用程式（PC1）。而且，係使用程式共有鑰匙對該應用程式加密（PC2）。

被設定為商品操作模式的機密LSI1，係作為實際的商品LSI操作。在商品LSI，係安裝在開發用LSI中生成的由程式共有鑰匙加密的應用程式，在其內部，用程式固有鑰匙將所安裝的應用程式變換成加密之應用程式（PD1）。在一般的商品操作下執行由程式固有鑰匙加密之應用程式。值得注意的是，在開發用LSI中亦可為調試應用程式

五、發明說明（10）

（PC4）執行該變換處理（PC3）。

機密LSI1，係藉由執行儲存於引導ROM60之引導程式而進行以下操作。

圖3為顯示引導程式的整個處理過程的流程圖。給機密LSI1通上電以後，便由CPU65執行儲存於引導ROM60之引導程式。如圖3所示，首先，將每一個硬體初始化（SZ0）。然後，從外部工具110讀入各種初始值，並將該讀入的初始值設定在機密記憶體10（SZ1）。

圖4為初始值設定處理SZ1的流程圖。首先，在跳線器44，判斷機密記憶體10是否已安裝在LSI內（SZ11）。接著，判斷不可改寫區域寫入旗標12是否為"已寫完"（SZ12），因為當為"已寫完"（SZ12為"是"）時，初始值便已設定在機密記憶體10，故結束處理SZ1。當不可改寫區域寫入旗標12為"可寫入"（SZ12為"否"）時，便將初始值寫至機密記憶體10。不僅將模式ID寫至機密記憶體10的不可改寫區域11，亦將加密的程式固有鑰匙、位址管理資訊、資料固有鑰匙寫至機密記憶體10的不可改寫區域11（SZ13、SZ16～SZ18）。值得注意的是，於開始的判斷結果為機密記憶體10在LSI的外部之時（SZ14為"否"），便將模式ID寫在表示商品操作模式的值上（SZ15）。是以，如機密記憶體10在LSI包外般之產品，便係只可在商品操作模式下操作。

接著，將不可改寫區域寫入旗標12設定為"已寫完"（SZ19）。是以，以後的不可改寫區域11便不能再改寫

五、發明說明（11）

了。而且，亦將加密種類識別符及安裝模式旗標寫至一般區域13、14（SZ1A）。而且，當模式ID顯示管理模式以外的模式之時（SZ1B為"否"），除了將已加密之種類識別符及安裝模式旗標寫至一般區域13、14以外，亦將已加密之共有鑰匙／鑰匙生成鑰匙寫至一般區域13、14（SZ1C）。

之後，回至圖3，執行前處理SZ2。此處，設定在機密記憶體10的不可改寫區域11之模式ID，係設定於鑰匙生成／更新定序器30的模式ID儲存暫存器31及模式定序器40的模式ID儲存暫存器41中；設定在機密記憶體10的第1一般區域13之加密種類識別符，係設定於鑰匙生成／更新定序器30的加密種類識別符儲存暫存器32及模式定序器40的加密種類識別符儲存暫存器42中；機密記憶體10的不可改寫區域11中所儲存的位址管理資訊，係設定在MEMC80的位址段儲存暫存器81中。至此處為止的操作，係與圖2之初始值設定階段PA0、PB0、PC0、PD0相對應。

之後，依據模式ID的值進行每一個模式下的操作（SZ3）。

當模式ID為"00"時，機密LSI1成為管理模式，係依據跳線器43的值（SA0）執行原始程式執行處理SA1或程式加密處理SA2。在鑰匙生成程式開發階段PA1，係進行原始程式執行處理SA1，生成鑰匙生成程式。該鑰匙生成程式儲存於外部記憶體100中。在鑰匙生成程式加密階段PA2，係由任意的鑰匙生成鑰匙對鑰匙生成程式加密。

當模式ID為"01"時，機密LSI1成為鑰匙生成模式，依

五、發明說明（12）

據安裝模式旗標的值（SB0）執行鑰匙生成器製造處理SB1或者是鑰匙管理／發行處理SB2。在鑰匙生成器製造階段PB1，係執行鑰匙生成器製造處理SB1，用程式固有鑰匙對由任意的鑰匙生成鑰匙加密的鑰匙生成程式再次加密。在鑰匙管理／發行階段PB2，係藉由執行由程式固有鑰匙加密之鑰匙生成程式，即可執行鑰匙管理／發行處理SB2，而生成鑰匙。

當模式ID為"10"時，機密LSI1成為開發模式，係依據跳線器43的值（SC0）來執行程式加密處理SC1、原始程式執行處理SC2、程式安裝處理SC3或者加密程式執行處理SC4。在應用程式開發階段PC1，係執行原始程式執行處理SC2，開發出應用程式。所開發的應用程式儲存於外部記憶體100中。在應用程式加密階段PC2，係執行程式加密處理SC1。在應用程式安裝階段PC3，係執行程式安裝處理SC3；在應用程式調試階段PC4，係執行加密程式執行處理SC4。SC3、SC4這些處理和商品操作模式之各個處理SD1、SD相同。

當模式ID為"11"時，機密LSI1成為商品操作模式，依據安裝模式旗標的值（SD0）來執行程式安裝處理SD1或者一般引導處理SD2。在商品安裝階段PD1，係執行程式安裝處理SD1。在商品操作階段PD2，係執行一般引導處理SD2。

圖5為顯示加密部2及其周邊部的結構的圖。如圖5所示，鑰匙生成／更新定序器30，其除具有模式ID儲存暫存

五、發明說明（13）

器31及加密種類識別符儲存暫存器32以外，亦擁有暫存器33及控制部34。該暫存器33，係對應於利用秘密運算處理部20執行的每一個順序而設、用於儲存其發行次數，該控制部34，係參考記憶體31、33，判斷是否可以執行各個順序（是否可以執行引導ROM60之每一個程式及外部程式），而控制秘密鑰匙運算處理部20的操作。於機密LSI1，每一個順序每發行一次，與之對應的記憶體33便加1。

程式加密種35，係為在對鑰匙解密時或者生成鑰匙時所用的種，包括共有鑰匙用和固有鑰匙用種。

在上述商品操作模式、開發模式，由控制部34施加制約，使得：將儲存於機密記憶體10之值設定在加密部2之每一個暫存器中的順序（機密Flash載入器(loader)）、生成鑰匙及對鑰匙解密的順序（鑰匙定序器）分別只能發行一次。例如，若起動機密LSI時，由引導程式先將儲存於機密記憶體之模式ID儲存至模式ID儲存暫存器31中，便再也不能對模式ID進行改寫了。再者，若在起動機密LSI時，對共有鑰匙和固有鑰匙解密，並將其儲存至秘密秘鑰運算處理部20內部的暫存器中，便再也不能生成鑰匙，亦不能對鑰匙解密了。因此，即使外部記憶體100中安裝了鑰匙生成程式，亦不能生成鑰匙。曾經解密之固有鑰匙，係儲存於外部介面50內的固有鑰匙儲存暫存器中，加密程式係用該固有鑰匙執行。程式之更新，係使用儲存於秘密秘鑰運算處理部20內部的暫存器之共有鑰匙、固有鑰匙執行。

五、發明說明（14）

值得注意的是，在上述鑰匙生成模式、管理模式中，因為解除了對鑰匙定序器的限制，故能夠生成鑰匙。

此處，可設置對應於程式加密種而設、儲存其使用次數的程式加密種使用次數儲存暫存器，以代替順序發行次數儲存暫存器33。因為在生成鑰匙及對鑰匙解密之時使用程式加密種，故例如只要用模式ID限制其使用次數，即使計數程式加密種的使用次數，亦能限制鑰匙的生成及對鑰匙的解密。

再者，程式加密種並不一定非要包括共有鑰匙用及固有鑰匙用種。

圖6為顯示共用匯流排及私用匯流排之設定方法的圖。此處，"私用匯流排"係指不能從外部存取（外部存取）的匯流排；外部介面50物理上也並非一定要獨立。換言之，作為接在私用匯流排91而設定之暫存器等，不能經由外部存取進行讀出和寫入。

位址，係分別施加給機密LSI1內部的暫存器等，共用匯流排位址儲存部82，係儲存位址中接在共用匯流排92上的暫存器等的位址（在圖6中，為"0X00000"～"0X10000"）。當有外部存取時，外部存取位址判斷部83，係參考共用匯流排位址儲存部82判斷是否要存取共用匯流排92，若如此便接收它。另一方面，因外部存取不是對共用匯流排92的存取時，意味著係對私用匯流排91的存取，故存取遭拒絕。

值得注意的是，於係來自CPU65的存取（內部存取）

五、發明說明（15）

之時，係不進行如此判斷，接收內部存取。

圖7為顯示外部介面50及其周邊的結構的圖。在圖7中，位址段儲存暫存器81，係儲存表示外部記憶體100之各個區域和位址的對應關係的位址管理資訊。此處，外部記憶體100，係分為：第1區域（設定範圍內的程式）、第2區域（設定範圍外的程式）、第3區域（設定區域內的資料）及第4區域（設定範圍外的資料）這四個區域，儲存各自的位址。

比較器85，其係參考儲存於位址段儲存暫存器81之位址管理資訊，判斷要輸入輸出的資訊的位址屬於上述第1～第4區域之哪一個區域，並將該判斷結果送至輸出入控制信號生成部84。

輸出入控制信號生成部84，其係依據從模式定序器40輸出的模式ID及跳線器判斷結果以及比較器85的輸出等，判斷使外部介面50所擁有的哪一個介面有效，並將該判斷結果作為輸出入控制信號送至外部輸出入模式控制部54。外部輸出入模式控制部54，係依據所接收的輸出入控制信號使某一個介面有效。值得注意的是，當模式ID顯示商品操作模式時，一定不使執行通過部52有效。是以，便受到控制而不執行儲存於外部記憶體100之原始程式。

在調試管理模式及開發模式之時，經由程式處理部51的執行用通過部52b讀入儲存於第1區域的程式；除了鑰匙生成模式、商品操作模式或者開發模式調試以外的其他時候，經由程式解碼用密碼引擎53讀入儲存於第1區域的程

五、發明說明（16）

式，這些程式可執行。另一方面，經由程式處理部51的加密用通過部52a讀入儲存於第2區域的程式，供給至加密部2加密或者是再加密，這些程式不可執行。

經由資料處理部55的資料加密解密用密碼引擎58讀入儲存於第3區域的資料；經由資料處理部55的通過部56讀入儲存於第4區域的資料。

經由加密用通過部52a取入的程式，係於加密部2的秘密秘鑰運算處理20中加密或者再次加密，之後又係經由加密用通過部52a讀至外部記憶體100的第1區域中。是以，以後便成為可執行的程式。

值得注意的是，資料係經由私用匯流排設定於位址段儲存暫存器81及模式ID儲存暫存器41。換言之，資料係藉由來自內部的存取設定者。再者，該資料設定係於機密LSI1重新設定後，僅執行一次。

圖8為顯示外部介面50的操作的圖。假設係一個商品操作模式。如圖8所示，安裝前，由共有鑰匙加密之應用程式，係儲存於外部記憶體100的第2區域（設定範圍外），因此這種狀態係不能執行。換言之，儲存於第2區域、由共有鑰匙加密的應用程式，係安裝時經由加密用通過部52a取至機密LSI1，該應用程式由共有鑰匙解密後，又由固有鑰匙再次加密，再次經由加密用通過部52a儲存至外部記憶體100的第1區域（設定範圍內）。於是，儲存於該第1區域、由固有鑰匙加密的應用程式，係經由程式解密用密碼引擎53取至機密LSI1內部，並係於機密LSI1內

五、發明說明 (17)

部執行。

值得注意的是，在開發模式執行以下操作。首先，調試時，將想要執行的程式事先寫至第1區域（設定區域內）中準備好。藉此，即使係原始程式，亦能經由執行用通過部52b取入並得以執行。加密時，係將想加密之程式事先寫至第2區域（設定範圍外）中準備好。藉此，若起動機密LSI1，便執行加密的順序，由共有鑰匙加密並儲存至外部記憶體100。安裝調試程式時，將要再次加密之程式事先寫至第2區域（設定範圍外）中準備好。而且，在調試已加密的程式時，係將已調試之加密程式事先寫至第1區域（設定範圍內）中準備好。藉此便解密、執行。

圖9為顯示機密記憶體10之存取控制的圖。如圖9所示，存取控制部95，係擁有：儲存不可改寫區域11之位址的暫存器96、儲存不可改寫區域寫入旗標12的位址的暫存器97以及可寫入／不可寫入判斷部98。暫存器96、97係構成為：資料一旦寫至暫存器96、97，便可藉由旗標管理等禁止進一步寫入。

存取控制如下所述。從CPU65至機密記憶體10的存取，係一定要經由存取控制部95執行。在指令（command）為"讀"之時，不管要存取的位址係不可改寫區域還是係一般區域的位址，機密記憶體10之資料係皆輸出至私用匯流排91中。另一方面，當指令為"寫"之時，可寫入／不可寫入判斷部98，係參考儲存地的位址、儲存於暫存器96的位址以及不可改寫區域寫入旗標12的值，判斷是否寫入。

五、發明說明（18）

具體而言，判斷係如下所述。

（旗標"已寫完"且不可寫入區域）・・・　不可寫入

（旗標"已寫完"且一般區域）　・・・　可寫入

（旗標"未寫入"且不可寫入區域）・・・　可寫入

（旗標"未寫入"且一般區域）　・・・　可寫入

值得注意的是，亦為機密記憶體10準備了"區域消去"、"晶片消去"等指令。於不可改寫區域11旗標12為"已寫完"時，一般區域接收"區域消去"，而不可寫入區域卻不接收。又，不接收"晶片消去"。

再者，在再生內容（資料）之時，採用以下方法係能提高安全性。

資料一開始放在外部RAM102的第4區域（設定範圍外），於資料係放在第4區域之時，資料或是處於由資料共有鑰匙（和程式共有鑰匙不同）加密的狀態或是處於明文狀態。因此便有由其他LSI不正當利用的可能性，而存在安全性問題。

為解決這一問題，對於特別想防止被不正當利用的影響、音樂等內容而言，係作成再生內容的程式，以便只能再生儲存於外部RAM102的第3區域（設定範圍內）的內容。將放在第3區域內的資料取至機密LSI1之時，該資料係於資料加密解密用密碼引擎58中解密。因為進行此解密時所使用之資料固有鑰匙，係由固有ID和隨機數組成，所以該資料固有鑰匙不僅隨機密LSI1之不同而異，而且每起動一次該資料固有鑰匙亦不同。因此，資料不易被不正當

利用，安全性亦提高。值得注意的是，因為再生內容的程式亦由固有鑰匙加密，故很難被竄改。

圖10及圖11為商品操作模式下一般引導處理的資料流程圖。在圖10，首先，係將儲存於機密記憶體10的不可改寫區域11中且加密之程式固有鑰匙Enc（程式固有鑰匙，MK0）、Enc（MK0，CK）設定在秘密鑰匙運算處理部20的加密鑰匙儲存暫存器中。用所安裝之程式加密種對該已加密之程式固有鑰匙解密而獲得程式固有鑰匙。所獲得之程式固有鑰匙，係設定在外部主介面50的程式解密用密碼引擎53的程式固有鑰匙儲存暫存器中。之後，係將儲存於機密記憶體10的不可改寫區域11的資料固有ID設定在秘密鑰匙運算處理部20的固有ID儲存暫存器中。係由CPU65產生隨機數，並將該隨機數設定在秘密鑰匙運算處理部20的隨機數儲存暫存器中。係由秘密鑰匙運算處理部20從資料固有ID和隨機數生成資料固有的資料加密解密用密碼引擎58的資料固有鑰匙儲存暫存器中。

之後，在圖11，係經由外部主介面50所擁有之程式處理部51的程式解密用密碼引擎53，對儲存於外部記憶體100中且由程式固有鑰匙加密之應用程式Enc（應用程式，程式固有鑰匙）解密並將其取至HASH運算部70中，計算HASH值。接著，對該已計算之HASH值和儲存於機密記憶體10之一般區域13的HASH值加以比較，檢查應用程式是否被竄改。當HASH值一致時，處理將移至儲存於外部記憶體100的應用程式Enc（應用程式，程式固有鑰匙），執行應

五、發明說明（20）

用。值得注意的是，當HASH值不一致時，便推測係有不正當行為，而執行不正當存取控制處理。

由CPU65執行應用程式。換言之，因為由機密LSI1內部的CPU65作為主體（master）進行存取控制，故外部存取位址判斷部83便和以後的操作即內部存取無關。藉著應用程式，由資料共有鑰匙加密的內容（原內容）係從外部RAM102的第4區域（不可再生區域）取至機密LSI1中。係於秘密秘鑰運算處理部20中利用已寫至機密記憶體10的資料共有鑰匙將所取入之內容解密。之後，再利用資料固有鑰匙經由外部介面50的資料處理部55的資料加密解密用密碼引擎58對所取入之內容加密，並寫至外部RAM102的第3區域（可再生區域）。之後，由該資料固有鑰匙加密之內容便可再生。再生時，係以資料固有鑰匙經由外部介面50的資料處理部55之資料加密解密用密碼引擎58解密。

圖式簡單說明

五、【圖式簡單說明】

圖1為顯示本發明的實施例所關係之作為半導體裝置的機密LSI的結構的方塊圖。

圖2為顯示使用了圖1的機密LSI的開發及產品化的整個流程的圖。

圖3為顯示引導程式的整個處理流程的流程圖。

圖4為初始值設定處理SZ1的流程圖。

圖5為顯示圖1中的機密LSI1之加密部及其周邊的結構的圖。

圖6為顯示圖1中的機密LSI1之共用匯流排與私用匯流排的設定方法的圖。

圖7為顯示圖1中的機密LSI1之外部主介面與其周邊的結構的圖。

圖8為顯示商品操作模式中外部主介面的操作的圖。

圖9為顯示機密記憶體的存取控制的圖。

圖10為商品操作模式之一般引導程式的一個資料流。

圖11為商品操作模式之一般引導程式的又一個資料流。

元件符號說明：

1　機密LSI（半導體裝置）

2　加密部

10　機密記憶體

20　秘密鑰匙運算處理部（加密運算部）

圖式簡單說明

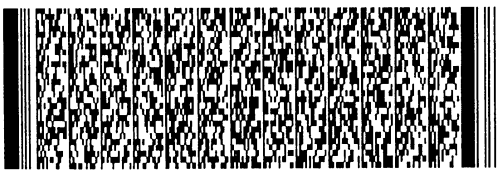
30 鑰匙生成／更新定序器（加密控制部）
31 模式ID儲存暫存器
33 順序發行次數儲存暫存器
35 儲存部
40 模式定序器
41 模式ID儲存暫存器
45 跳線值判斷部
50 外部介面
51 程式處理部
52 通過部
52a 執行用通過部
52b 加密用通過部
53 程式加解密用密碼引擎
55 資料處理部
56 通過部
58 資料加密／解密用密碼引擎
60 引導ROM
81 位址段儲存暫存器
82 共用匯流排位址儲存部
83 外部存取位址判斷部
100 外部記憶體

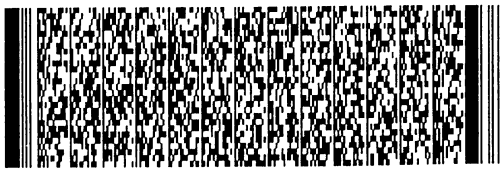
四、中文發明摘要　（發明名稱：擁有加密部的半導體裝置、擁有外部介面的半導體裝置及內容再生方法）

本發明旨在提供一種安全性位準很高的半導體裝置。機密LSI1，係擁有：對程式加密的加密部2以及用以在它和外部記憶體100之間輸出入程式、資料的外部介面50。在加密部2，針對由鑰匙生成／更新定序器30判斷出的不允許執行的順序，係禁止秘密秘鑰運算處理20的操作。

五、英文發明摘要　（發明名稱：SEMICONDUCTOR DEVICE INCLUDING ENCRYPTION SECTION, SEMICONDUCTOR DEVICE INCLUDING EXTERNAL INTERFACE, AND CONTENT REPRODUCTION METHOD）

A secure LSI device 1 includes an encryption section 2 for encrypting a program, and an external I/F 50 for inputting/outputting a program or data from/to an external memory 100. In the encryption section 2, the operation of a private key arithmetic processing section 20 is prohibited with respect to a sequence whose execution is determined by a key-generation/update sequencer 30





四、中文發明摘要　（發明名稱：擁有加密部的半導體裝置、擁有外部介面的半導體裝置及內容再生方法）

五、英文發明摘要　（發明名稱：SEMICONDUCTOR DEVICE INCLUDING ENCRYPTION SECTION, SEMICONDUCTOR DEVICE INCLUDING EXTERNAL INTERFACE, AND CONTENT REPRODUCTION METHOD）

to be impermissible. In the external I/F 50, a program processing section 51 and a data processing section 55 are structured independently from each other.

六、申請專利範圍

1. 一種半導體裝置，其特徵係在於：

係包括：執行對程式加密及對程式解密中之至少一個的加密部，

所述加密部，係擁有加密運算部，其係能執行含有對程式進行加密處理及解密處理的複數個順序；以及加密控制部，其係判斷是否允許執行所述加密運算部能執行的每一個順序，對判斷為不允許執行的順序，便禁止所述加密運算部的操作。

2. 如申請專利範圍1所述之半導體裝置，其中：

所述複數個順序，係含有鑰匙的加密處理及解密處理。

3. 如申請專利範圍1所述之半導體裝置，其中：

所述加密控制部，係擁有用以儲存模式ID的模式ID儲存暫存器，而且，所述加密控制部，係依據所述模式ID儲存暫存器中所儲存的模式ID的值判斷是否允許執行每一個順序。

4. 如申請專利範圍3所述之半導體裝置，其中：

所述加密控制部，係擁有：對應於所述每一個順序而設且用以儲存其發行次數的暫存器；

所述加密控制部，係除了依據所述模式ID的值判斷是否允許執行每一個順序以外，亦依據儲存於所述暫存器之

六、申請專利範圍

所述每一個順序的發行次數判斷是否允許執行每一個順序。

5. 如申請專利範圍3所述之半導體裝置，其中：

係擁有有不可改寫區域的機密記憶體，所述不可改寫區域中儲存著所述模式ID；

所述模式ID儲存暫存器，係僅於起動該半導體裝置時可寫入，而且起動時係寫入自所述機密記憶體的所述不可改寫區域讀出的所述模式ID。

6. 如申請專利範圍5所述之半導體裝置，其中：

係擁有儲存引導程式的引導ROM；

將所述模式ID寫至所述模式ID儲存暫存器之操作，係由儲存於所述引導ROM之引導程式執行。

7. 如申請專利範圍3所述之半導體裝置，其中：

係擁有儲存表示該半導體裝置是否係第一次起動的安裝模式旗標的機密記憶體；

所述加密控制部，係除依據所述模式ID值以外，亦依據所述安裝模式旗標以判斷是否允許執行每一個順序。

8. 如申請專利範圍1所述之半導體裝置，其中：

係擁有儲存與所述複數個順序之至少一個順序相對應的引導程式的引導ROM；

六、申請專利範圍

所述加密運算部，係藉由執行儲存於所述引導ROM之引導程式執行順序。

9. 如申請專利範圍1所述之半導體裝置，其中：

係擁有控制手段，使得：不能從該半導體裝置外部存取所述加密運算部及加密控制部所擁有的暫存器。

10. 一種半導體裝置，其特徵係在於：

於該半導體裝置和外部記憶體之間，係擁有用以進行程式、資料的輸出入的外部介面；

所述外部介面，係擁有：輸出入程式的程式處理部及輸出入資料的資料處理部；

所述程式處理部和所述資料處理部，係構成為相互獨立。

11. 如申請專利範圍10所述之半導體裝置，其中：

所述程式處理部，係擁有：將程式原樣輸出入的通過部；以及程式解密用密碼引擎，其係接收儲存於所述外部記憶體的加密之程式，將其解密為原始程式，再供向該半導體裝置內部。

12. 如申請專利範圍11所述之半導體裝置，其中：

所述通過部，係擁有：執行用通過部和加密用通過部；

六、申請專利範圍

經由所述執行用通過部輸入的程式，係於該半導體裝置中執行，另一方面，經由所述加密用通過部輸入的程式係供向加密部並被加密。

13. 如申請專利範圍12所述之半導體裝置，其中：

係擁有儲存表示所述外部記憶體之各個區域和位址間之對應關係的位址管理資訊的位址段儲存暫存器；

當存取所述外部記憶體而讀入程式之時，係參考所述位址管理資訊，決定使所述加密用通過部、所述執行用通過部及所述程式解密用密碼引擎中之哪一個有效。

14. 如申請專利範圍13所述之半導體裝置，其中：

所述位址段儲存暫存器，係僅於該半導體裝置起動時可以寫入。

15. 如申請專利範圍14所述之半導體裝置，其中：

係擁有有不可改寫區域的機密記憶體，所述不可改寫區域中儲存著所述位址管理資訊；

所述位址段儲存暫存器，係於起動該半導體裝置時，寫入從所述機密記憶體的所述不可改寫區域讀出的所述位址管理資訊。

16. 如申請專利範圍13所述之半導體裝置，其中：

係擁有具有用以儲存模式ID的模式ID儲存暫存器的模

六、申請專利範圍

式定序器；

另外亦依據儲存於所述模式ID儲存暫存器之模式ID的值決定使所述加密用通過部、所述執行用通過部及所述程式解密用密碼引擎中之哪一個有效。

17. 如申請專利範圍16所述之半導體裝置，其中：

所述模式定序器，係擁有跳線值判斷部；

另外亦依據由所述跳線值判斷部判斷出的跳線值，決定使所述加密用通過部、所述執行用通過部及所述程式解密用密碼引擎中之哪一個有效。

18. 如申請專利範圍10所述之半導體裝置，其中：

所述資料處理部，係擁有：將資料原樣輸出入的通過部及在輸出入資料時進行加密或者解密的資料加密解密用密碼引擎。

19. 一種內容再生方法，其特徵係在於：

包括：

將儲存於外部記憶體的不可再生區域之原內容取至LSI中的步驟；

在所述LSI，使用儲存於內部記憶體之固有ID生成資料固有鑰匙的步驟；

在所述LSI，使用所述資料固有鑰匙對所述原內容加密的步驟；

六、申請專利範圍

將已加密之內容儲存至所述外部記憶體的可再生區域中的步驟；

將儲存於所述可再生區域之所述已加密之內容取至所述LSI中，利用所述資料固有鑰匙將該已加密之內容解密並再生該已加密之內容的步驟。

20. 如申請專利範圍19所述之內容再生方法，其中：

儲存於不可再生區域之所述原內容，係為一由資料共有鑰匙加密的內容；

在使用所述資料固有鑰匙將所述原內容加密之前，使用儲存於內部記憶體之所述資料共有鑰匙將所述原內容解密。

弍圖

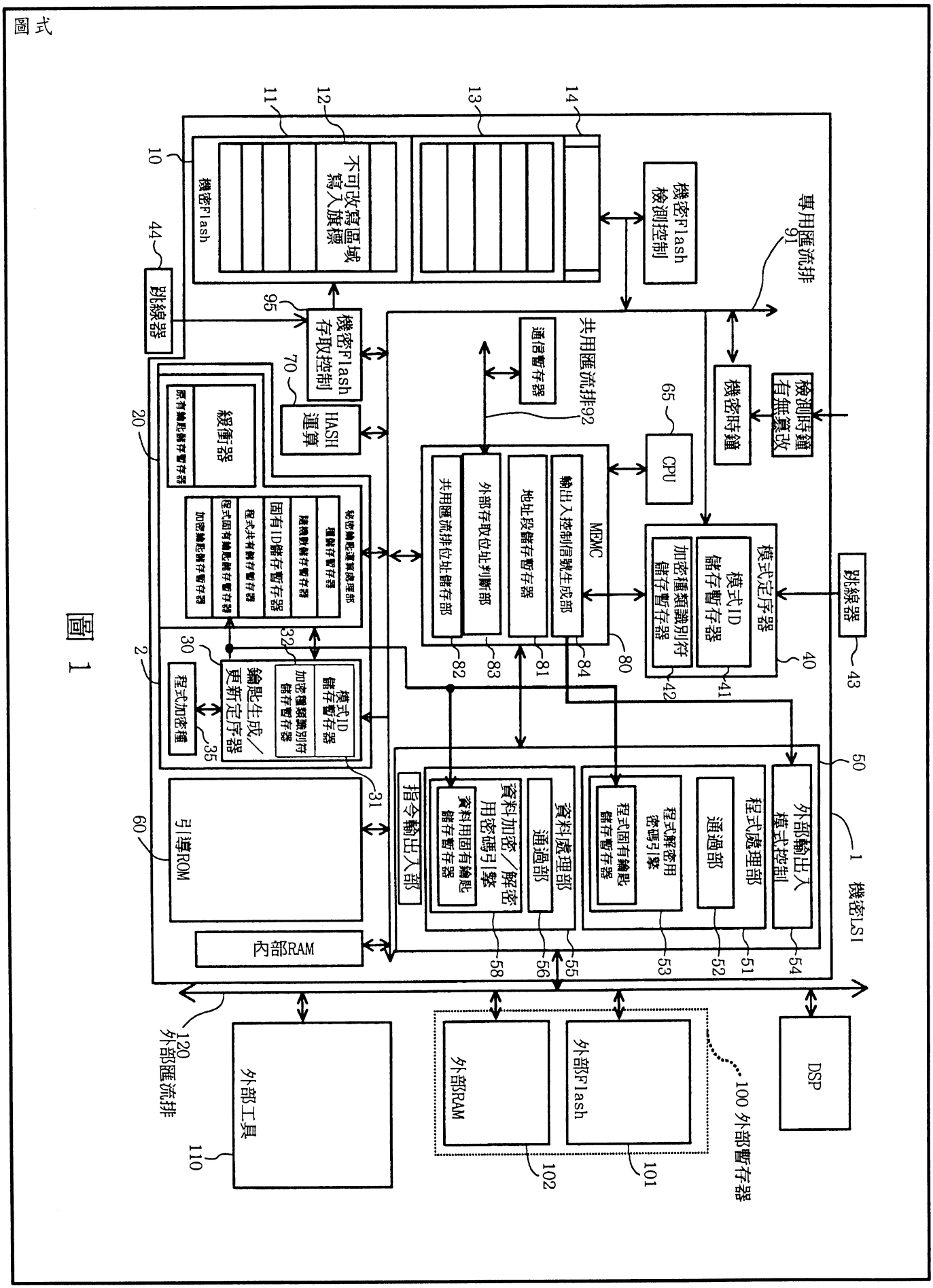
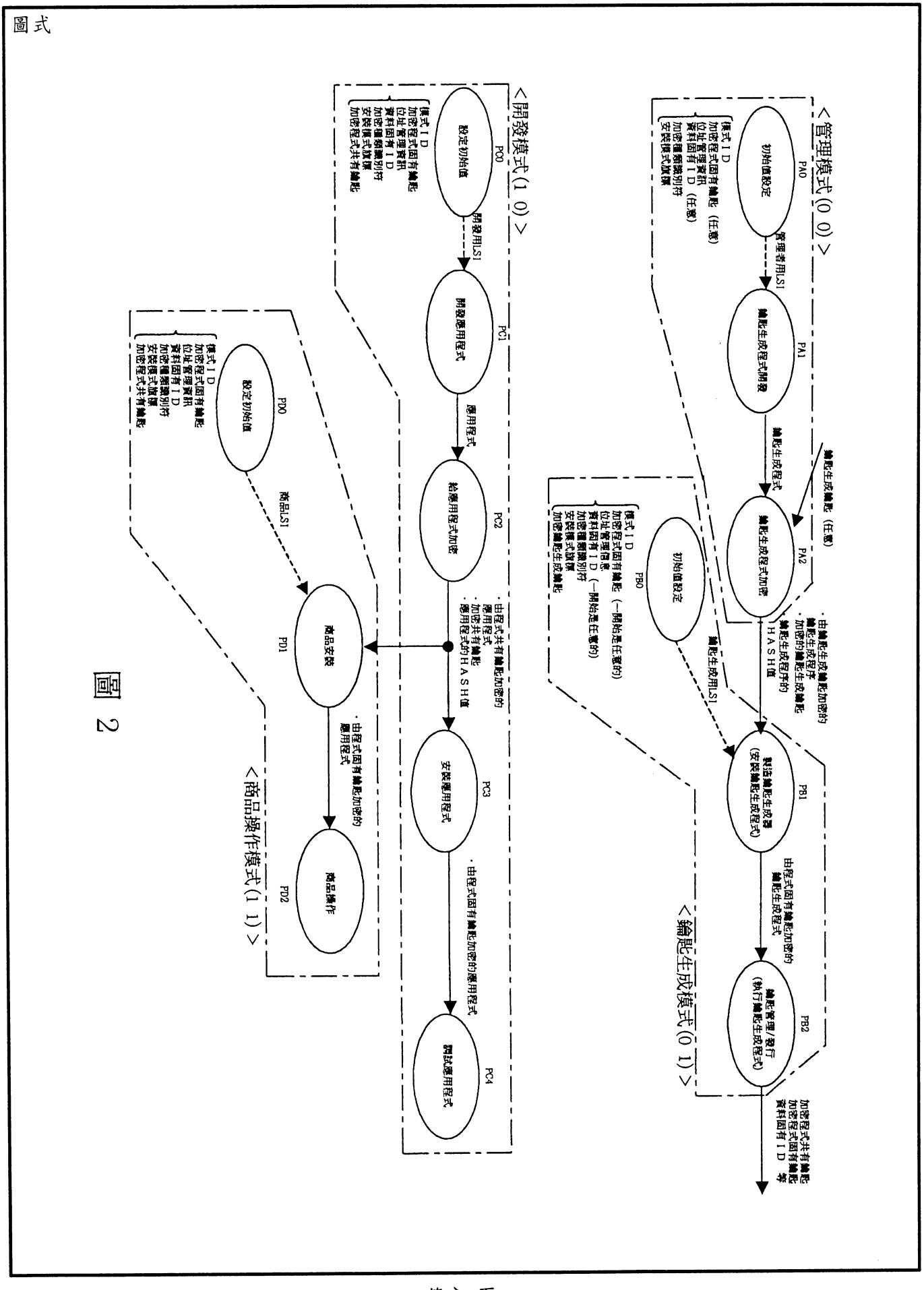

機密LSI
1
外部輸出入模式控制
54
程式處理部
51
通過部
52
程式解密用密碼引擎
53
程式固有鑰匙儲存暫存器
資料處理部
55
通過部
56
資料加密／解密用密碼引擎
58
資料用固有鑰匙儲存暫存器
指令輸出入部
內部RAM
引導ROM
60
31
模式ID儲存暫存器
加密種類識別符儲存暫存器
鑰匙生成／更新定序器
32
30
程式加密種
35
2
緩衝器
原有鑰匙儲存暫存器
20
HASH運算
70
機密Flash存取控制
95
跳線器
44
機密Flash
不可改寫區域寫入旗標
10
11
12
13
14
機密Flash檢測控制
專用匯流排
91
共用匯流排92
通信暫存器
CPU
65
MEMC
輸出入控制信號生成部
84
地址段儲存暫存器
81
外部存取位址判斷部
83
共用匯流排位址儲存部
82
80
模式定序器
40
模式ID儲存暫存器
41
加密種類識別符儲存暫存器
42
跳線器
43
機密時鐘
檢測時鐘有無竄改
DSP
外部Flash
101
外部RAM
102
100 外部暫存器
外部工具
110
120
外部匯流排

圖 1

圖式


<管理模式(0 0)>
PA0
初始值設定
管理者用LSI
PA1
鑰匙生成程式開發
鑰匙生成程式
PA2
鑰匙生成程式加密
鑰匙生成用LSI
PB0
初始值設定
PB1
製造鑰匙生成器
(安裝鑰匙生成程式)
由程式固有鑰匙加密的
鑰匙生成程式
PB2
鑰匙管理/發行
(執行鑰匙生成程式)
<鑰匙生成模式(0 1)>
<開發模式(1 0)>
PC0
設定初始值
開發用LSI
PC1
開發應用程式
應用程式
PC2
給應用程式加密
PC3
安裝應用程式
PC4
調試應用程式
PD0
設定初始值
商品LSI
PD1
商品安裝
PD2
商品操作
<商品操作模式(1 1)>
圖 2

圖式

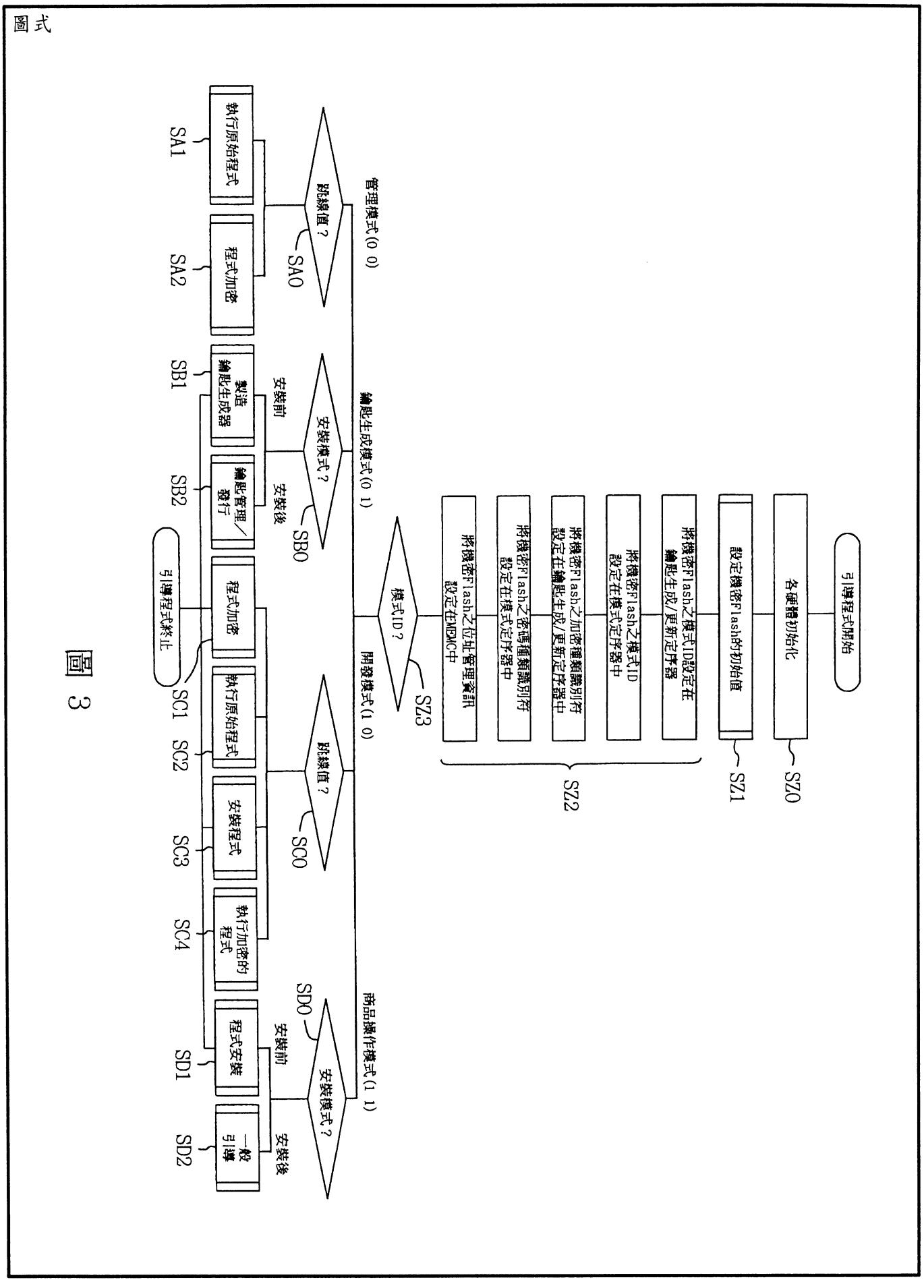

引導程式開始
各硬體初始化
SZ0
設定機密Flash的初始值
SZ1
將機密Flash之模式ID設定在
鑰匙生成/更新定序器
將機密Flash之模式ID
設定在模式定序器中
將機密Flash之加密種類識別符
設定在鑰匙生成/更新定序器中
將機密Flash之密碼種類識別符
設定在模式定序器中
將機密Flash之位址管理資訊
設定在MDMC中
SZ2
模式ID？
SZ3
管理模式(0 0)
鑰匙生成模式(0 1)
開發模式(1 0)
商品操作模式(1 1)
跳線值？
SA0
安裝模式？
SB0
跳線值？
SC0
安裝模式？
SD0
安裝前
安裝後
執行原始程式
SA1
程式加密
SA2
製造
鑰匙生成器
SB1
鑰匙管理/
發行
SB2
程式加密
SC1
執行原始程式
SC2
安裝程式
SC3
執行加密的
程式
SC4
程式安裝
SD1
一般
引導
SD2
引導程式終止

圖 3

圖式

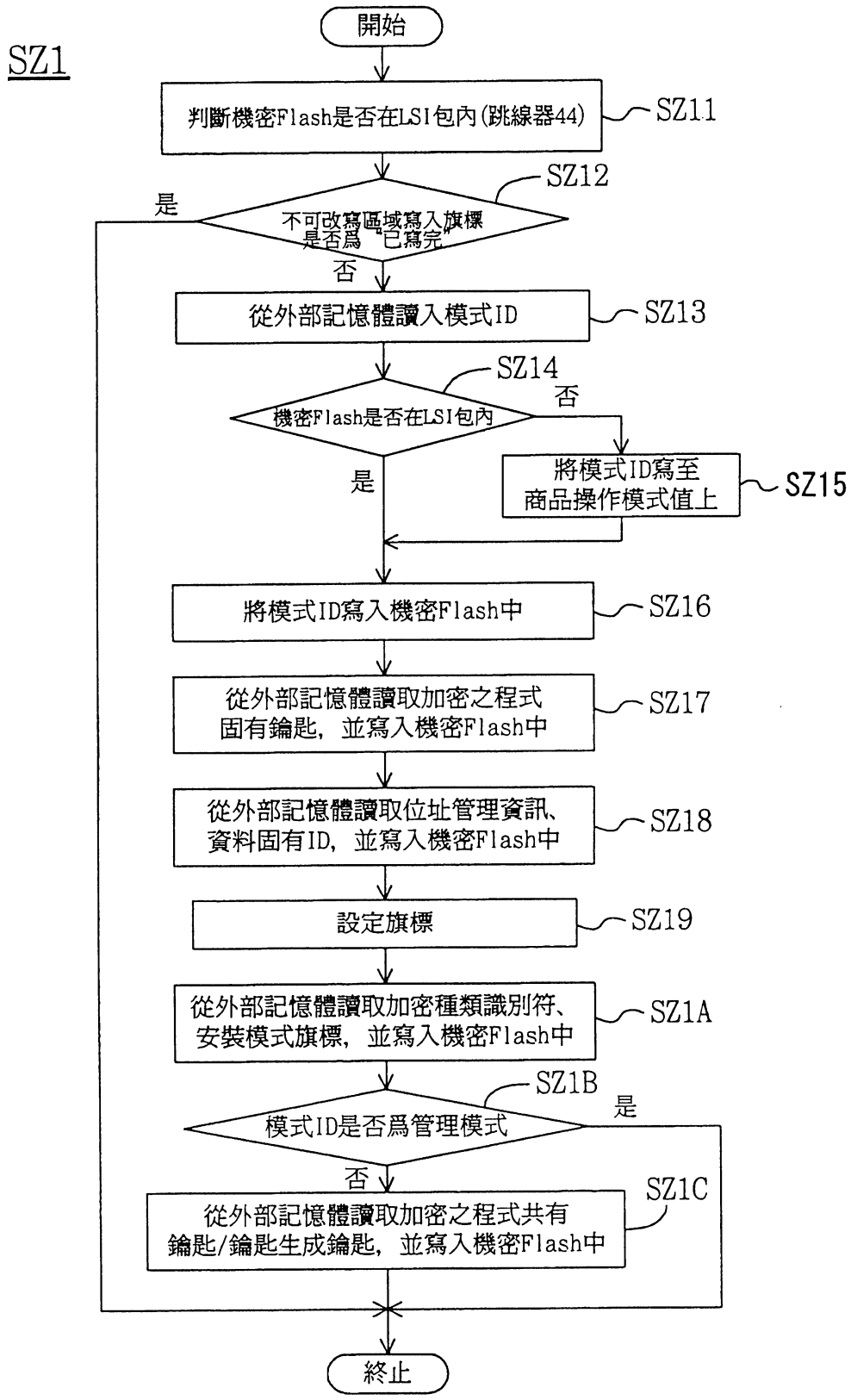

SZ1
開始
判斷機密Flash是否在LSI包內(跳線器44)
SZ11
SZ12
不可改寫區域寫入旗標是否爲"已寫完"
是
否
從外部記憶體讀入模式ID
SZ13
SZ14
機密Flash是否在LSI包內
否
是
將模式ID寫至商品操作模式值上
SZ15
將模式ID寫入機密Flash中
SZ16
從外部記憶體讀取加密之程式固有鑰匙，並寫入機密Flash中
SZ17
從外部記憶體讀取位址管理資訊、資料固有ID，並寫入機密Flash中
SZ18
設定旗標
SZ19
從外部記憶體讀取加密種類識別符、安裝模式旗標，並寫入機密Flash中
SZ1A
SZ1B
模式ID是否爲管理模式
是
否
SZ1C
從外部記憶體讀取加密之程式共有鑰匙/鑰匙生成鑰匙，並寫入機密Flash中
終止

圖 4

式圖

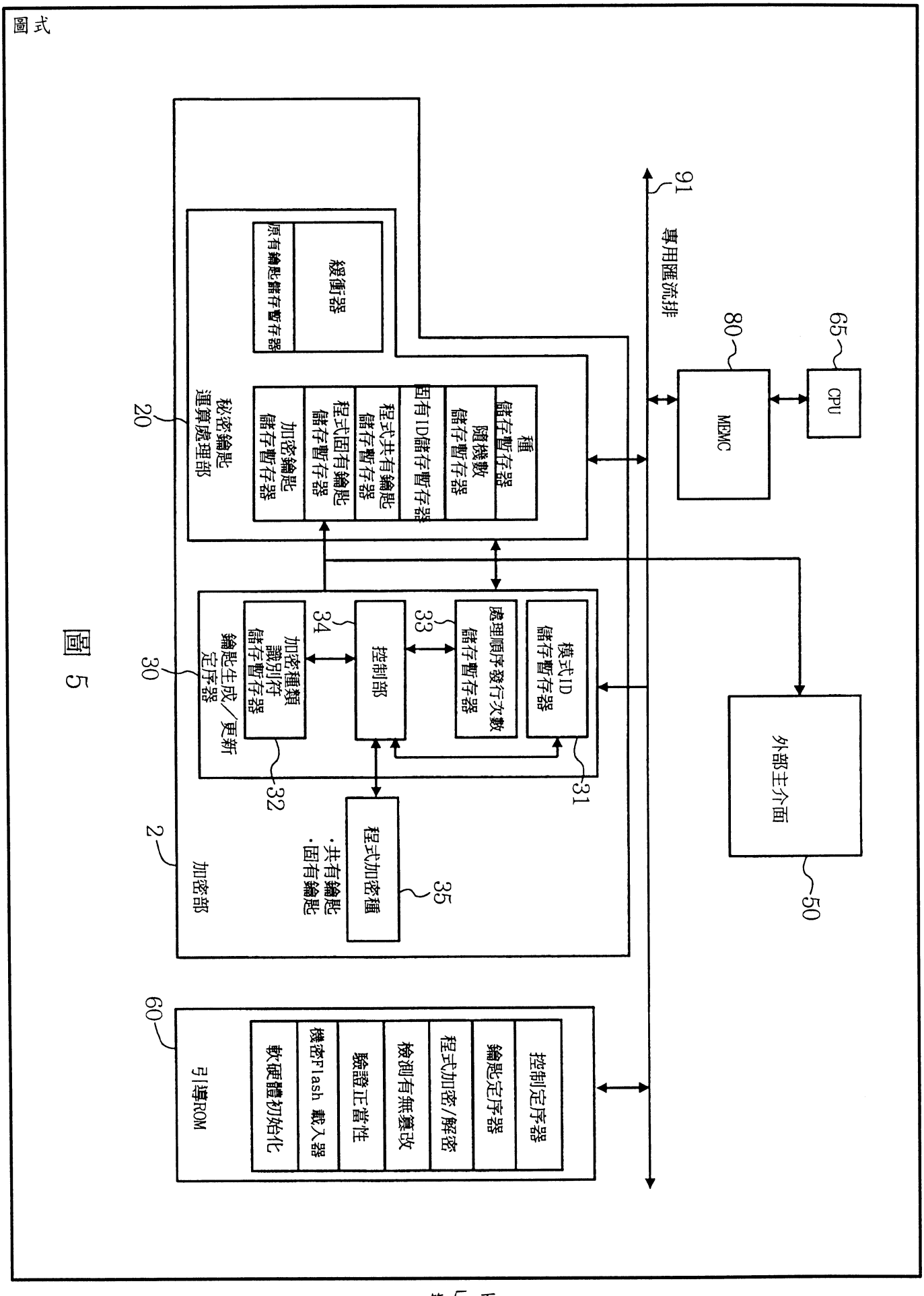

91
專用匯流排
65
CPU
80
MEMC
緩衝器
原有鑰匙儲存暫存器
種
儲存暫存器
隨機數
儲存暫存器
固有ID儲存暫存器
程式共有鑰匙
儲存暫存器
程式固有鑰匙
儲存暫存器
加密鑰匙
儲存暫存器
秘密鑰匙
運算處理部
20
模式ID
儲存暫存器
31
處理順序發行次數
儲存暫存器
33
控制部
34
加密種類
識別符
儲存暫存器
32
鑰匙生成/更新
定序器
30
程式加密種
35
·共有鑰匙
·固有鑰匙
2
加密部
外部主介面
50
60
控制定序器
鑰匙定序器
程式加密/解密
檢測有無篡改
驗證正當性
機密Flash 載入器
軟硬體初始化
引導ROM

圖 5

圖式

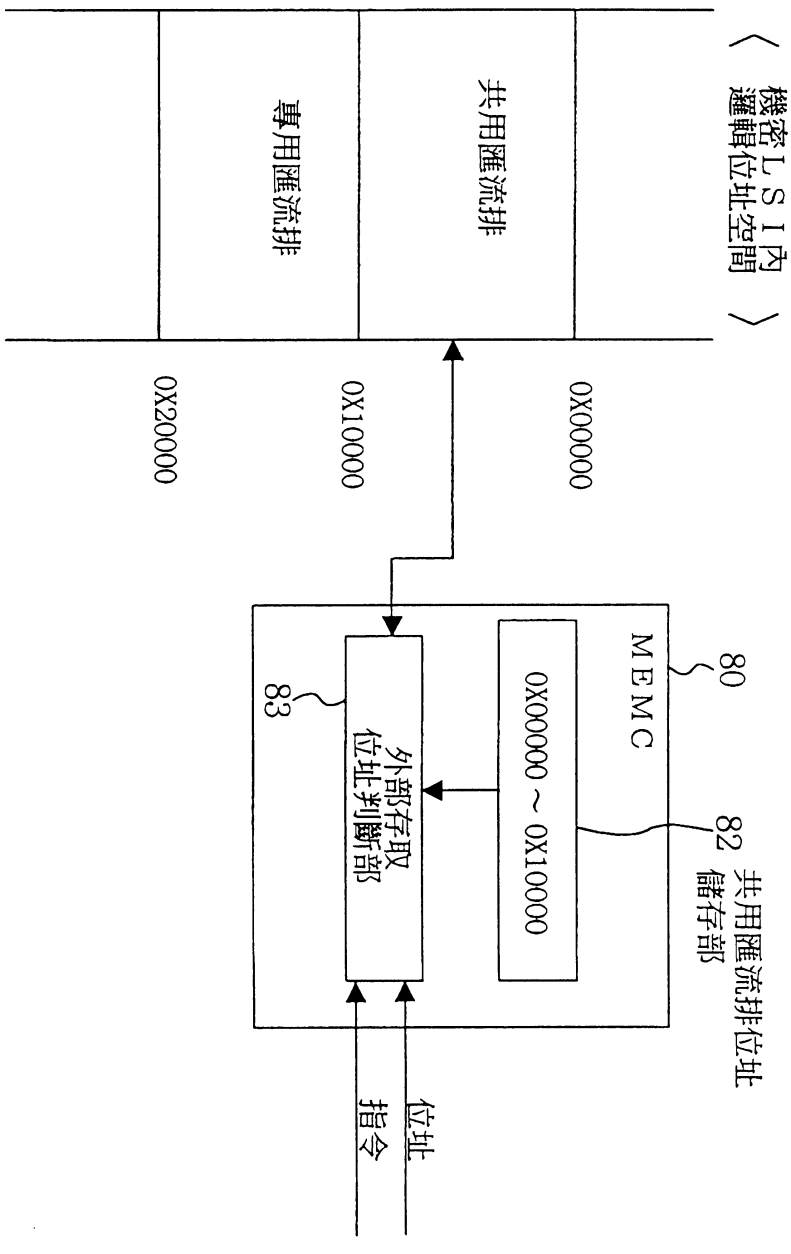

〈機密ＬＳＩ內邏輯位址空間〉
共用匯流排
專用匯流排
0X00000
0X10000
0X20000
MEMC
80
共用匯流排位址儲存部
82
0X00000 ~ 0X10000
外部存取位址判斷部
83
位址
指令

圖 6

圖式

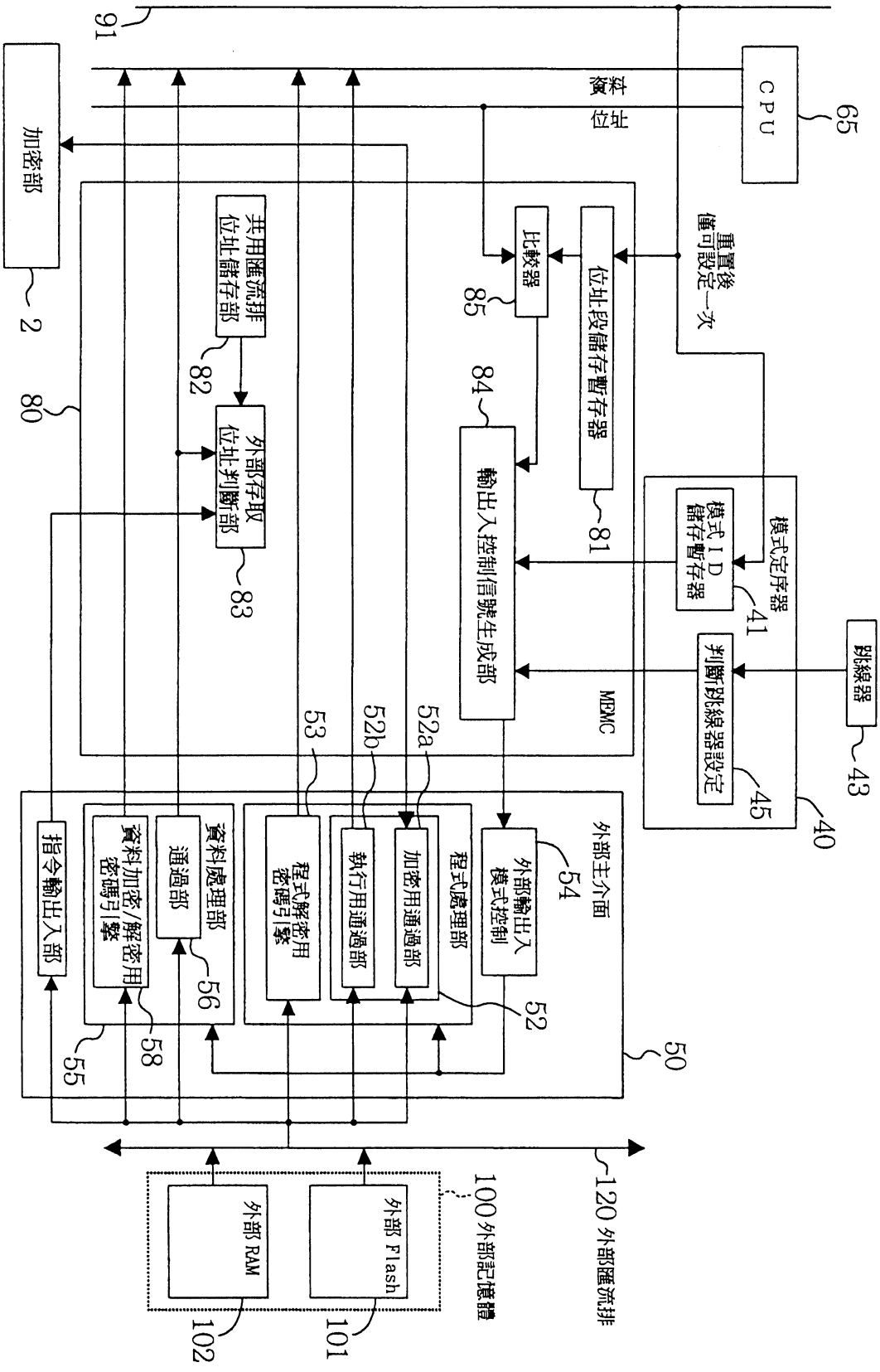

91
位址匯流排
CPU
65
加密部
2
80
共用匯流排
位址儲存部
82
外部存取
位址判斷部
83
比較器
85
位址段儲存暫存器
81
84
輸出入控制信號生成部
MEMC
重置後
僅可設定一次
模式定序器
模式ID
儲存暫存器
41
判斷跳線器設定
45
跳線器
43
40
外部主介面
54
外部輸出入
模式控制
程式處理部
52
加密用通過部
52a
執行用通過部
52b
程式解密用
密碼引擎
53
資料處理部
通過部
56
資料加密/解密用
密碼引擎
58
指令輸出入部
55
50
120 外部匯流排
100 外部記憶體
外部 Flash
101
外部 RAM
102

圖 7

圖式

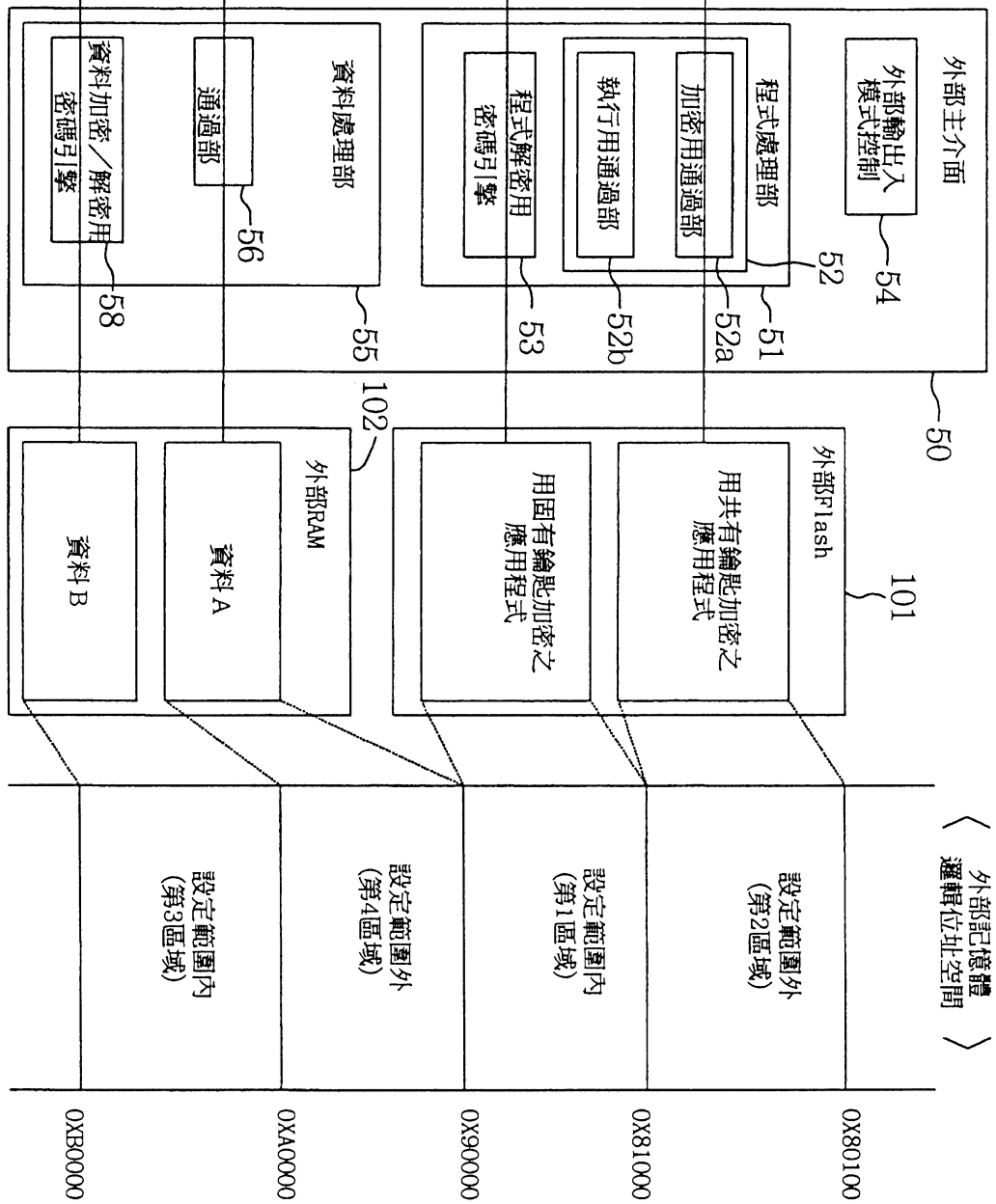

外部主介面
外部輸出入模式控制
54
程式處理部
52
加密用通過部
51
52a
執行用通過部
52b
程式解密用
密碼引擎
53
資料處理部
55
通過部
56
資料加密／解密用
密碼引擎
58
50
102
外部RAM
資料A
資料B
101
外部Flash
用共有鑰匙加密之應用程式
用固有鑰匙加密之應用程式
〈外部記憶體邏輯位址空間〉
設定範圍外(第2區域)
設定範圍內(第1區域)
設定範圍外(第4區域)
設定範圍內(第3區域)
0X80100
0X81000
0X90000
0XA0000
0XB0000

圖 8

圖式

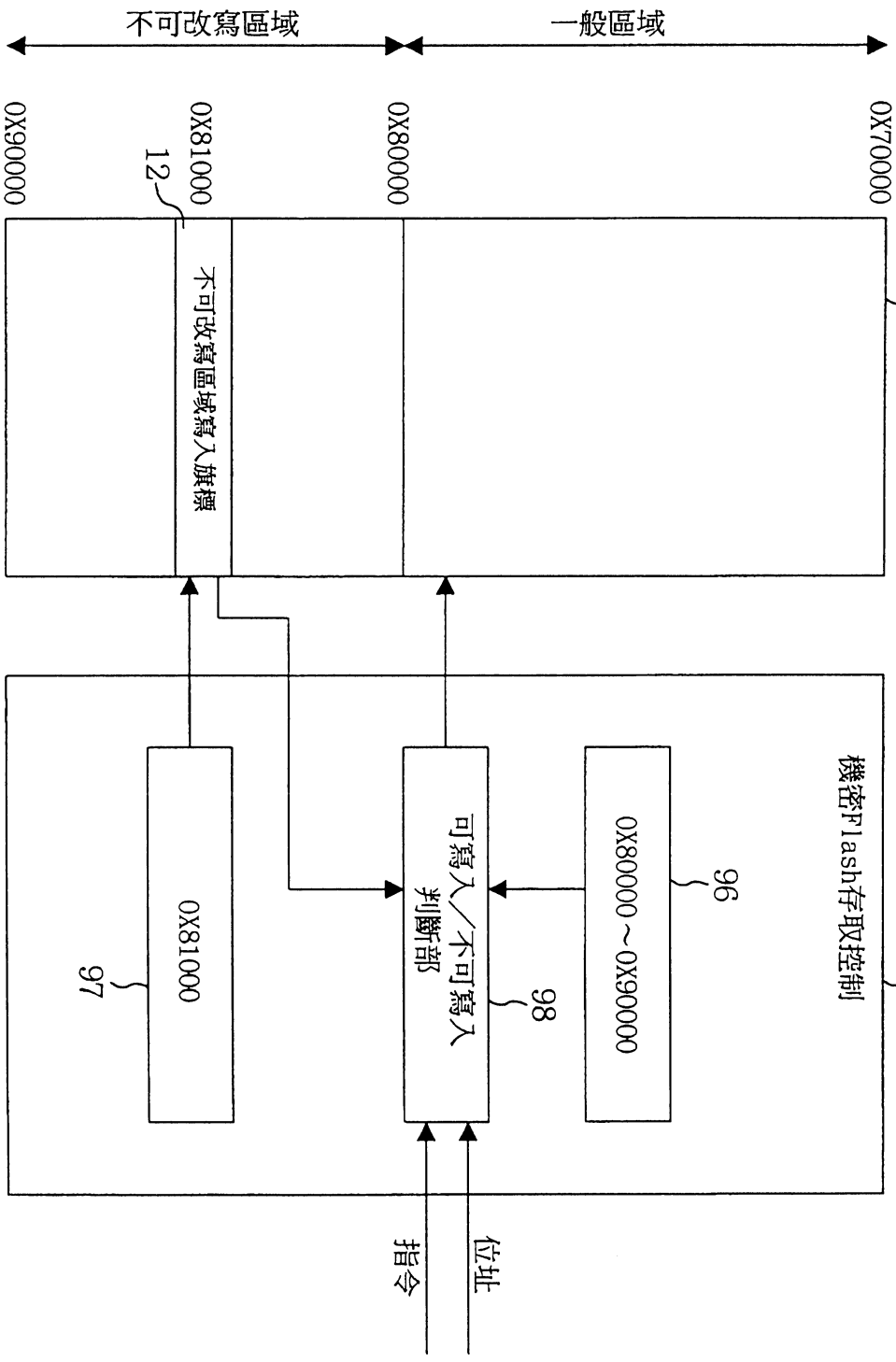

不可改寫區域
一般區域
0X90000
0X81000
12
0X80000
0X70000
10 機密Flash
不可改寫區域寫入旗標
機密Flash存取控制
95
96
0X80000～0X90000
98
可寫入／不可寫入判斷部
97
0X81000
指令
位址

圖 9

圖式

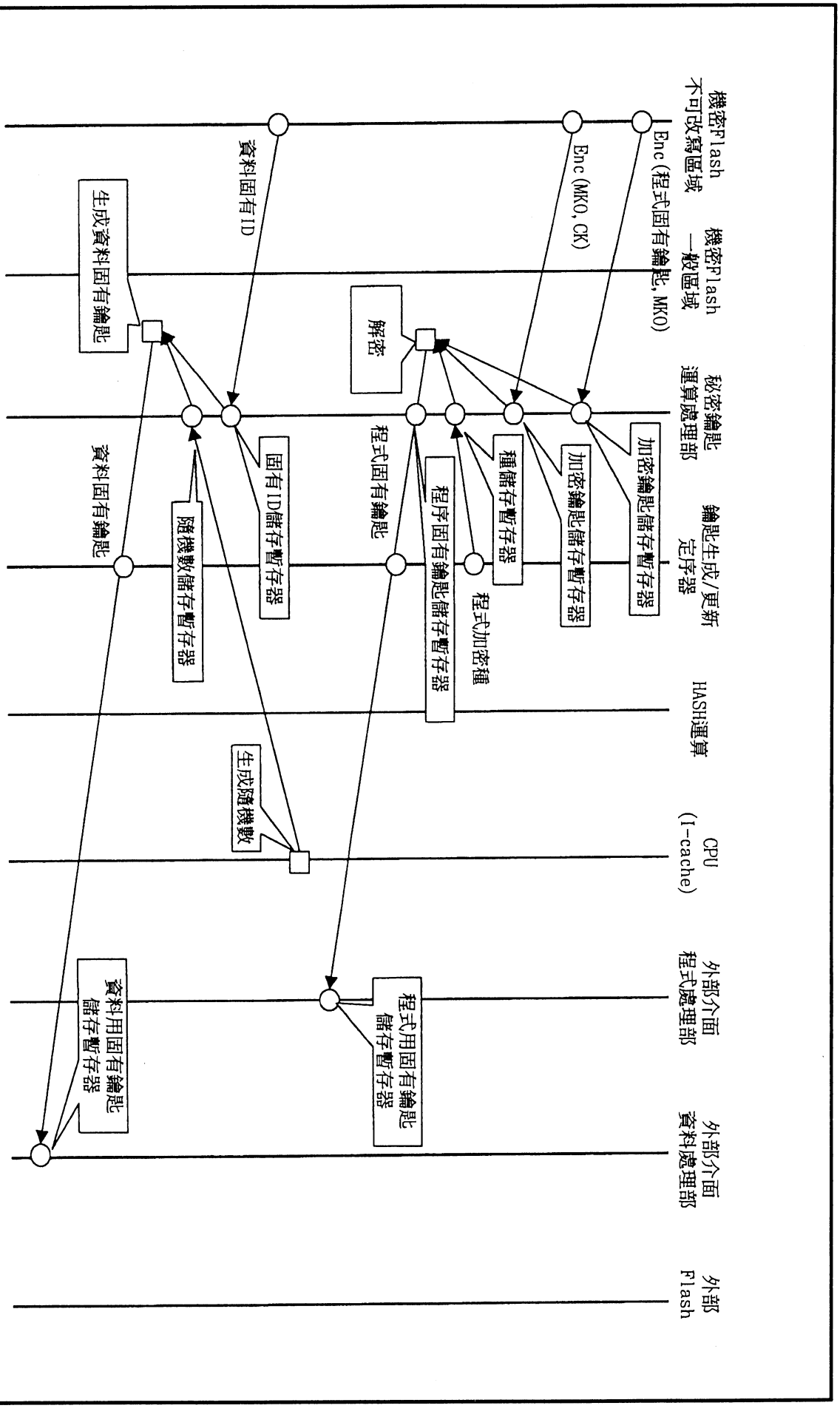

機密Flash
不可改寫區域
機密Flash
一般區域
秘密鑰匙
運算處理部
鑰匙生成/更新
定序器
HASH運算
CPU
(I-cache)
外部介面
程式處理部
外部介面
資料處理部
外部
Flash
Enc (程式固有鑰匙, MKO)
Enc (MKO, CK)
資料固有ID
生成資料固有鑰匙
解密
加密鑰匙儲存暫存器
加密鑰匙儲存暫存器
種儲存暫存器
程式加密種
程序固有鑰匙儲存暫存器
程式固有鑰匙
固有ID儲存暫存器
資料固有鑰匙
隨機數儲存暫存器
生成隨機數
程式用固有鑰匙
儲存暫存器
資料用固有鑰匙
儲存暫存器

圖 10

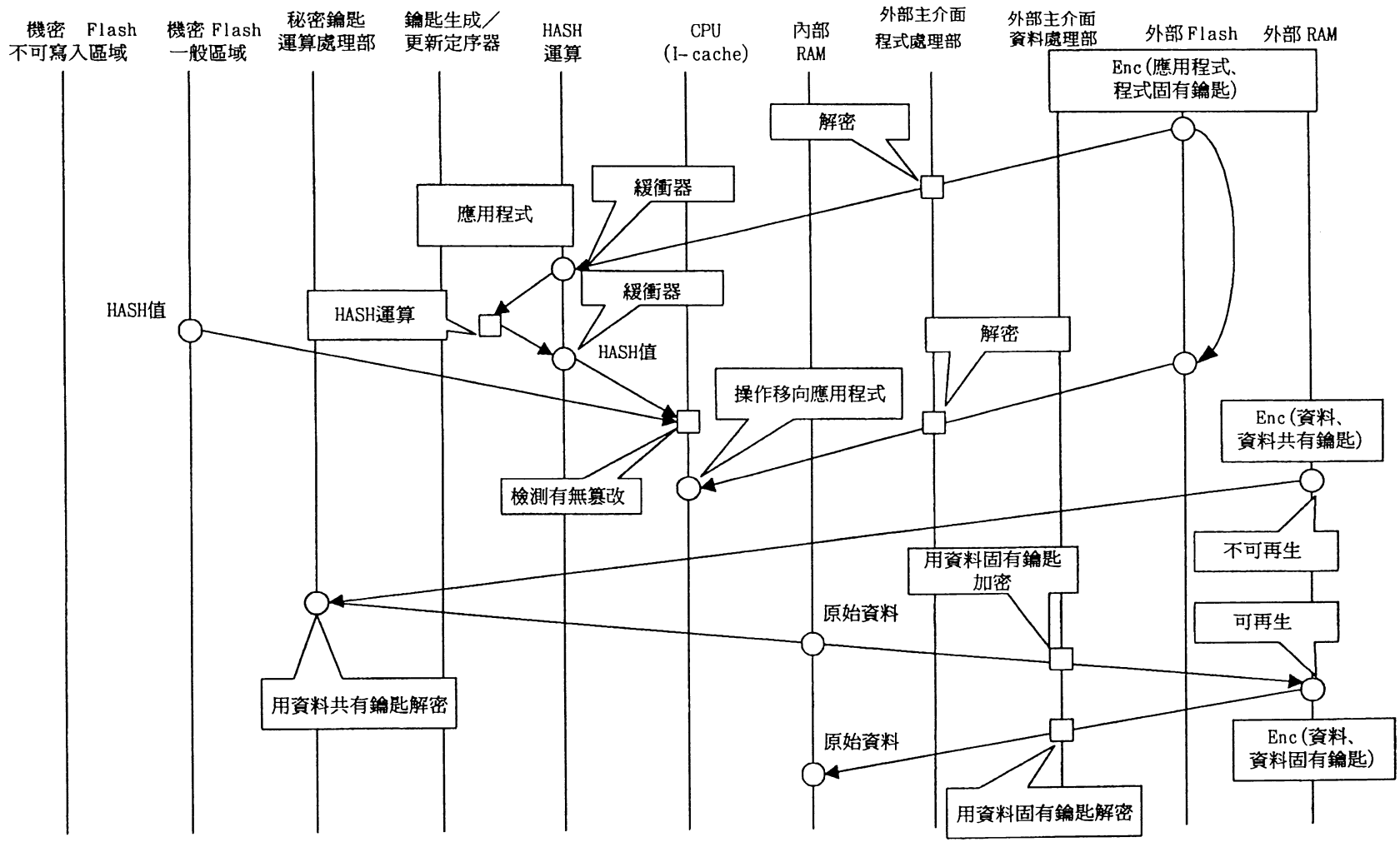

機密 Flash
不可寫入區域
機密 Flash
一般區域
秘密鑰匙
運算處理部
鑰匙生成／
更新定序器
HASH
運算
CPU
(I-cache)
內部
RAM
外部主介面
程式處理部
外部主介面
資料處理部
外部 Flash
外部 RAM
Enc(應用程式、
程式固有鑰匙)
解密
緩衝器
應用程式
緩衝器
HASH值
HASH運算
HASH值
解密
操作移向應用程式
Enc(資料、
資料共有鑰匙)
檢測有無篡改
不可再生
用資料固有鑰匙
加密
原始資料
可再生
用資料共有鑰匙解密
原始資料
Enc(資料、
資料固有鑰匙)
用資料固有鑰匙解密

圖 11

六、指定代表圖

（一）、本案代表圖為：第 1 圖

（二）、本案代表圖之元件代表符號簡單說明：

1　機密LSI（半導體裝置）

2　加密部

10　機密記憶體

11　不可改寫區域

12　不可改寫區域寫入旗標

13　一般區域

14　一般區域

20　秘密鑰匙運算處理部（加密運算部）

30　鑰匙生成／更新定序器（加密控制部）

31　模式ID儲存暫存器

32　加密種類識別符儲存暫存器

35　儲存部

40　模式定序器

41　模式ID儲存暫存器

42　加密種類識別符儲存暫存器

43　跳線器

44　跳線器

50　外部介面

51　程式處理部

52　通過部

53　程式加解密用密碼引擎

54　外部輸出入模式控制部

六、指定代表圖

55 資料處理部
56 通過部
58 資料加密／解密用密碼引擎
60 引導ROM
65 CPU
70 Hash運算部
80 MEMC
81 位址段儲存暫存器
82 共用匯流排位址儲存部
83 外部存取位址判斷部
84 輸出入控制信號生成部
91 私用匯流排
92 共用匯流排
95 存取控制部
100 外部記憶體
101 快閃記憶體
102 外部RAM
110 外部工具
120 外部匯流排