

發明專利說明書

200426596

(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：93109570

※申請日期：93.4.6

※IPC 分類：G06F13/36

壹、發明名稱：(中文/英文)

拌碼器電路

SCRAMBLER CIRCUIT

貳、申請人：(共 1 人)

姓名或名稱：(中文/英文)

日商夏普股份有限公司

SHARP KABUSHIKI KAISHA

代表人：(中文/英文)

町田 勝彦

MACHIDA, KATSUHIKO

住居所或營業所地址：(中文/英文)

日本國大阪府大阪市阿倍野區長池町22番22號

22-22, NAGAIKE-CHO, ABENO-KU, OSAKA-SHI, OSAKA 545-8522,
JAPAN

國 籍：(中文/英文)

日本 JAPAN

參、發明人：(共 1 人)

姓 名：(中文/英文)

大山 茂郎

OHYAMA, SHIGEO

住居所地址：(中文/英文)

日本國奈良縣奈良市二名2-2458-14

2-2458-14, NIMYO, NARA-SHI, NARA 631-0072, JAPAN

國 籍：(中文/英文)

日本 JAPAN

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. 日本；2003年04月08日；特願2003-103739
2. 日本；2003年05月29日；特願2003-152234
- 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. 日本；2003年04月08日；特願2003-103739
2. 日本；2003年05月29日；特願2003-152234
- 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】

本發明係關於資料處理裝置之安全性技術，特別係關於在半導體積體電路所構成之資料處理裝置中，可確保內部資訊，以防止惡意之攻擊者經由探測讀出或改變半導體積體電路內部資訊、及透過剝離分析讀出半導體積體電路內部資訊之安全性技術。

【先前技術】

在使用於儲存個人資訊等機密資訊，處理該資訊之IC卡等系統之單晶片微控制器中，要求高安全性，為避免受到攻擊者之攻擊(機密資訊之分析行為)，使內部資訊不被讀出或竄改，有必要保護此等資訊。

以往，通常將在含記憶體與單晶片控制器之邏輯電路間傳達信號之位址匯流排、資料匯流排之配線不規則連接，使各信號線所具有之機能難以特別設定，藉以從分析行為中保護資訊。但，最近的分析技術在現實的技術層次上，已可透過剝離分析，執行信號線之特別設定。

對此問題，在下列日本特開平11-203237號公報中，曾經揭示利用將匯流排上之信號週期性地變更順序，以執行匯流排攪拌之方法。上述公報所揭示之技術如圖15所示。符號1表示半導體積體電路，其內部係由CPU(Central Processing Unit：中央處理裝置)10、RAM(Random Access Memory；隨機存取記憶體)20、ROM(Read Only Memory：唯讀記憶體)30、E²PROM(Electrically Erasable Programmable

ROM:電可消除可程式化唯讀記憶體)40等之機能區塊所構成，另外包含時間控制電路60。在各區塊10、20、30、40之I/O部(資料輸出入部)及位址輸出入部，以鄰接於此等之形態設有第1拌碼器電路11、21、31、41。且配置使各第1拌碼器電路11、21、31、41互相連接之匯流排線50。時間控制電路60在特定時間輸出時間控制信號，各第1拌碼器電路11、21、31、41係依照此時間控制信號更換匯流排線50之各信號之連接，以執行攪拌。即，利用時間系列地執行攪拌，使在匯流排線50上傳達之資訊之分析更為困難。又，在各第1拌碼器電路11、21、31、41之外部(匯流排線50側)，以更換信號方式攪拌，但在其內側(記憶體RAM 20、ROM 30、E²PROM 40側)則以復原成原來之資料方式攪拌。

如此，在圖15所示之技術中，CPU 10與記憶體(RAM 20、ROM 30、E²PROM 40)間之資料雖可被攪拌，但記憶體上之資料則未被攪拌。即，匯流排線50上之資料雖可予以保護，但對於直接讀出或竄改儲存於記憶體上或其內部之資料，則處於無防備狀態。

如此，對於攻擊者在IC內部之匯流排及記憶體進行探測而讀出或竄改資料，並透過剝離分析由構成單體之記憶體讀出或竄改資料之行為，仍有未能充分執行安全性對策之缺點。

【發明內容】

本發明係鑒於上述問題所研發而成，其目的在於可將在匯流排上傳達之信號攪拌，且為使攪拌之資料不僅保存於

記憶體上，並保存於其內部，對匯流排上或記憶體上之任何資料之直接讀出或竄改，提供不能解碼原來之資訊之電路。

為達成此目的之本發明之拌碼器電路之特徵在於其係利用特定之攪拌處理將4位元以上之被處理資料變換成同位元數之已處理資料者；前述被處理資料分割成2位元以上之第1資料區塊與和前述第1資料區塊同位元數之第2資料區塊所構成，且前述已處理資料分割成分別和前述第1資料區塊同位元數之第3資料區塊與第4資料區塊所構成；且包含第1攪拌單元，其係對前述第1資料區塊執行特定之第1攪拌處理，以輸出同位元數之第1中間資料者；第1運算單元，其係執行前述第2資料區塊與前述第1中間資料之各位元之互斥"或"運算，以輸出前述第3資料區塊者；第2攪拌單元，其係對前述第3資料區塊執行與前述第1攪拌處理相同或相異之第2攪拌處理，以輸出同位元數之第2中間資料者；第2運算單元，其係執行前述第2中間資料與前述第1資料區塊之各位元之互斥"或"運算，以輸出前述第4資料區塊者。

另外，本發明之拌碼器電路之特徵在於前述攪拌單元係將輸入資料值，依據固定於該攪拌單元之變換規則變換成單一意義地決定之輸出資料值者。

依據具有上述特徵之本發明之拌碼器電路，可獲得對被處理資料施以攪拌處理之已處理資料，不能預測原來之資訊。又，適宜地設定第1及第2攪拌單元之攪拌處理之變換規則時，可多式多樣地自由變更攪拌處理之算法，謀求安

全性之提高。

為達成此目的之本發明之解拌器電路之特徵在於其係利用特定之解拌處理將4位元以上之已攪拌處理資料逆變換成同位元數之處理前資料者；前述已攪拌處理資料係分割成2位元以上之第5資料區塊與和前述第5資料區塊同位元數之第6資料區塊所構成，且前述處理前資料係分割成分別和前述第5資料區塊同位元數之第7資料區塊與第8資料區塊所構成；且包含第3攪拌單元，其係對前述第5資料區塊執行特定之第3攪拌處理，以輸出同位元數之第3中間資料者；第3運算單元，其係執行前述第6資料區塊與前述第3中間資料之各位元之互斥"或"運算，以輸出前述第7資料區塊者；第4攪拌單元，其係對前述第7資料區塊執行與前述第3攪拌處理相同或相異之第4攪拌處理，以輸出同位元數之第4中間資料者；第4運算單元，其係執行前述第4中間資料與前述第5資料區塊之各位元之互斥"或"運算，以輸出前述第8資料區塊者。

另外，本發明之解拌器電路之特徵在於前述攪拌單元係將輸入資料值，依據固定於該攪拌單元之變換規則變換成單一意義地決定之輸出資料值者。

依據具有上述特徵之本發明之解拌器電路，可使被本發明之拌碼器電路攪拌處理之已攪拌處理資料逆變成原來之處理前資料。又，本發明之解拌器電路可利用與拌碼器電路相同之電路構成，以將拌碼器電路之第1攪拌單元使用於第4攪拌單元，將拌碼器電路之第2攪拌單元使用於第3攪拌

單元之方式簡單地構成。

另外，在本發明之拌碼器電路及解拌器電路中，最好採用攪拌單元係由換接對應於輸入資料之各位元之多數輸入端子與對應於輸出資料之各位元之輸出端子間之配線之一部分或全部所構成，且藉前述配線之換接，固定前述變換規則之構成方法。此時，採用藉前述配線之換接，對前述輸入資料執行1位元或2位元以上之循環移位操作之構成方法。或，採用藉前述配線之換接，對前述輸入資料之特定之2位元執行更換操作之構成方法。或，採用藉前述配線之換接，組合地執行對前述輸入資料之1位元或2位元以上之循環移位操作與對前述輸入資料之特定之2位元之更換操作之構成方法。尤其，採用最後之構成方法時，可網羅有關配線換接之全部組合。

另外，在本發明之拌碼器電路及解拌器電路中，最好也採用攪拌單元係包含對輸入資料之一部分或全部之位元施以特定之邏輯運算之邏輯運算電路，藉前述邏輯運算電路固定前述變換規則之構成方法。此時，採用前述邏輯運算電路對前述輸入資料之一部分或全部之位元，施行2位元以上之邏輯運算之構成方法。

另外，在本發明之拌碼器電路及解拌器電路中，最好攪拌單元係包含對輸入資料之一部分或全部之位元與前述輸入資料輸入時之位址資料之一部分或全部之位元，施行特定之邏輯運算之邏輯運算電路所構成，藉前述邏輯運算電路，對應於前述位址資料之位址值而單一意義地固定前述

變換規則。

另外，在本發明之拌碼器電路及解拌器電路中，最好攪拌單元係包含對輸入資料之一部分或全部之位元與保持於特定之非揮發性記憶體之變換規則固定用資料，施行特定之邏輯運算之邏輯運算電路所構成，藉前述邏輯運算電路，且對應於前述變換規則固定用資料之資料值而單一意義地固定前述變換規則。

另外，在本發明之拌碼器電路及解拌器電路中，最好攪拌單元係包含選擇電路，其係依據輸入資料被預先固定之變換規則變換成單一意義地決定之輸出資料之攪拌子單元之前述變換規則相異之多數、與對應於前述輸入資料輸入時之特定資訊而變化之選擇規則，選擇並輸出相同輸入資料輸入後之前述多數攪拌子單元之輸出資料之1者；且依照前述變換規則所選擇之前述攪拌子單元，以單一意義地決定之方式固定於該攪拌單元之前述變換規則。此時，最好在拌碼器電路中，包含前述多數攪拌子單元之前述攪拌子單元係包含碼產生電路，其係依照前述輸入資料輸入於前述多數攪拌子單元時之特定資訊而產生選擇碼，且與前述輸入時之位址資料相關連地將其記憶於特定之非揮發性記憶體者；及查閱表，其係個別地使前述選擇碼與前述多數攪拌子單元相對應者；前述選擇電路係構成由依據前述碼產生電路產生之前述選擇碼與前述查閱表所指定之前述多數攪拌子單元中之1選擇前述輸出資料。又，解拌器電路最好採用包含前述多數攪拌子單元之前述攪拌單元係包含碼

讀出電路，其係依照前述輸入資料輸入於前述多數攪拌子單元時之位址資訊而讀出記憶於特定之非揮發性記憶體之選擇碼者；及查閱表，其係個別地使前述選擇碼與前述多數攪拌子單元相對應者；前述選擇電路係構成由依據前述碼讀出電路讀出之前述選擇碼與前述查閱表所指定之前述多數攪拌子單元中之1選擇前述輸出資料。

利用上述攪拌單元之各構成方法，可利用硬體規定多種多樣之規則作為攪拌單元之攪拌處理之變換規則。因此，不能或極難以施行攪拌處理前後之相關資料之解碼。

本發明之資料處理裝置之特徵在於其係以內部匯流排連接多數機能區塊所構成，且在前述內部匯流排與外部匯流排之第1匯流排介面部包含以前述內部匯流排上之一部分或全部之資料為前述被處理資料，以前述外部匯流排上之一部分或全部之資料為前述已處理資料之本發明之拌碼器電路。

依據具有上述特徵之本發明之資料處理裝置，可在對內部匯流排上之資料施以攪拌處理後，傳送至外部，例如記憶於外部之記憶體裝置等，故可快速提高資料之安全性。

又，本發明之資料處理裝置之特徵在於其係以內部匯流排連接多數機能區塊所構成，且在前述內部匯流排與外部匯流排之第2匯流排介面部包含以前述內部匯流排上之一部分或全部之資料為前述處理前資料，以前述外部匯流排上之一部分或全部之資料為前述已攪拌處理資料之本發明之解拌器電路。

依據具有上述特徵之本發明之資料處理裝置，可利用由外部接收被本發明之拌碼器電路施以攪拌處理之已攪拌處理資料後，以解拌器電路施以解拌處理，逆變換成原來之處理前資料，故可一面確保資料之安全性，一面在內部匯流排上利用原來之處理前資料。

另外，本發明之資料處理裝置之特徵在於其係以內部匯流排連接多數機能區塊所構成，且在前述內部匯流排與外部匯流排之第1匯流排介面部包含以前述內部匯流排上之一部分或全部之資料為前述被處理資料，以前述外部匯流排上之一部分或全部之資料為前述已處理資料之本發明之拌碼器電路，且在前述內部匯流排與外部匯流排之第2匯流排介面部包含以前述內部匯流排上之一部分或全部之資料為前述處理前資料，以前述外部匯流排上之一部分或全部之資料為前述已攪拌處理資料之本發明之解拌器電路。

依據具有上述特徵之本發明之資料處理裝置，可在對內部匯流排上之資料施以攪拌處理後，傳送至外部，例如記憶於外部之記憶體裝置等，故可快速提高資料之安全性。另外，可利用由外部接收被本發明之拌碼器電路施以攪拌處理之已攪拌處理資料後，以解拌器電路施以解拌處理，逆變換成原來之處理前資料，故可一面確保資料之安全性，一面在內部匯流排上利用原來之處理前資料。

在此，拌碼器電路雖未必需要與攪拌處理同一資料處理裝置內之解拌器電路之解拌處理對象之已攪拌處理資料之拌碼器電路相同，但若相同時，由於可在同一資料處理裝

置內處理攪拌處理與解拌處理雙方之動作，故可執行將已攪拌處理資料記憶於外部之記憶裝置，將其讀出而再利用之作業等。

但，後者之情形，也就是說，在解拌器電路解拌處理同一資料處理裝置內之拌碼器電路之已攪拌處理資料之情形，可利用將拌碼器電路之第1攪拌單元使用於解拌器電路之第4攪拌單元，將拌碼器電路之第2攪拌單元使用於解拌器電路之第3攪拌單元之方式簡單地加以實現。

另外，本發明之資料處理裝置之特徵在於其係以第2內部匯流排連接前述多數機能區塊所構成，且在前述第2內部匯流排與第2外部匯流排之第3匯流排介面部包含以前述第2內部匯流排上之一部分或全部之資料為前述被處理資料，以前述第2外部匯流排上之一部分或全部之資料為前述已處理資料之本發明之拌碼器電路。依據具有此特徵之本發明之資料處理裝置，可快速提高資料及資料處理上之安全性。

又，在本發明之資料處理裝置中，也可採用將前述內部匯流排與前述外部匯流排，或前述第2內部匯流排與第2外部匯流排分別分割成多數區塊，並在前述各區塊包含本發明之拌碼器電路或解拌碼器電路之構成方式。

另外，在本發明之資料處理裝置中，其特徵在於前述內部匯流排與前述外部匯流排為資料匯流排，前述第2內部匯流排與前述第2外部匯流排為位址匯流排。依據具有上述特徵之本發明之資料處理裝置，由於在同一資料處理裝置內

包含將資料匯流排攪拌處理之拌碼器電路、與解拌處理之解拌器電路，故可攪拌處理資料匯流排與記憶體上之資料。又，可在資料處理裝置內設置攪拌處理位址匯流排之拌碼器電路，以已攪拌處理之位址存取記憶體時，可更安全地保護資料。

另外，本發明之資料處理裝置之特徵在於以形成於同一半導體基板上之半導體積體電路構成前述多數機能區塊及前述匯流排介面部。另外，作為前述機能區塊，以包含作為含算術邏輯運算器，且控制前述內部匯流排與前述外部匯流排之單晶片微控制器之機能為其特徵。由於此等特徵，攻擊者不可能或極難進行在IC內部之匯流排及記憶體進行探測而讀出或竄改資料，並透過剝離分析由構成單體之記憶體讀出或竄改資料之行為。

本發明之IC卡之特徵在於使用作為本發明之資料處理裝置系統控制用之單晶片微控制器。依據具有此特徵之本發明之IC卡，可對資料匯流排與記憶體上之資料施以攪拌處理，實現高安全性之IC卡。

【實施方式】

以下，依據圖式，說明有關本發明之拌碼器電路、解拌器電路及具備此等電路之資料處理裝置之一實施形態。

圖1係表示具有本實施形態之拌碼器電路220、230、解拌器電路240之半導體積體電路100(以下稱為「IC」)之內部構成之一例。

圖1所示之IC 100係具有作為本發明之資料處理裝置之

一例之CPU 200、以CPU 200與外部資料匯流排600及外部位址匯流排700互相連接之ROM 300、RAM 400、電性可改寫之快閃E²PROM等非揮發性記憶體500等外部記憶體群，而構成作為單晶片微電腦。

在CPU 200內，經由內部資料匯流排213，使ALU(算術邏輯運算器)210、快取記憶體211、指令解碼器控制器212、暫存器群214、資料匯流排控制電路215等相互連接。又，暫存器群214係被連接於位址匯流排控制電路216。

CPU 200係利用第1拌碼器電路230對內部資料匯流排213上之資料進行攪拌處理，並輸出至外部資料匯流排600。又，由外部資料匯流排600輸入資料時，利用解拌器電路240進行解拌處理，並輸出至內部資料匯流排213。

CPU 200對外部記憶體群存取時之位址係被以第2拌碼器電路220施行攪拌處理之位址所存取。又，第1拌碼器電路230與第2拌碼器電路220之攪拌處理之算法可以相同也可相異。也就是說，在第1、第2拌碼器電路220、230間，固定後述之拌碼器電路之變換規則之攪拌單元之電路構成可為相同構成，也可為個別不同之構成。

在圖1所示之實施形態中，雖對位址匯流排施行攪拌處理，但位址匯流排之攪拌處理並非必須動作。因此，如圖2所示，採用僅對資料匯流排施行攪拌處理而不設置第2拌碼器電路220之構成也無妨。在此，在圖2所示之構成中，除不具有第2拌碼器電路220以外，其他均與圖1之實施形態相同。

其次，說明有關本發明之拌碼器電路(第1拌碼器電路230、第2拌碼器電路220)及解拌器電路240之電路構成。以下，在拌碼器電路中，第1拌碼器電路230與第2拌碼器電路220之基本之電路構成相同，故僅說明其中一方。圖3A係表示拌碼器電路230之電路圖，圖3B係表示解拌器電路240之電路圖。

如圖3A所示，將攪拌處理前之資料分割成第1資料區塊B1($n/2$ bit~ $n-1$ bit)、第2資料區塊B0(0 bit~ $n/2-1$ bit)之2個資料區塊之資料係被輸入至拌碼器電路230。又，拌碼器電路230係輸出由第3資料區塊B1'($n/2$ bit~ $n-1$ bit)、第4資料區塊B0'(0 bit~ $n/2-1$ bit)之2個資料區塊構成之攪拌處理後之同位元數之資料。

拌碼器電路230係由對輸入B1施行第1攪拌處理之第1攪拌單元231、對第1攪拌單元231之輸出(第1中間資料)與輸入B0依各位元計算互斥"或"之多數互斥"或"電路所構成之第1運算單元233、對第1運算單元233之輸出之第3資料區塊B1'施行第2攪拌處理之第2攪拌單元232、對第2攪拌單元232之輸出(第2中間資料)與輸入B1依各位元計算互斥"或"而輸出第4資料區塊B0'之多數互斥"或"電路所構成之第2運算單元234所構成。

同樣地，如圖3B所示，將解拌處理前之已攪拌處理資料分割成第5資料區塊B1'($n/2$ bit~ $n-1$ bit)、第6資料區塊B0'(0 bit~ $n/2-1$ bit)之2個資料區塊之資料係被輸入至解拌器電路240。又，解拌器電路240係輸出由第7資料區塊B1"($n/2$

bit~n-1 bit)與第8資料區塊B0"(0 bit~n/2-1 bit)之2個資料區塊所構成而在攪拌處理前被解拌處理逆變換之同位元數之處理前資料。

解拌器電路240係由對輸入B1'施行第3攪拌處理(在本實施形態中，與前述第2攪拌處理相同)之第3攪拌單元232(在本實施形態中，與第2攪拌單元232)、對第3攪拌單元232之輸出(第3中間資料)與輸入B0'依各位元計算互斥"或"之多數互斥"或"電路所構成之第3運算單元233、對第3運算單元233之輸出之第7資料區塊B1"施行第4攪拌處理(在本實施形態中，與前述第1攪拌處理相同)之第4攪拌單元231(在本實施形態中，與第1攪拌單元231)、對第4攪拌單元231之輸出(第4中間資料)與輸入B1'依各位元計算互斥"或"而輸出第8資料區塊B0"之互斥"或"電路所構成之第4運算單元234所構成。

在此，各攪拌單元231、232所施行之攪拌處理係構成將輸入資料值，依據固定於該攪拌單元之變換規則變換成單一意義地決定之輸出資料值。

在此，需要注意之處在於：拌碼器電路230內之第1攪拌單元231與解拌器電路240內之第4攪拌單元231必須採用依據相同變換規則施行相同之攪拌處理之電路構成之點上。同樣情形，拌碼器電路230內之第2攪拌單元232與解拌器電路240內之第3攪拌單元232也必須採用相同之電路構成。又，第1、第4攪拌單元231與第2、第3攪拌單元232既可採用相同之構成，亦可採用個別之構成。但，採用個別

之電路構成時，更可提高安全性。又，第1至第4運算單元233、234分別在電路構成上相同。

其次，將第1(第4)攪拌單元231之操作以S1函數加以表現，將第2(第3)攪拌單元232之操作以S2函數加以表現，而說明拌碼器電路230與解拌器電路240之動作。

拌碼器電路230之動作(攪拌處理)可利用以下之式1及式2加以表示：

(式1)

$$B1'=B0 \text{ xor } S1(B1)$$

(式2)

$$B0'=B1 \text{ xor } S2(B1')$$

其次，解拌器電路240之動作(解拌處理)可利用以下之式3及式4加以表示：

(式3)

$$B1''=B0' \text{ xor } S2(B1')$$

(式4)

$$B0''=B1' \text{ xor } S1(B1'')$$

利用式1~式4之公式表示拌碼器電路230所攪拌處理之資料在解拌器電路240之解拌處理中被逆變換而恢復為原來之資料之過程。將式2之B0'代入式3之B0'而消去B0'時，得下述之式5。在此，多變數之互斥"或"運算不管其運算順序如何，均可獲得相同之運算結果，且相同數值彼此之互斥"或"均為0，故成為如式6所示。

(式5)

$$B1'' = B1 \text{ xor } S2(B1') \text{ xor } S2(B1')$$

(式 6)

$$B1'' = B1 \text{ xor } 0 = B1$$

其次，將式 4 之 $B1'$ 代入式 1 之 $B1'$ 而消去 $B1'$ 時，得下述之式 7。再將式 6 之 $B1''$ 代入式 7 之 $B1''$ 而加以消去，多變數之互斥"或"運算不管其運算順序如何，均可獲得相同之運算結果，且相同數值彼此之互斥"或"均為 0，故成為如式 8 所示。

(式 7)

$$B0'' = B0 \text{ xor } S1(B1) \text{ xor } S1(B1'')$$

(式 8)

$$B0'' = B0 \text{ xor } S1(B1) \text{ xor } S1(B1) = B0$$

以上，由式 1~式 8 可證明攪拌處理前之資料 $B0$ 、 $B1$ 與攪拌處理後之資料 $B0''$ 、 $B1''$ 相同。又，上述之計算不依存函數 $S1$ 及 $S2$ 之運算內容而均可成立，故只要各函數 $S1$ 及 $S2$ 能滿足對輸入之任意值均可單一意義地決定輸出之條件，即可任意選擇第 1、第 2 攪拌單元 231、232 所施行之攪拌處理之內容。因此，只要考慮安全強度與電路規模等成本或實現容易性之調適而選擇最適之處理作為函數 $S1$ 及 $S2$ 即可。

其次，說明有關固定規定第 1 或第 2 攪拌單元 231、232 之各攪拌處理之變換規則用之電路構成。首先，圖 4 係表示第 1 或第 2 攪拌單元 231、232 之電路構成之第 1 實施例。

對輸入 $[D_{n-1}, D_{n-2}, \dots, D1, D0]$ ，使輸出 $[SD_{n-1}, SD_{n-2}, \dots, SD1, SD0]$ 施行 1 位元之向右移位。利用此

操作，輸出 $[SD_{n-1}, SD_{n-2}, \dots, SD_1, SD_0]$ 可表現成如以下之式9所示。又，假設D0會循環地移位至左側第1位元。

(式9)

$$\begin{aligned} & [SD_{n-1}, SD_{n-2}, \dots, SD_1, SD_0] \\ & = [D_0, D_{n-1}, \dots, D_2, D_1] \end{aligned}$$

圖5係表示第1或第2攪拌單元231、232之電路構成之第2實施例。

對輸入 $[D_{n-1}, D_{n-2}, \dots, D_1, D_0]$ ，使輸出 $[SD_{n-1}, SD_{n-2}, \dots, SD_1, SD_0]$ 施行各相鄰之2位元之調換。利用此操作，輸出 $[SD_{n-1}, SD_{n-2}, \dots, SD_1, SD_0]$ 可表現成如以下之式10所示。

(式10)

$$\begin{aligned} & [SD_{n-1}, SD_{n-2}, \dots, SD_1, SD_0] \\ & = [D_{n-2}, D_{n-1}, \dots, D_0, D_1] \end{aligned}$$

另外，在圖中並未予以顯示，即作為第1或第2攪拌單元231、232之電路構成之第3實施例，也可藉將上述第1實施例與第2實施例予以任意組合，而實現更多樣之配線之更換連接。

圖6係表示第1或第2攪拌單元231、232之電路構成之第4實施例。在上述第1~第3實施例中，係利用換接對應於輸入資料之各位元之多數輸入端子與對應於輸出資料之各位元之輸出端子間之配線而加以實現，但在如圖6所示之第4實施例中，則利用對輸入資料之各位元施行特定之邏輯運算方式加以實現。具體而言，係對輸入 $[D_{n-1}, D_{n-2}, \dots,$

D1、D0]，使輸出[SD_{n-1}、SD_{n-2}、．．、SD1、SD0]在相鄰之位元間施行nand("與")運算。利用此操作，輸出[SD_{n-1}、SD_{n-2}、．．、SD1、SD0]可表現成如以下之式11所示。

(式11)

$$\begin{aligned} & [\text{SD}_{n-1}, \text{SD}_{n-2}, \dots, \text{SD}_1, \text{SD}_0] \\ & = [\text{D}_0 \text{ nand } \text{D}_{n-1}, \dots, \text{D}_1 \text{ nand } \text{D}_0] \end{aligned}$$

在此，邏輯運算之種類並非限定於nand，且施行運算之位元數也可適宜地加以變更。

圖7係表示第1或第2攪拌單元231、232之電路構成之第5實施例。在上述第1~第4實施例中，由輸入資料對輸出資料之變換規則不管位址資料之位址值如何，均經常保持一定，但在圖7所示之第5實施例中，係對該輸入資料，利用對應於該輸入資料之記憶體之位址施行邏輯運算，以實現因各位址而異之攪拌處理。

具體而言，使輸出[SD_{n-1}、SD_{n-2}、．．、SD1、SD0]在輸入[D_{n-1}、D_{n-2}、．．、D1、D0]與位址[AD_{n-1}、AD_{n-2}、．．、AD1、AD0]間依各位元施行xor(互斥"或")運算。利用此操作，輸出SD[n-1:0]可表現成如以下之式12所示。

(式12)

$$\begin{aligned} & [\text{SD}_{n-1}, \text{SD}_{n-2}, \dots, \text{SD}_1, \text{SD}_0] \\ & = [\text{D}_{n-1} \text{ xor } \text{AD}_{n-1}, \dots, \text{D}_0 \text{ xor } \text{AD}_0] \end{aligned}$$

如式12所示，對任意之位址值，規定攪拌處理之變換規則可單一意義地加以決定，故在同一攪拌單元231、232內，

即使變換規則因位址值之變化而變化時，在逆變換時，也可利用相同之位址值，保證逆變換成攪拌處理前之資料。即，位址值具有可作為規定攪拌處理之變換規則之鍵資訊之機能。

在此，邏輯運算之種類並非限定於互斥"或"運算，且鍵資訊(在本實施例中，為位元值)之位元數及施行運算之位元數也可適宜地加以變更。

圖8係表示第1或第2攪拌單元231、232之電路構成之第6實施例。在上述第1~第5實施例中，攪拌單元內之更換連接及邏輯運算電路等之硬體構成或邏輯運算電路與位元值之組合若相同時，輸入資料與輸出資料間之變換規則即可經常保持一定。相對地，在圖8所示之第6實施例中，係對輸入資料，使用保管於鍵保管用之非揮發性記憶體250之鍵資訊(變換規則固定用資料)施行邏輯運算，即使相同之硬體構成或位元值，亦可實現因攪拌單元而異之攪拌處理。

具體而言，使輸出[SD_{n-1}、SD_{n-2}、．．、SD₁、SD₀]在輸入[D_{n-1}、D_{n-2}、．．、D₁、D₀]與鍵資訊[K_{n-1}、K_{n-2}、．．、K₁、K₀]間依各位元施行xor(互斥"或")運算。利用此操作，輸出SD[n-1:0]可表現成如以下之式13所示。

(式13)

$$\begin{aligned} & [\text{SD}_{n-1}, \text{SD}_{n-2}, \dots, \text{SD}_1, \text{SD}_0] \\ & = [\text{D}_{n-1} \text{ xor } \text{K}_{n-1}, \dots, \text{D}_0 \text{ xor } \text{K}_0] \end{aligned}$$

保管於鍵保管用之非揮發性記憶體250之鍵資訊既可在包含此攪拌單元之裝置之製造階段加以固定，亦可利用以

可改寫之非揮發性記憶體另行設置之寫入手段，在製造後設定於任意值。

在此，邏輯運算之種類並非限定於互斥"或"運算，且鍵資訊之位元數及施行運算之位元數也可適宜地加以變更。

圖9及圖10係表示第1(第4)或第2(第3)攪拌單元231、232之電路構成之第7及第8實施例。在上述第1~第6實施例中，輸入資料與輸出資料間之變換規則在同一攪拌單元中經常保持一定，但在第7及第8實施例中，係準備多數使用於輸入資料之變換規則相異之攪拌子單元235，並具備有選擇電路236，使其依據因輸入資料輸入時之特定資訊而變化之變換規則，選擇並輸出數目相同於被所準備之各攪拌子單元235輸出之各變換規則攪拌處理之攪拌子單元235之個數之輸出資料(中間輸出資料)之1個，藉此，即使在相同之攪拌單元中，固定於該攪拌單元之變換規則也可依輸入時之特定資訊而逐次變化，以實現更複雜之攪拌及解拌處理。也就是說，變換規則並非為攪拌單元所固有，而係可依輸入時之特定資訊而單一意義地加以固定。

在此，作為各攪拌子單元235，可利用上述第1或第2攪拌單元231、232之電路構成之第1~第6實施例之攪拌單元，或具有該等變換規則2種以上複合而成之變換規則之新攪拌單元所構成。

第7實施例係表示限定於使用於拌碼器電路230之第1或第2攪拌單元231、232之實施例，第8實施例係表示限定於使用於解拌器電路240之第3或第4攪拌單元232、231之實施

例。第1~第6實施例之攪拌單元係拌碼器電路230之第1或第2攪拌單元231、232、與解拌器電路240之第3或第4攪拌單元232、231等分別對應之攪拌單元彼此相同之攪拌單元，但在第7及第8實施例中，各使用之場所則受到固定。但，在拌碼器電路230與解拌器電路240之間對應之第7實施例之攪拌單元與第8實施例之攪拌單元中，被固定之變換規則卻相同。以下，說明各電路之詳細內容。

如圖9所示，第7實施例之攪拌單元係由多數攪拌子單元235、選擇電路236、依輸入時之特定資訊而產生選擇碼，且將其與該依輸入時之位址資料之位址值相關連地記憶於選擇碼儲存用之非揮發性記憶體260之碼產生電路237、及使碼產生電路237產生之多數選擇碼與多數攪拌子單元235個別地對應之查閱表238所構成。在此，非揮發性記憶體260因與後述第8實施例之攪拌單元所共有，故設置於攪拌單元外也無妨。

碼產生電路237依據輸入資料輸入時距離啟動時之經過時間資訊、位址資料之位址值，隨時利用隨機數等產生不同之選擇碼。又，產生之選擇碼最好事先限定於攪拌子單元235之個數份。但選擇碼數即使不等於攪拌子單元235之個數，只要查閱表238可執行上述對應，即無問題。碼產生電路237係將產生之選擇碼與當時之位址資料之位址值共同記憶於非揮發性記憶體260，或將產生之選擇碼與當時之位址資料之位址值儲存於以1比1對應之非揮發性記憶體260之位址區域。

查閱表238係產生指示選擇與碼產生電路237產生之選擇碼相對應之1個攪拌子單元235之選擇指示信號，選擇電路236選擇依據該選擇指示信號所選擇之來自攪拌子單元235之中間輸出資料，並將其輸出作為攪拌單元之輸出資料。

如圖10所示，第8實施例之攪拌單元係由多數攪拌子單元235、選擇電路236、依輸入資料輸入時之位址資料之位址值，由選擇碼儲存用之非揮發性記憶體260讀出選擇碼之碼讀出電路239、及使相同於第7實施例之攪拌單元數之多數選擇碼與多數攪拌子單元235個別地對應之查閱表238所構成。在此，非揮發性記憶體260因與第7實施例之攪拌單元所共有，故設置於攪拌單元外也無妨。

碼讀出電路239依據輸入資料輸入時之位址資料之位址值，由非揮發性記憶體260讀出與該位址值共同被記憶之選擇碼。或讀出記憶於與該位址值以1比1相對應之非揮發性記憶體260之位址區域之選擇碼。

查閱表238係產生指示選擇與碼讀出電路239讀出之選擇碼相對應之1個攪拌子單元235之選擇指示信號，選擇電路236選擇依據該選擇指示信號所選擇之來自攪拌子單元235之中間輸出資料，並將其輸出作為攪拌單元之輸出資料。

另外，在圖中並未予以顯示，即作為第1或第2攪拌單元231、232之電路構成之第9實施例，採用以下之構成方式也相當理想：即在1個攪拌單元231、232內設有多數例如任意選擇自上述第1~第8實施例之攪拌單元中之攪拌單元之攪拌子單元，並在內部將各攪拌子單元間連接所構成，以便

可對至少1個攪拌子單元，輸入第9實施例之攪拌單元之輸入資料，由至少1個攪拌子單元輸出第9實施例之攪拌單元之輸出資料，將其他至少1個攪拌子單元之輸出資料之全部或一部分輸入至至少1個攪拌子單元。利用此構成，可實現更複雜且多樣之攪拌處理。

圖11A及B係使用具體的數值表示拌碼器電路230與解拌器電路240之各處理流程。假設在此所使用之第1至第4攪拌單元231、232中，第1及第4攪拌單元231係使用圖4所示之第1實施例之構成，第2及第3攪拌單元232係使用圖5所示之第2實施例之構成。

首先，圖11A係表示攪拌處理之流程。對原來之資料"10011010"，使上位4位元"1001"在第1攪拌單元231施行向右移位1位元，結果成為"1100"。其次，在第1運算單元233取"1100"與原來之資料之下位4位元"1010"之互斥"或"時，結果成為"0110"。其次，施行在第2攪拌單元232鄰接此"0110"之2位元彼此之調換，結果成為"1001"。最後，在第2運算單元234取"1001"與"1001"之互斥"或"，結果成為"0000"。由以上，攪拌處理後之已處理資料為"01100000"。

其次，圖11B係表示解拌處理之流程。對已攪拌處理資料"01100000"，施行在第3(第2)攪拌單元232鄰接上位4位元"0110"之2位元彼此之調換，結果成為"1001"。其次，在第3運算單元233取"1001"與已攪拌處理資料之下位4位元"0000"之互斥"或"時，結果成為"1001"。其次，施行使此"1001"在第4(第1)攪拌單元231向右移位1位元，結果成為

"1100"。最後，在第4運算單元234取"1100"與已攪拌處理資料之上位4位元"0110"之互斥"或"，結果成為"1010"。由以上，攪拌處理後之資料為"10011010"，與攪拌處理前之原來資料一致。

其次，說明本發明之資料處理裝置之另一實施形態。

〈1〉在上述實施形態中，採用對n位元寬之匯流排，具有1個拌碼器電路220或230，對n位元寬之匯流排，具有1個解拌器電路240之構成，但也可採用對n位元寬之匯流排，具有2個以上之拌碼器電路220、230與2以上之解拌器電路240之構成。

圖12係表示將被處理資料M等分時之拌碼器電路230'之一例。此時，只要在每鄰接之2個資料區塊設置M/2個份之上述拌碼器電路即可。又，依照每1資料區塊對而改變各拌碼器電路230內之第1及第2攪拌單元231、232，即可更進一步提高安全性。

同樣地，圖13係表示將已攪拌處理資料M等分時之解拌器電路240'之一例。此時，也只要在每鄰接之2個資料區塊設置M/2個份之上述解拌器電路240即可。

〈2〉在上述實施形態中，係以CPU 200具有攪拌處理與解拌處理成對之拌碼器電路230與解拌器電路240之構成形態為例加以說明，但採用拌碼器電路230與解拌器電路240僅具有其中之一方之構成也無妨。又，解拌器電路240也可採用可對自己之拌碼器電路230以外之拌碼器電路所攪拌處理之已處理資料進行解碼處理之解拌器電路。又，此情形，

成對之攪拌處理與解拌處理需分散在2個以上之資料處理裝置中執行。

〈3〉圖14係表示將本發明之資料處理裝置適用於IC卡之情形之構成例。

IC卡110具有以CPU 200與外部資料匯流排600及外部位址匯流排700互相連接之ROM 300、RAM 400、非揮發性記憶體500等外部記憶體群，另外，並具有輔助運算器111、UART/IO 112與定時器113所構成。一般，IC卡要求安全性，故需在設計上下工夫。為防止攻擊者將目標特別鎖定於CPU及輔助運算器或內部資料匯流排位於晶片上之何處，採用不分離成各區塊，而在半導體積體電路上設計成整塊之方式。由於半導體製程之微細化，使得成為整塊之內部資料匯流排等受到探測等攻擊變成非常困難。因此，一般，攻擊者可能嘗試對CPU與記憶體間之資料匯流排等分離之區塊間之信號進行探測等。因此，對區塊間之外部資料匯流排600及各記憶體上之資料施以攪拌處理時，可提供具備安全性之IC卡。

又，作為本發明之應用，雖以IC卡加以說明，但本發明之也可廣泛地利用於處理個人資訊等機密資訊之機器及系統。

〈4〉圖1、圖2及圖14所例示之本發明之資料處理裝置係以將包含外部記憶體群等周邊區塊單晶片化成為半導體積體電路之例加以說明，但只要多數機能區塊以內部匯流排連接，並在內部匯流排與外部匯流排之匯流排介面部設置本

發明之拌碼器電路或解拌器電路，則資料處理裝置與周邊區塊未必需要單晶片化。

〈5〉在上述實施形態中，係假設拌碼器電路230及解拌器電路240所處理之資料為偶數位元，內部資料匯流排213及外部資料匯流排600等資料匯流排也為偶數位元，但匯流排寬為奇數位元之情形，也可僅使被處理資料之1位元由攪拌處理或解拌處理對象移位，或追加假的1位元使其成為偶數位元。

〈6〉在上述實施形態中，係假設拌碼器電路230及解拌器電路240所處理之資料為並行資料，但內部資料匯流排213及外部資料匯流排600等其中之一方或雙方使用串行匯流排也無妨。處理串行資料時，只要暫時對資料施以串行・並行變換後，再使用拌碼器電路230及解拌器電路240即可。又，處理對象之資料亦可為並行資料與串行資料並存。例如，在內部匯流排為8位元而外部匯流排為16位元之情形等，亦可採用將內部匯流排之8位元資料分2次讀入後，在拌碼器電路230施行攪拌處理而將16位元資料轉送至外部匯流排之形態。

如以上所詳述，依據本發明之拌碼器電路、解拌器電路及資料處理裝置，可在CPU內部施行資料之攪拌處理、解拌處理。即，僅被攪拌處理後之資料會經由資料匯流排信號被傳達至CPU外部，使被攪拌處理後之資料被儲存於連接於此匯流排之外部記憶體。因此，對於外部匯流排上之信號之探測及記憶體零件之剝離分析，也可獲得非常高之

資訊之機密性。另外，將位址匯流排信號也列為攪拌之對象，可使其分析更為困難。在拌碼器電路或解拌器電路之內部，不僅施行利用攪拌單元之信號之攪拌處理，且施行配合互斥"或"運算處理之安全處置(資料之隱藏化)，除可實現不會被解碼之極高安全性外，並可確實以邏輯方法復原原來之資料，故可提供資料之可靠性極高之資料處理裝置。

本發明雖透過實施形態加以記述，但鑑於精通此技術領域者在不脫離本發明之精神或範圍之情況下，仍能對此作種種模仿或變更，因此，本發明之範圍應依據後述申請專利範圍之項予以界定。

【圖式簡單說明】

圖1係表示具有本發明之拌碼器電路與解拌器電路之資料處理裝置之一實施形態之內部構成之一例之區塊構成圖。

圖2係表示具有本發明之拌碼器電路與解拌器電路之資料處理裝置之另一實施形態之內部構成之一例之區塊構成圖。

圖3A、B係表示本發明之拌碼器電路與解拌器電路之一實施形態之電路構成之區塊構成圖。

圖4係表示在本發明之拌碼器電路與解拌器電路所使用之攪拌單元之第1實施例之電路構成圖。

圖5係表示在本發明之拌碼器電路與解拌器電路所使用之攪拌單元之第2實施例之電路構成圖。

圖6係表示在本發明之拌碼器電路與解拌器電路所使用

之攪拌單元之第4實施例之電路構成圖。

圖7係表示在本發明之拌碼器電路與解拌器電路所使用之攪拌單元之第5實施例之電路構成圖。

圖8係表示在本發明之拌碼器電路與解拌器電路所使用之攪拌單元之第6實施例之電路構成圖。

圖9係表示在本發明之拌碼器電路所使用之攪拌單元之第7實施例之電路構成圖。

圖10係表示在本發明之解拌器電路所使用之攪拌單元之第8實施例之電路構成圖。

圖11A、B係表示在本發明之拌碼器電路與解拌器電路之資料處理流程之說明圖。

圖12係表示本發明之拌碼器電路之另一實施形態之區塊構成圖。

圖13係表示本發明之解拌器電路之另一實施形態之區塊構成圖。

圖14係表示本發明之IC卡之一實施形態之內部構成之一例之區塊構成圖。

圖15係以往公報所揭示之攪拌技術之說明圖。

【圖式代表符號說明】

10	CPU
11、21、31、41	匯流排加密電路
20	RAM
30	ROM
40	E ² PROM

50	匯流排線
60	時間控制電路
111	輔助運算器
112	UART/IO
113	定時器
211	快取記憶體
212	指令解碼器控制器
213	內部資料匯流排
214	暫存器群
215	資料匯流排控制電路
216	位址匯流排控制電路
220	第 2 加密電路
230	第 1 加密電路
236	選擇電路
237	碼產生電路
238	查閱表
239	碼讀出電路
240	解密電路
260	選擇碼儲存用記憶體
500	系統控制信號非揮發性記憶體
600	資料匯流排
700	位址匯流排

伍、中文發明摘要：

本發明之目的在於提供一種不被解釋記憶體內部或匯流排上之資訊之高安全性之資料處理裝置及可實現IC卡之拌碼器電路。拌碼器電路係被處理資料由2資料區塊(B1)、(B0)組成，已處理資料由2資料區塊(B1')、(B0')組成，且包含第1攪拌單元(231)，其係對資料區塊(B1)執行第1攪拌處理，輸出第1中間資料者；第1運算單元(233)，其係執行資料區塊(B0)與第1中間資料之互斥"或"運算，輸出資料區塊(B1')者；第2攪拌單元(232)，其係對資料區塊(B1')執行第2攪拌處理，輸出第2中間資料者；及第2運算單元(234)，其係執行第2中間資料與資料區塊(B1)之互斥"或"運算，輸出資料區塊(B0')者。

陸、英文發明摘要：

This invention is intended to provide a scrambler circuit capable of realizing a data processing device or an IC card having high security enough to prevent information in a memory or information on a bus from being decrypted. The scrambler circuit has to-be-processed data divided into two data blocks (B1 and B0) and processed data divided into two data blocks (B1' and B0'), and includes a first scrambler unit (231) that conducts first scrambling to the data block (B1) and that outputs first intermediate data, a first arithmetic unit (233) that performs an exclusive OR operation between the data block (B0) and the first intermediate data and that outputs the data block (B1'), a second scrambler unit (232) that conducts second scrambling to the data block (B1') and that outputs second intermediate data, and a second arithmetic unit (234) that performs an exclusive OR operation between the second intermediate data and the data block (B1) and that outputs the data block (B0').

拾、申請專利範圍：

1. 一種拌碼器電路，其係利用特定之攪拌處理將4位元以上之被處理資料變換成同位元數之已處理資料者；且

前述被處理資料係分割成2位元以上之第1資料區塊與和與前述第1資料區塊同位元數之第2資料區塊所構成，且前述已處理資料係分割成分別和前述第1資料區塊同位元數之第3資料區塊與第4資料區塊所構成；

前述拌碼器電路包含：

第1攪拌單元，其係對前述第1資料區塊執行特定之第1攪拌處理，輸出同位元數之第1中間資料者；

第1運算單元，其係執行前述第2資料區塊與前述第1中間資料之各位元之互斥"或"運算，輸出前述第3資料區塊者；

第2攪拌單元，其係對前述第3資料區塊執行與前述第1攪拌處理相同或相異之第2攪拌處理，輸出同位元數之第2中間資料者；及

第2運算單元，其係執行前述第2中間資料與前述第1資料區塊之各位元之互斥"或"運算，輸出前述第4資料區塊者。

2. 如申請專利範圍第1項之拌碼器電路，其中

前述攪拌單元係將輸入資料值，依據固定於該攪拌單元之變換規則變換成唯一決定之輸出資料值者。

3. 如申請專利範圍第2項之拌碼器電路，其中

前述第1或第2攪拌單元係換接對應於輸入資料之各位

元之多數輸入端子與對應於輸出資料之各位元之輸出端子間之配線之一部分或全部所構成，且藉前述配線之換接，固定前述變換規則者。

4. 如申請專利範圍第3項之拌碼器電路，其中

前述第1或第2攪拌單元係藉前述配線之換接，對前述輸入資料執行1位元或2位元以上之循環移位操作者。

5. 如申請專利範圍第3項之拌碼器電路，其中

前述第1或第2攪拌單元係藉前述配線之換接，對前述輸入資料之特定之2位元執行更換操作者。

6. 如申請專利範圍第3項之拌碼器電路，其中

前述第1或第2攪拌單元係藉前述配線之換接，組合地執行對前述輸入資料之1位元或2位元以上之循環移位操作與對特定之2位元之更換操作者。

7. 如申請專利範圍第2項之拌碼器電路，其中

前述第1或第2攪拌單元具有對輸入資料之一部分或全部之位元施以特定之邏輯運算之邏輯運算電路，藉前述邏輯運算電路固定前述變換規則者。

8. 如申請專利範圍第7項之拌碼器電路，其中

前述邏輯運算電路係對前述輸入資料之一部分或全部之位元，施行2位元以上之邏輯運算者。

9. 如申請專利範圍第2項之拌碼器電路，其中

前述第1或第2攪拌單元具有對輸入資料之一部分或全部之位元與前述輸入資料輸入時之位址資料之一部分或全部之位元施以特定之邏輯運算之邏輯運算電路，藉前

述邏輯運算電路，以按照前述位址資料之位址值而唯一決定之方式固定前述變換規則者。

10. 如申請專利範圍第2項之拌碼器電路，其中

前述第1或第2攪拌單元具有對輸入資料之一部分或全部之位元與保持於特定之非揮發性記憶體之變換規則固定用資料，施行特定之邏輯運算之邏輯運算電路，藉前述邏輯運算電路，以按照前述變換規則固定用資料之資料值而唯一決定之方式固定前述變換規則者。

11. 如申請專利範圍第2項之拌碼器電路，其中

前述第1或第2攪拌單元具備選擇電路，其係依據將輸入資料變換成基於被預先固定之變換規則而唯一決定之輸出資料之攪拌子單元之前述變換規則相異之多數與按照前述輸入資料輸入時之特定資訊而變化之變換規則，選擇並輸出相同輸入資料輸入後之前述多數攪拌子單元之輸出資料之1者；且依照基於前述選擇規則所選擇之前述攪拌子單元，以唯一決定之方式固定固定於該攪拌單元之前述變換規則者。

12. 如申請專利範圍第11項之拌碼器電路，其中

包含前述多數攪拌子單元之前述攪拌子單元係包含碼產生電路，其係依照前述輸入資料輸入於前述多數攪拌子單元時之特定資訊而產生選擇碼，且與前述輸入時之位址資料相關連地記憶於特定之非揮發性記憶體者；及查閱表，其係個別地使前述選擇碼與前述多數攪拌子單元相對應者；

前述選擇電路係由前述碼產生電路產生之前述選擇碼與依據前述查閱表所決定之前述多數攪拌子單元中之1選擇前述輸出資料者。

13. 一種解拌器電路，其係利用特定之解拌處理將4位元以上之已攪拌處理資料逆變換成同位元數之處理前資料者；且

前述已攪拌處理資料係分割成2位元以上之第5資料區塊與和前述第5資料區塊同位元數之第6資料區塊所構成，且前述處理前資料係分割成分別和前述第5資料區塊同位元數之第7資料區塊與第8資料區塊所構成；

前述解拌器電路包含：

第3攪拌單元，其係對前述第5資料區塊執行特定之第3攪拌處理，輸出同位元數之第3中間資料者；

第3運算單元，其係執行前述第6資料區塊與前述第3中間資料之各位元之互斥"或"運算，輸出前述第7資料區塊者；

第4攪拌單元，其係對前述第7資料區塊執行與前述第3攪拌處理相同或相異之第4攪拌處理，輸出同位元數之第4中間資料者；及

第4運算單元，其係執行前述第4中間資料與前述第5資料區塊之各位元之互斥"或"運算，輸出前述第8資料區塊者。

14. 如申請專利範圍第13項之解拌器電路，其中

前述攪拌單元係將輸入資料值，依據固定於該攪拌單元之變換規則變換成唯一決定之輸出資料值者。

15. 如申請專利範圍第13項之解拌器電路，其中

前述第3或第4攪拌單元係換接對應於輸入資料之各位元之多數輸入端子與對應於輸出資料之各位元之輸出端子間之配線之一部分或全部所構成，且藉前述配線之換接，固定前述變換規則者。

16. 如申請專利範圍第15項之解拌器電路，其中

前述第3或第4攪拌單元係藉前述配線之換接，對前述輸入資料執行1位元或2位元以上之循環移位操作者。

17. 如申請專利範圍第15項之解拌器電路，其中

前述第3或第4攪拌單元係藉前述配線之換接，對前述輸入資料之特定之2位元執行更換操作者。

18. 如申請專利範圍第15項之解拌器電路，其中

前述第3或第4攪拌單元係藉前述配線之換接，組合地執行對前述輸入資料之1位元或2位元以上之循環移位操作與對特定之2位元之更換操作者。

19. 如申請專利範圍第14項之解拌器電路，其中

前述第3或第4攪拌單元具有對輸入資料之一部分或全部之位元施以特定之邏輯運算之邏輯運算電路，藉前述邏輯運算電路固定前述變換規則者。

20. 如申請專利範圍第19項之解拌器電路，其中

前述邏輯運算電路係對前述輸入資料之一部分或全部之位元，施行2位元以上之邏輯運算者。

21. 如申請專利範圍第14項之解拌器電路，其中

前述第3或第4攪拌單元具有對輸入資料之一部分或全

部之位元與前述輸入資料輸入時之位址資料之一部分或全部之位元施以特定之邏輯運算之邏輯運算電路，藉前述邏輯運算電路，以按照前述位址資料之位址值而唯一決定之方式固定前述變換規則者。

22. 如申請專利範圍第14項之解拌器電路，其中

前述第3或第4攪拌單元具有對輸入資料之一部分或全部之位元與保持於特定之非揮發性記憶體之變換規則固定用資料，施行特定之邏輯運算之邏輯運算電路，藉前述邏輯運算電路，以按照前述變換規則固定用資料之資料值而唯一決定之方式固定前述變換規則者。

23. 如申請專利範圍第14項之解拌器電路，其中

前述第3或第4攪拌單元具備選擇電路，其係依據將輸入資料變換成基於被預先固定之變換規則而唯一決定之輸出資料之攪拌子單元之前述變換規則相異之多數與按照前述輸入資料輸入時之特定資訊而變化之變換規則，選擇並輸出相同輸入資料輸入後之前述多數攪拌子單元之輸出資料之1者；且依照基於前述選擇規則所選擇之前述攪拌子單元，以唯一決定之方式固定於該攪拌單元之前述變換規則者。

24. 如申請專利範圍第23項之解拌器電路，其中

包含前述多數攪拌子單元之前述攪拌子單元係包含碼讀出電路，其係依照前述輸入資料輸入於前述多數攪拌子單元時之位址資料而讀出記憶於特定之非揮發性記憶體之選擇碼者；及查閱表，其係個別地使前述選擇碼與

前述多數攪拌子單元相對應者；

前述選擇電路係由前述碼讀出電路讀出之前述選擇碼與依據前述查閱表所決定之前述多數攪拌子單元中之1選擇前述輸出資料者。

25. 一種資料處理裝置，其係

以內部匯流排連接多數機能區塊；

在前述內部匯流排與外部匯流排之第1匯流排介面部設置申請專利範圍第1項之拌碼器電路；

前述拌碼器電路係輸入前述內部匯流排上之一部分或全部之資料作為前述被處理資料，輸出前述外部匯流排上之一部分或全部之資料作為前述已處理資料者。

26. 如申請專利範圍第25項之資料處理裝置，其中

將前述內部匯流排與前述外部匯流排分割成多數區塊，在前述各區塊設置前述拌碼器電路者。

27. 一種資料處理裝置，其係

以內部匯流排連接多數機能區塊；

在前述內部匯流排與外部匯流排之第2匯流排介面部設置申請專利範圍第13項之解拌器電路；

前述解拌器電路係輸入前述外部匯流排上之一部分或全部之資料作為前述已攪拌處理資料，輸出前述內部匯流排上之一部分或全部之資料作為逆變換後之前述處理前資料者。

28. 如申請專利範圍第25項之資料處理裝置，其中

在前述內部匯流排與外部匯流排之第2匯流排介面部

設置申請專利範圍第13項之解拌器電路；

前述解拌器電路係輸入前述外部匯流排上之一部分或全部之資料作為前述已攪拌處理資料，輸出前述內部匯流排上之一部分或全部之資料作為逆變換後之前述處理前資料者。

29. 如申請專利範圍第28項之資料處理裝置，其中

前述拌碼器電路之前述第1攪拌單元與前述解拌器電路之前述第4攪拌單元施行依據相同變換規則之相同攪拌處理，前述拌碼器電路之前述第2攪拌單元與前述解拌器電路之前述第3攪拌單元施行依據相同變換規則之相同攪拌處理者。

30. 如申請專利範圍第27項之資料處理裝置，其中

將前述內部匯流排與前述外部匯流排分割成多數區塊，在前述各區塊設置前述拌碼器電路者。

31. 如申請專利範圍第25項之資料處理裝置，其中

前述內部匯流排與前述外部匯流排係資料匯流排者。

32. 如申請專利範圍第25項之資料處理裝置，其中

以第2內部匯流排連接前述多數機能區塊所構成；

在前述第2內部匯流排與第2外部匯流排之第3匯流排介面部設置申請專利範圍第1項之拌碼器電路；

前述拌碼器電路係輸入前述第2內部匯流排上之一部分或全部之資料作為前述被處理資料，輸出前述第2外部匯流排上之一部分或全部之資料作為前述已處理資料者。

33. 如申請專利範圍第32項之資料處理裝置，其中

將前述第2內部匯流排與前述第2外部匯流排分割成多數區塊，在前述各區塊設置前述拌碼器電路者。

34. 如申請專利範圍第32項之資料處理裝置，其中

前述第2內部匯流排與前述第2外部匯流排係位址匯流排者。

35. 如申請專利範圍第25項之資料處理裝置，其中

前述多數機能區塊及前述匯流排介面部係以形成於同一半導體基板上之半導體積體電路構成者。

36. 如申請專利範圍第35項之資料處理裝置，其中

作為前述機能區塊，包含算術邏輯運算器，具有作為控制前述內部匯流排與前述外部匯流排之單晶片微電腦之機能者。

37. 一種IC卡，其係

將申請專利範圍第36項之資料處理裝置使用作為系統控制用之單晶片微電腦者。

拾壹、圖式：

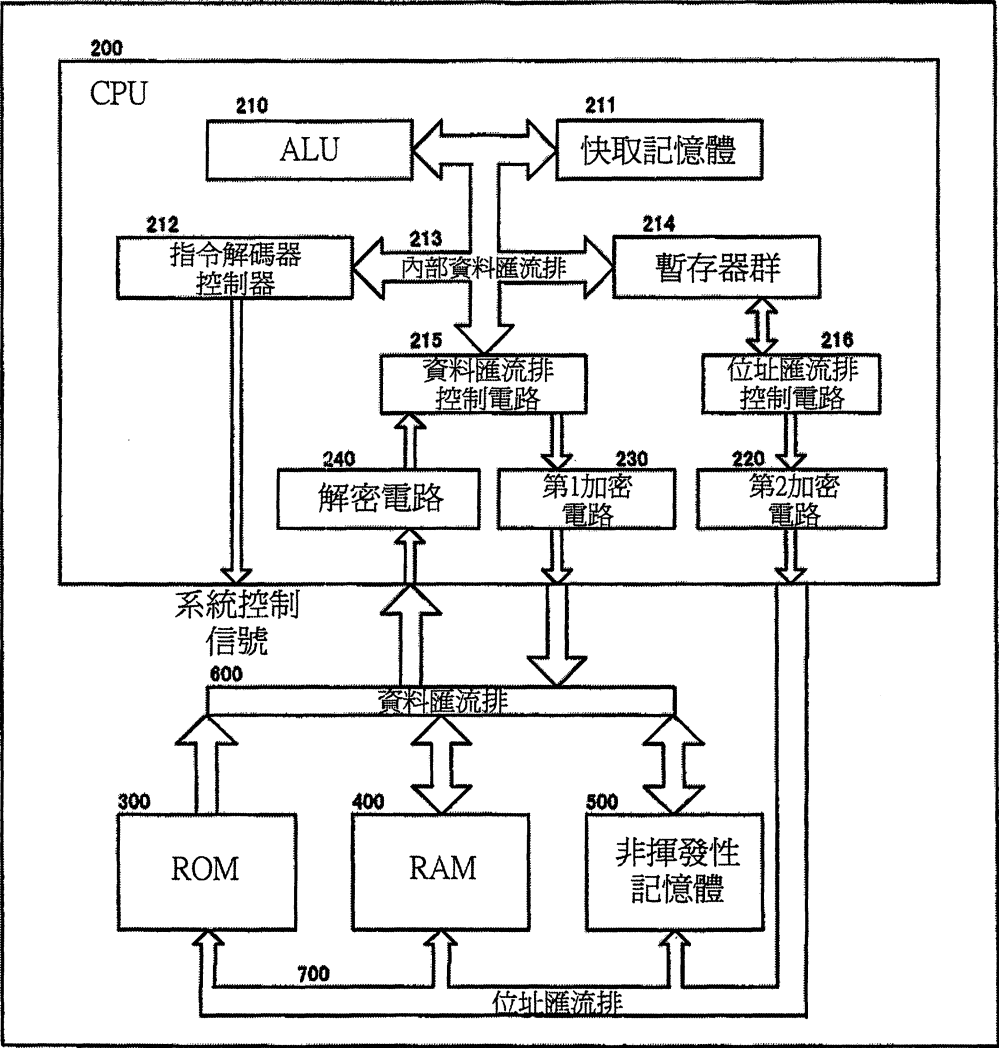


圖 1

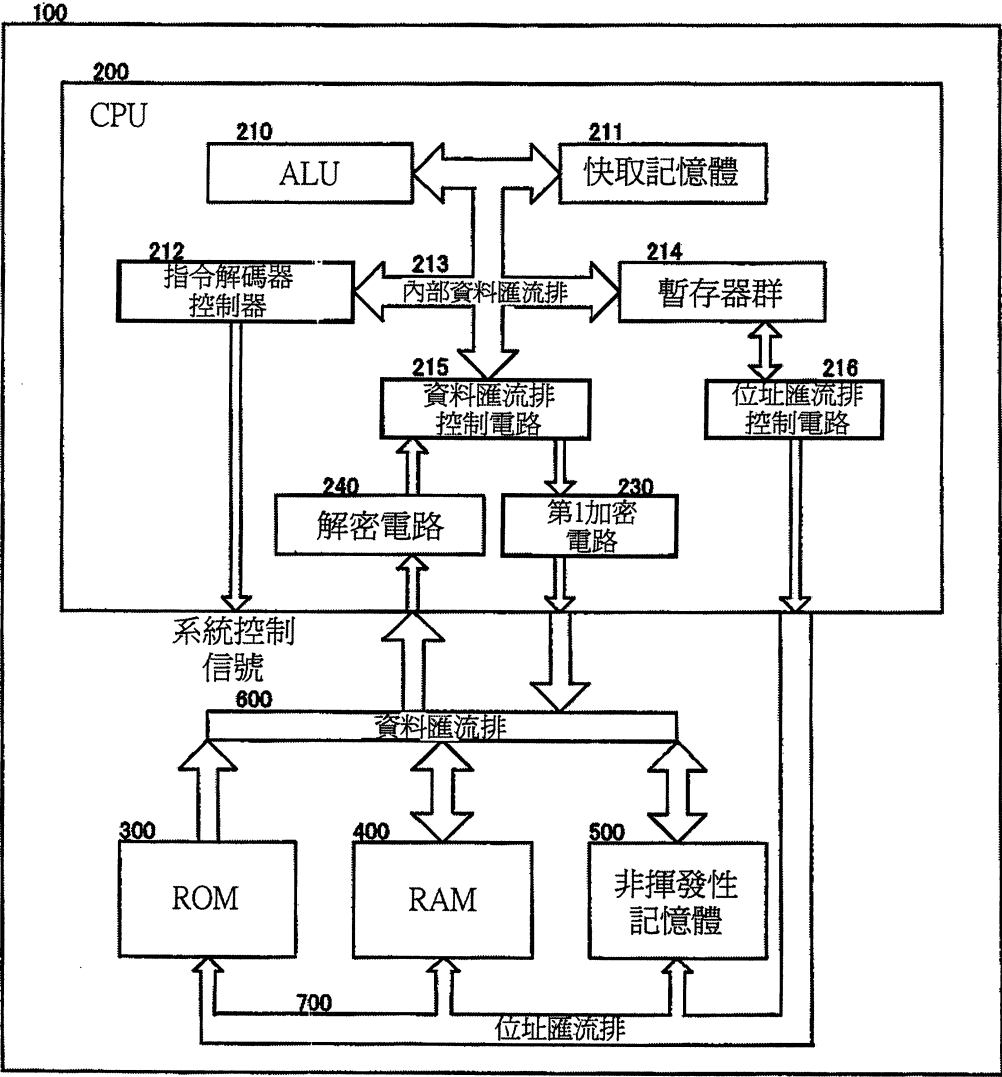


圖 2

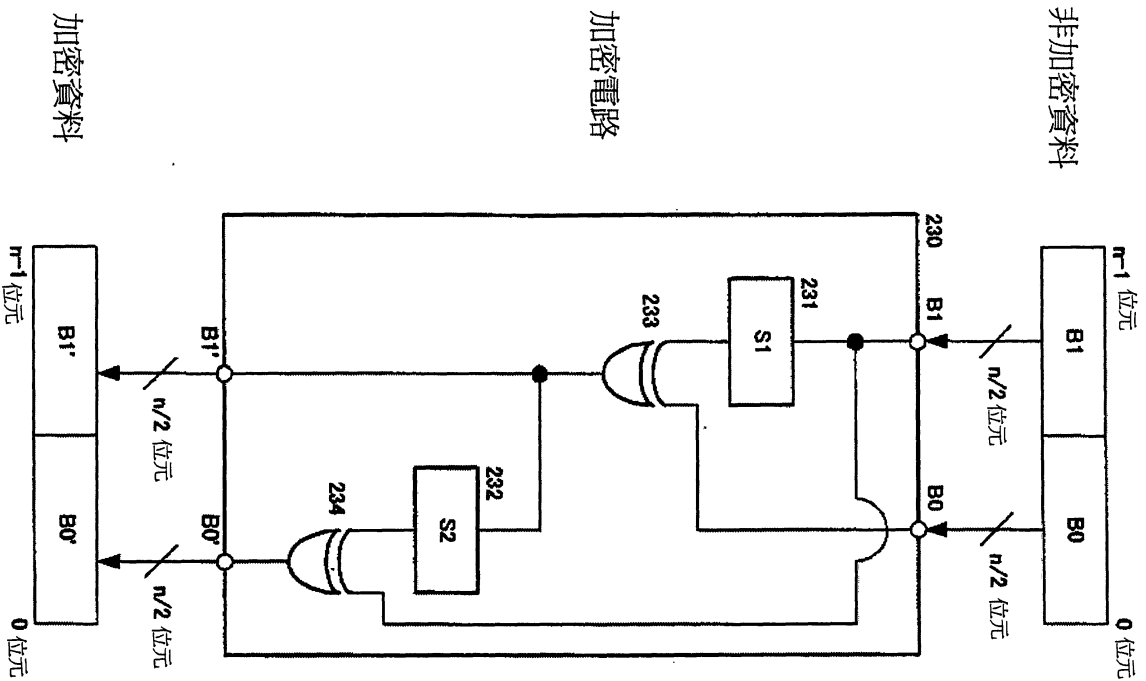


圖 3 A

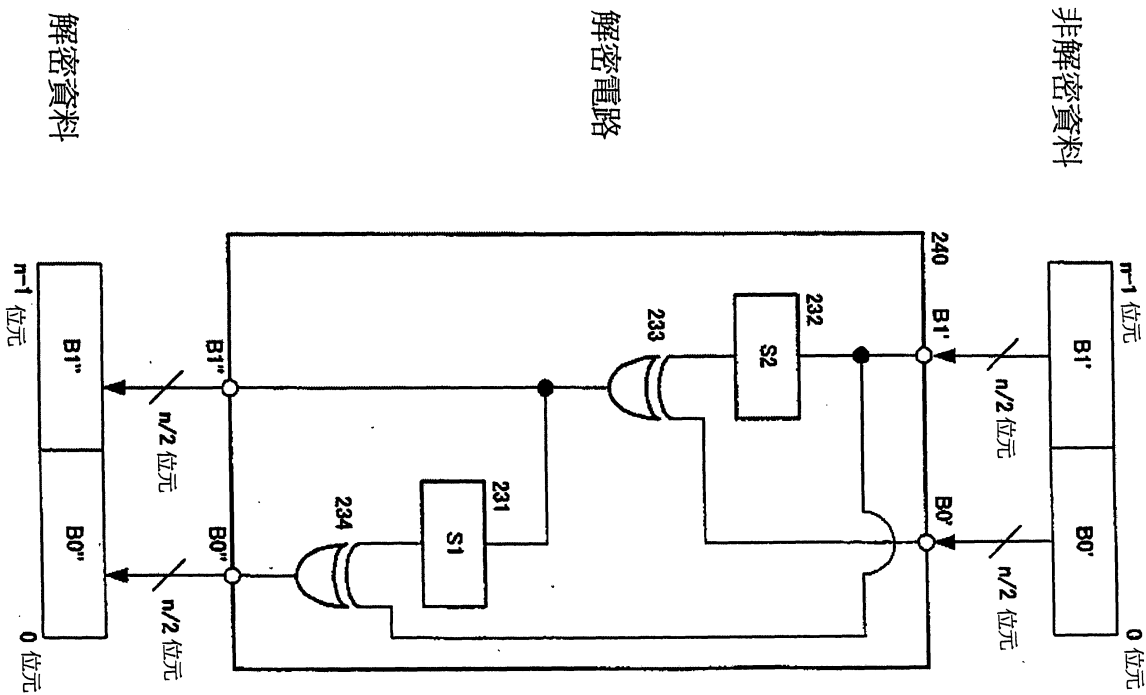
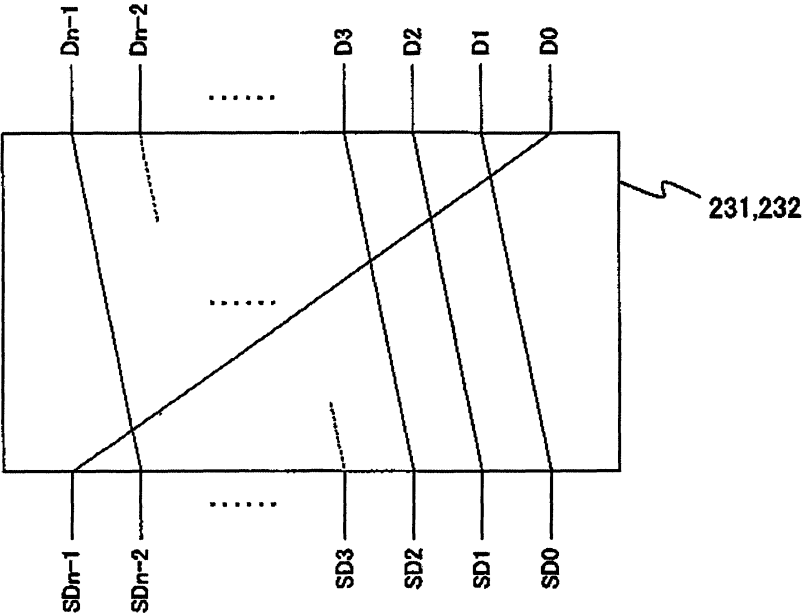
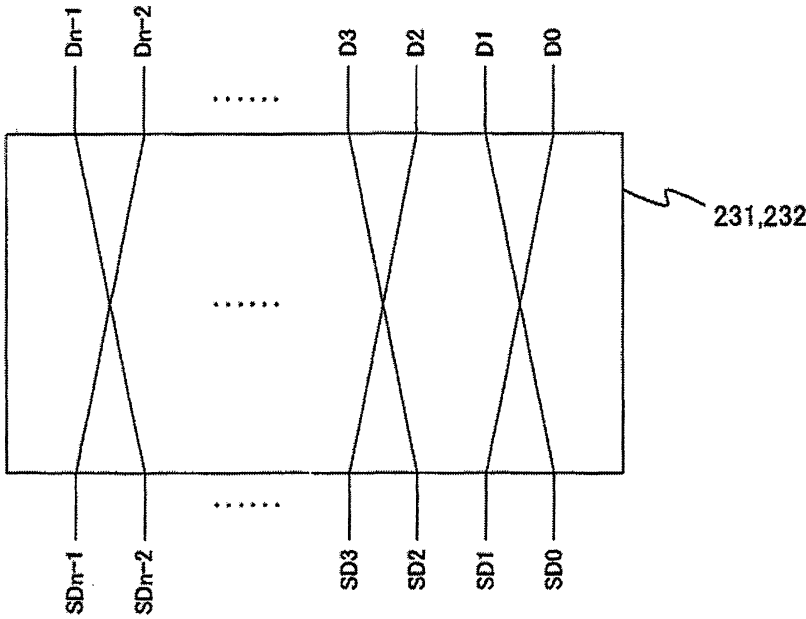


圖 3 B



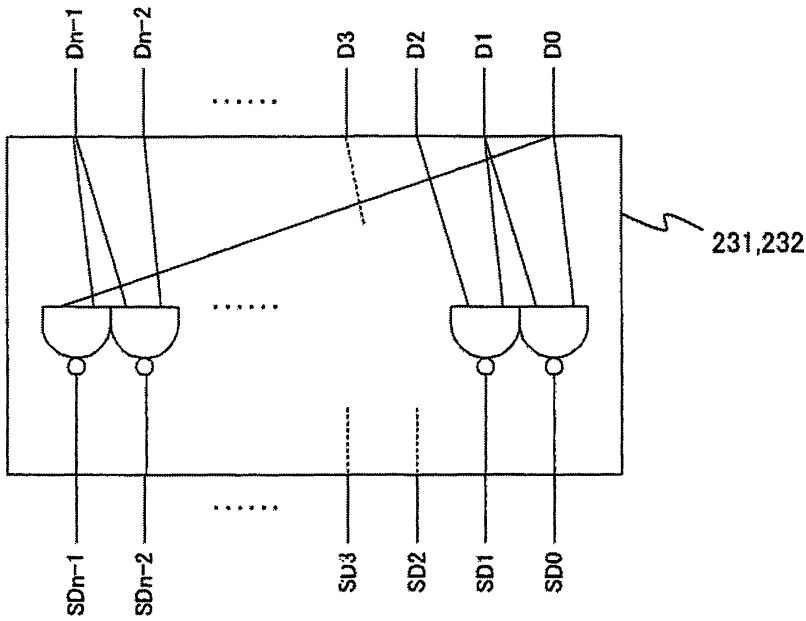
向右移位1位元

圖 4



各相鄰之2位元
彼此調換

圖 5



在相鄰之2位元間
施行 nand ("與") 運算

圖 6

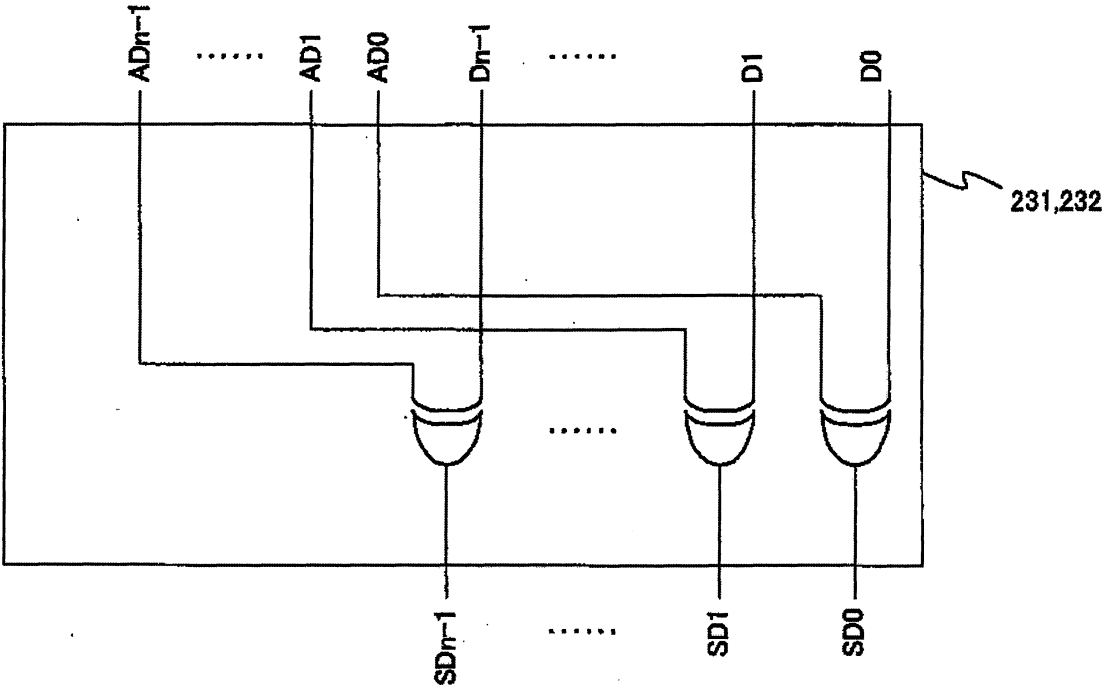


圖 7

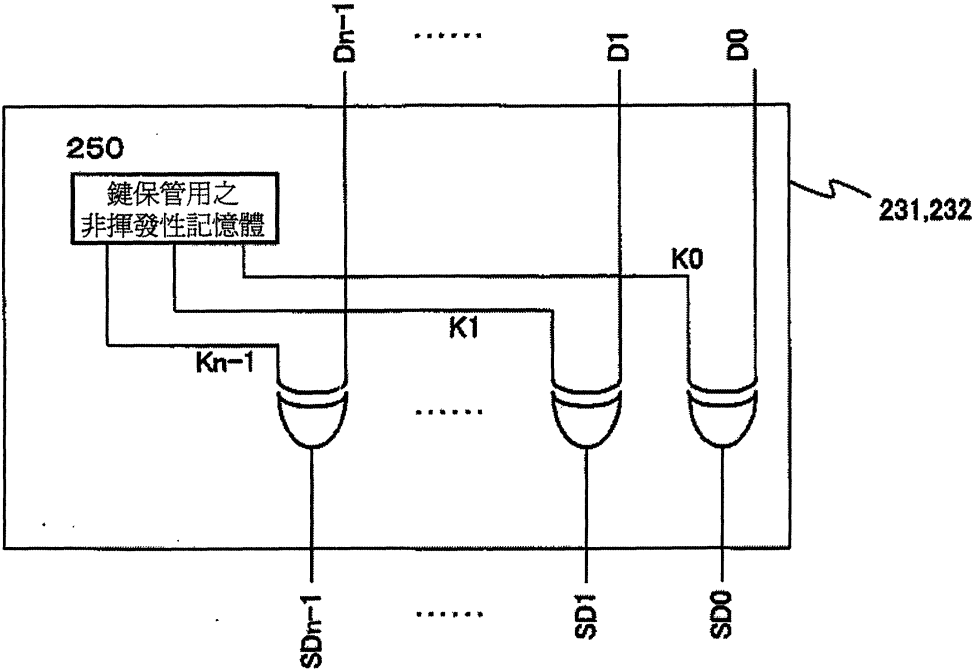


圖 8

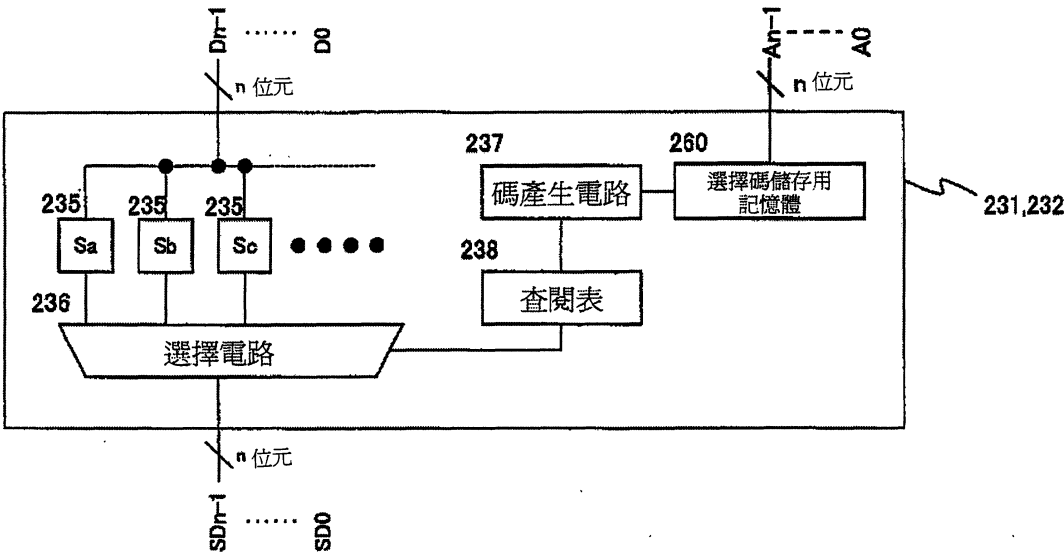


圖 9

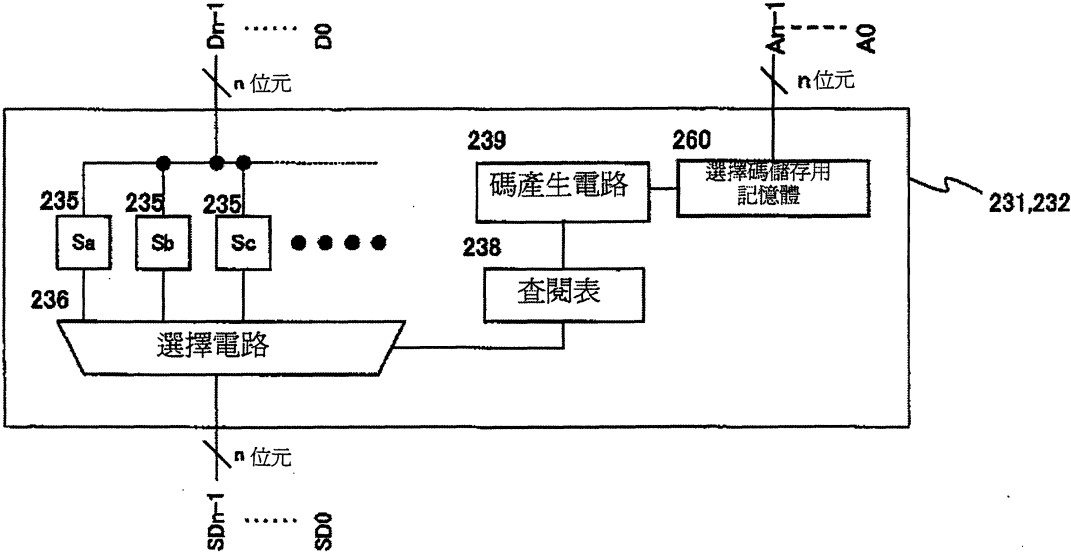


圖 10

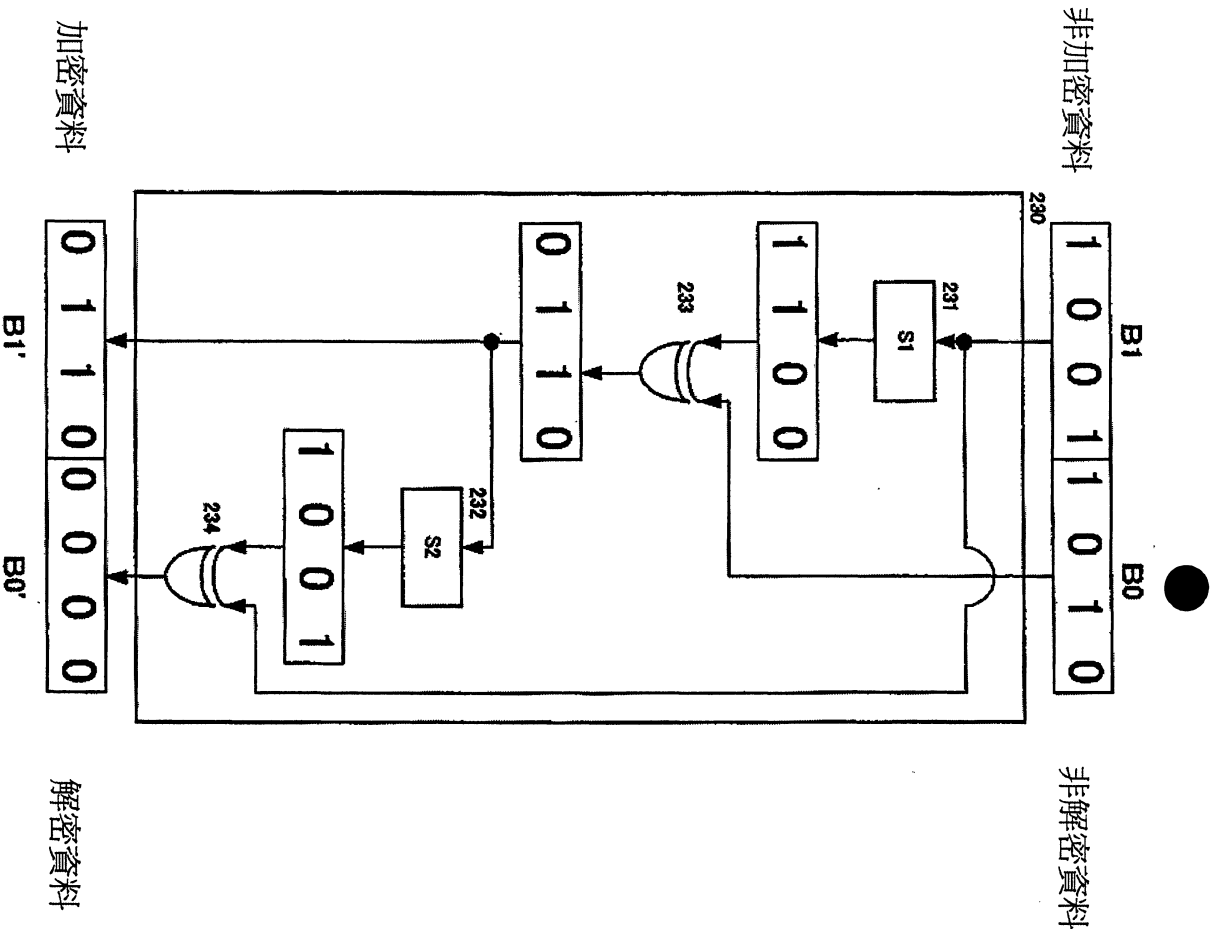


圖 11A

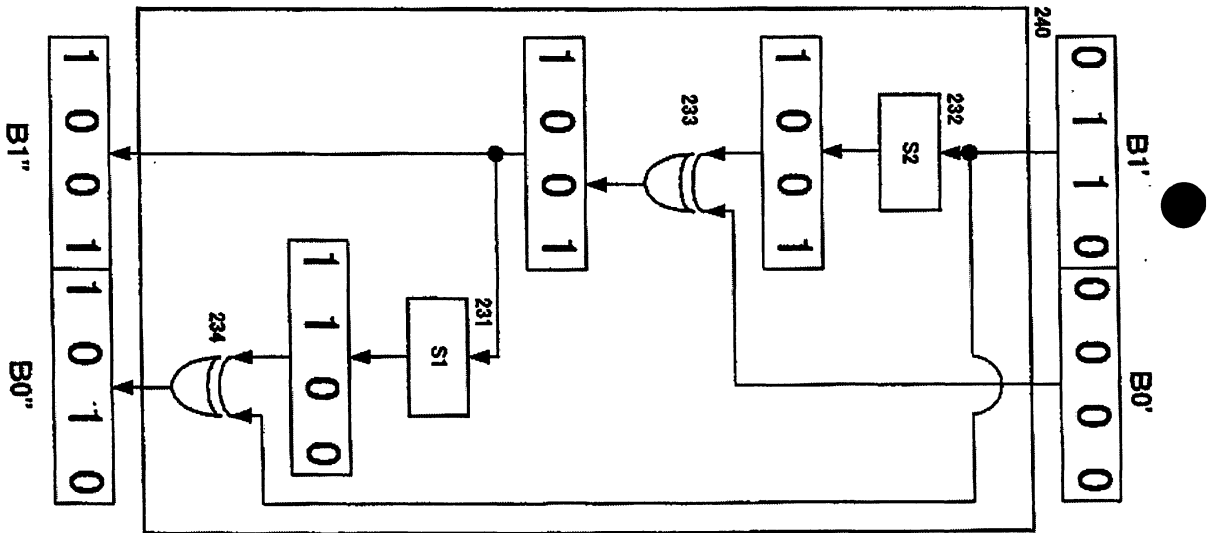


圖 11B

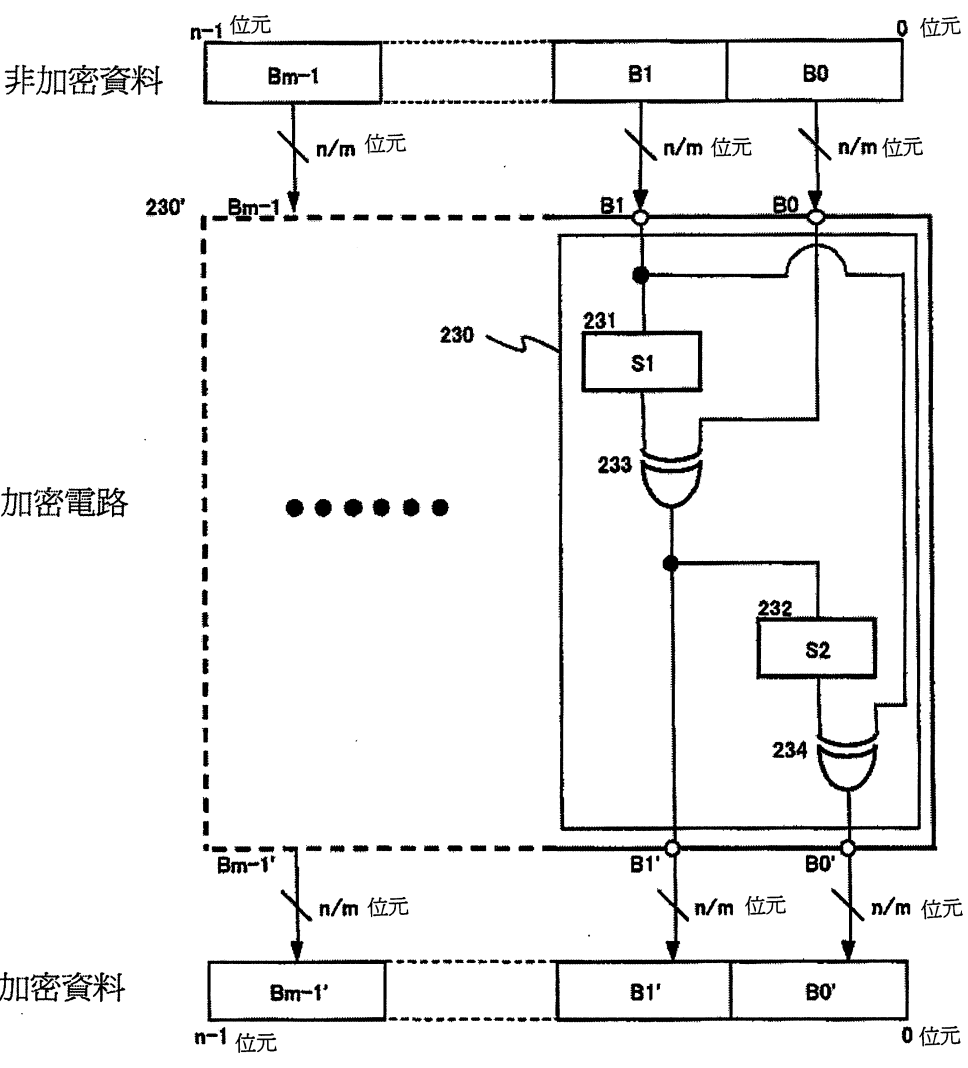


圖 12

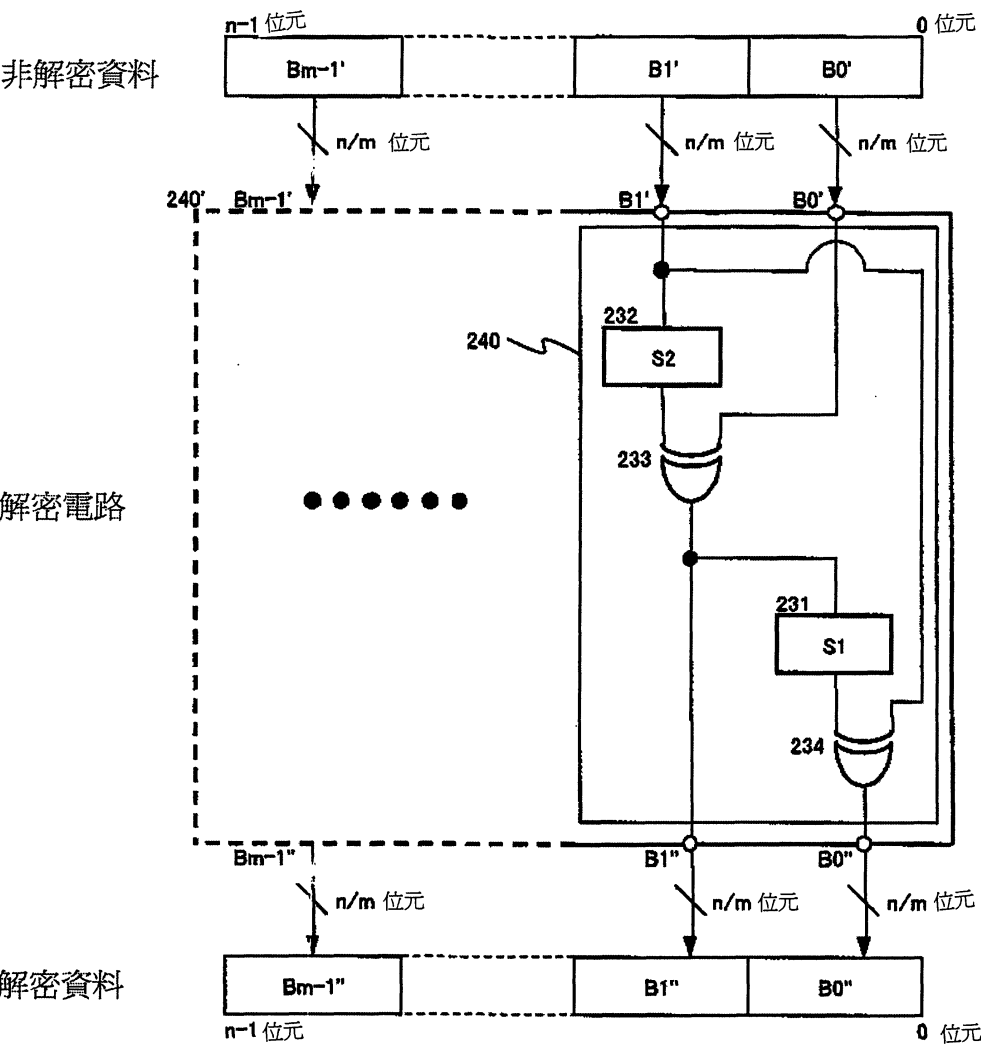


圖 13

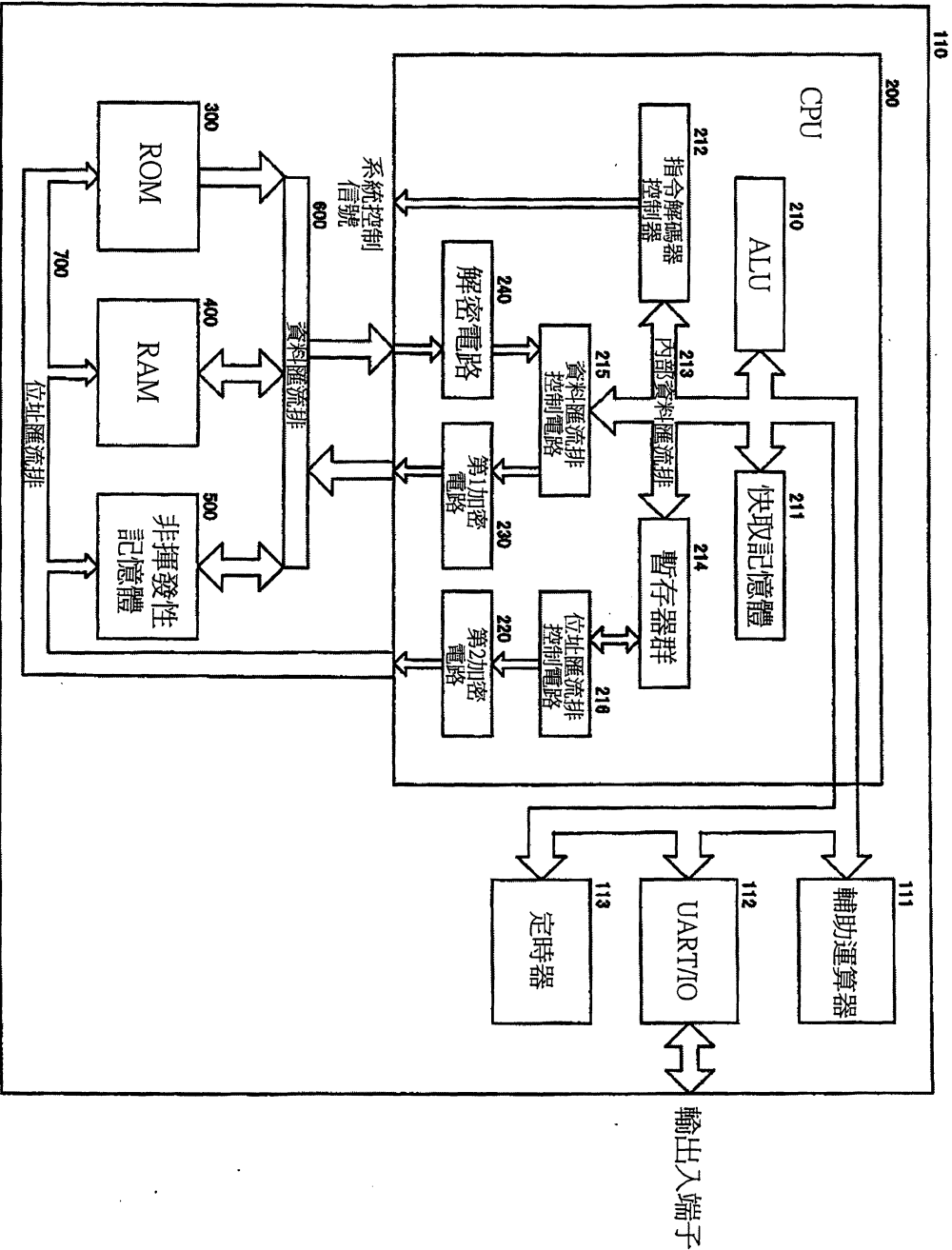


圖 14

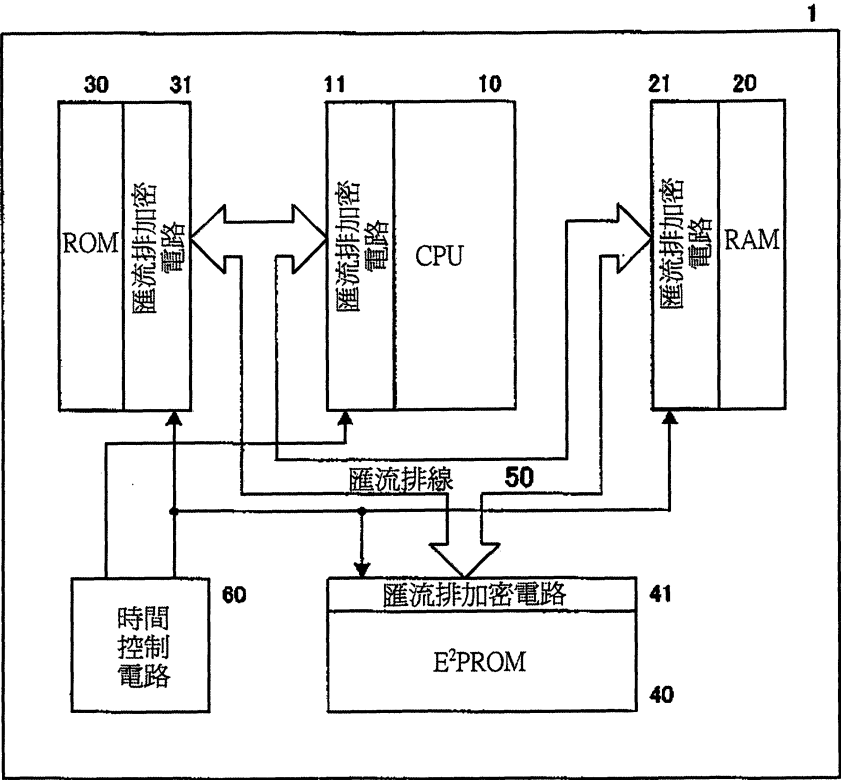


圖 15 先前技術

柒、指定代表圖：

(一)本案指定代表圖為：第 (3) 圖。

(二)本代表圖之元件代表符號簡單說明：

230 第1拌碼器電路

231 第1攪拌單元

232 第2攪拌單元

233 第1運算單元

234 第2運算單元

240 解拌器電路

捌、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

(無)