三、發明人：(共 4 人)

姓　名：(中文/英文)

1. 涉谷　香士
SHIBUTANI, KYOJI

2. 白井　太三
SHIRAI, TAIZO

3. 秋下　徹
AKISHITA, TORU

4. 盛合　志帆
MORIAI, SHIHO

國　籍：(中文/英文)

1. 日本　JAPAN

2. 日本　JAPAN

3. 日本　JAPAN

4. 日本　JAPAN

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. 日本；2006年09月01日；特願2006-238226

2.

☐ 無主張專利法第二十七條第一項國際優先權：

1.

2.

☐ 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】

本發明係關於一種密碼處理裝置、密碼處理方法、以及電腦程式。更詳細而言，關於一種執行Feistel型公用密鑰區塊密碼處理之密碼處理裝置、密碼處理方法、以及電腦程式。

【先前技術】

最近，隨著網路通信、電子商務貿易發展，通信中確保安全成為重要問題。確保安全之一個方法為密碼技術，目前，現實中實施有使用各種密碼化方法之通信。

例如下述系統正得到應用，其於IC卡等小型裝置中嵌入密碼處理模組，於IC卡與作為資料讀取寫入裝置之讀寫器之間進行資料之收發，並進行識別處理、或者收發資料之密碼化、解密。

密碼處理演算法中存在各種類型，對其大致分類，則可分類為將密碼化密鑰與解密密鑰設為相異之密鑰例如公開密鑰與私密密鑰的公開密鑰密碼方式，及將密碼化密鑰與解密密鑰設為公用密鑰的公用密鑰密碼方式。

公用密鑰密碼方式中亦存在各種演算法，而其中之一方式如下所述，以公用密鑰為基礎生成複數密鑰，使用所生成之複數密鑰，重複執行區塊單元(64位元、128位元等)之資料轉換處理。應用上述密鑰生成方式與資料轉換處理之演算法的具有代表性者為公用密鑰區塊密碼方式。

作為代表性之公用密鑰區塊密碼之演算法，例如眾所周

知有過去之作為美國標準密碼之DES(Data Encryption Standard，資料加密標準)演算法，目前之作為美國標準加密之AES(Advanced Encryption Standard，高級加密標準)演算法等。

如此公用密鑰區塊密碼之演算法，主要由具有重複執行輸入資料轉換之F函數部的回合函數部，及生成回合函數部之各回合中F函數部中 所應用之回合密鑰的密鑰排程部構成。密鑰排程部根據作為私密密鑰之萬能密鑰(主密鑰)，首先生成增加位元數之擴展密鑰，並根據生成之擴展密鑰，生成回合函數部之各回合中F函數部中所應用之回合密鑰(副密鑰)。

作為執行應用如此回合函數(F函數)之演算法的具體結構，眾所周知有Feistel結構。Feistel結構，具有藉由作為資料轉換函數之回合函數(F函數)之簡單重複，將明文轉換為密文之結構。對應用Feistel結構之密碼處理進行揭示之文獻例如有非專利文獻1、非專利文獻2。

然而，作為應用該Feistel結構之公用密鑰區塊密碼處理的問題點，存在密碼分析造成之密鑰洩漏。作為密碼分析或攻擊方法之代表性方法，眾所周知有藉由分析複數具有一定差分之輸入資料(明文)與其輸出資料(密文)，而分析各回合函數中之應用密鑰的差分分析(亦稱差分解讀法或差分攻擊)，或根據明文與對應密文進行分析的線性分析(亦稱線性解讀法或線性攻擊)。

密碼分析易於進行密鑰分析，會導致其密碼處理之安全

性較低。於習知之密碼演算法中，回合函數(F函數)部之線性轉換部中應用之處理(轉換矩陣)在各段之回合中相等，因此易於進行分析，結果招緻密鑰分析之容易性。

作為應對上述問題之構成，提出有Feistel結構之回合函數(F函數)部之線性轉換部中，以每個回合進行切換之方式配置兩個以上不同矩陣的構成。該技術稱為擴散矩陣切換機構(DSM：Diffusion Switching Mechanism，以下DSM)。藉由該DSM，可提高對於差分攻擊或線性攻擊之耐受性。關於應用該擴散矩陣切換機構(DSM)之密碼處理構成，例如揭示於專利文獻1。

然而，執行應用擴散矩陣切換機構(DSM)之密碼處理之情形時，必須裝設設定有不同矩陣之不同回合函數(F函數)，又，必須預先製定複數回合函數，並依據序列進行切換，故必須設置新的控制機構，構成密碼處理裝置之情形時，所需構成將會增多，故將阻礙裝置小型化，造成成本上升。又，存在隨著切換控制會使處理速度下降之問題。

[專利文獻1]日本專利特開2006-72054號

[非專利文獻1] K. Nyberg, "Generalized Feistel networks", ASIACRYPT'96, SpringerVerlag, 1996, pp.91-104。

[非專利文獻2] Yuliang Zheng, Tsutomu Matsumoto, Hideki Imai: On the Construction of Block Ciphers Provably Secure and Not Relying on Any Unproved

Hypotheses. CRYPTO 1989: 461-480

【發明內容】

[發明所欲解決之問題]

本發明係鑒於上述問題點所完成者，其目的在於提供一種密碼處理裝置、密碼處理方法、以及電腦程式，上述者係將應用有擴散矩陣切換機構(DSM)之密碼處理構成加以改良，使裝設成本不致上升，便可執行高速之密碼處理，而上述擴散矩陣切換機構(DSM)係Feistel結構之回合函數(F函數)部之線性轉換部中，以每個回合進行切換之方式配置兩個以上不同矩陣。

[解決問題之技術手段]

本發明之第一態樣係一種密碼處理裝置，其特徵在於：其係執行Feistel型公用密鑰區塊密碼處理者，且包含：

資料處理部，其係選擇性應用至少兩種以上不同F函數作為回合函數，執行複數回合之回合運算；及

記憶體，其儲存有複數F函數對應表，該等F函數對應表係將對應於上述兩種以上不同F函數各個的輸入值與輸出值或中間值賦予對應；

上述資料處理部係下述結構：

依據預先規定之密碼處理序列，取得與各回合中應用之F函數對應的F函數對應表之存取用位址，並藉由應用取得位址之記憶體存取，讀取對應於各回合F函數的F函數對應表，根據表格參照，取得相對於輸入值之輸出值或中間值，獲得依據各F函數之資料轉換結果。

再者，於本發明之密碼處理裝置之一實施態樣中，其中上述資料處理部係下述結構：執行依據具有擴散矩陣切換機構(DSM：Diffusion Switching Mechanism)的Feistel結構之密碼處理，上述擴散矩陣切換機構係選擇性應用設定有至少2個以上不同矩陣作為各回合F函數中應用於線性轉換處理的轉換矩陣之至少2個以上不同F函數。

再者，於本發明之密碼處理裝置之一實施態樣中，其中上述資料處理部係下述結構：執行基於Feistel結構之密碼處理，上述Feistel結構係依據將密碼處理對象資料2分割之資料序列數(分割數)d=2之設定，執行密碼處理。

再者，於本發明之密碼處理裝置之一實施態樣中，其中上述資料處理部係下述結構：執行基於擴展型Feistel結構之密碼處理，上述擴展型Feistel結構係依據將密碼處理對象資料分割為3個以上之資料序列數(分割數)d≧3之設定，執行密碼處理。

再者，於本發明之密碼處理裝置之一實施態樣中，其中上述資料處理部係下述結構：執行預先設定之密碼函數，並於執行該密碼函數時，各回合適當地切換與各回合中應用之F函數對應的F函數對應表之存取用位址，讀取對應於各回合F函數的F函數對應表，並根據表格參照，取得相對於輸入值之輸出值或中間值，獲得依據各F函數之資料轉換結果。

再者，於本發明之密碼處理裝置之一實施態樣中，其中上述記憶體係下述結構：儲存有將相對於各F函數之輸入

值或輸入值之構成資料、及F函數之輸出值或中間值或該等構成資料賦予對應之F函數對應表。

再者，本發明之第二態樣係一種密碼處理方法，其特徵在於：其係於密碼處理裝置中，執行Feistel型公用密鑰區塊密碼處理者，且包含：

於資料處理部中，選擇性應用至少兩種以上不同F函數作為回合函數，執行複數回合之回合運算之資料處理步驟；

上述資料處理步驟包含下述步驟：

依據預先規定之密碼處理序列，取得與各回合中應用之F函數相對應之F函數對應表之存取用位址；

執行應用上述取得位址之記憶體存取，自儲存有將對應於上述兩種以上不同F函數各個之輸入值與輸出值或中間值賦予對應之複數F函數對應表的記憶體讀取對應於各回合F函數之F函數對應表；及

參照自記憶體中所讀取之表格，取得相對於F函數輸入值之輸出值或中間值，獲得依據各F函數之資料轉換結果。

再者，本發明之第三態樣係一種電腦程式，其特徵在於：其係於密碼處理裝置中，使Feistel型公用密鑰區塊密碼處理執行者，且包含：

於資料處理部中，選擇性應用至少兩種以上不同F函數作為回合函數，執行複數回合之回合運算的資料處理步驟；

上述資料處理步驟係使下述步驟執行之步驟；

依據預先規定之密碼處理序列，取得與各回合中應用之F函數相對應之F函數對應表之存取用位址；

使應用上述取得位址之記憶體存取執行，自儲存有將與上述兩種以上不同F函數各個對應之輸入值與輸出值或中間值賦予對應之複數F函數對應表的記憶體中讀取對應於各回合F函數之F函數對應表；及

使參照自記憶體中所讀取之表格，取得相對於F函數輸入值之輸出值或中間值，取得依據各F函數之資料轉換結果。

再者，本發明之電腦程式係可藉由以電腦可讀之形式提供之記憶媒體、通信媒體例如CD或FD、MO等記錄媒體、或者網路等通信媒體，而對例如可執行各種程式代碼之電腦系統提供之電腦程式。藉由以電腦可讀之形式提供上述程式，而於電腦系統上實現相應程式之處理。

本發明之進而其他目的、特徵或優點藉由基於下述本發明之實施例或所附圖式的更詳細說明當可明瞭。再者，本說明書中，所謂系統係指複數裝置之邏輯性集合構成，並非限定於各構成之裝置處於同一殼體內。

[發明之效果]

根據本發明之一實施例構成，於藉由選擇性應用至少兩種以上不同F函數作為回合函數之回合運算執行密碼處理的構成中，將賦予對應於各個F函數之輸入值與輸出值或中間值對應的複數F函數對應表儲存於記憶體內，依據預

先規定之密碼處理序列，應用對應於各回合F函數之表格存取用位址，自記憶體中讀取F函數對應表，並基於表格參照，取得對於輸入值之輸出值或中間值，獲得依據各F函數之資料轉換結果。根據本構成，可依據對應於各回合而變更之位址，取得各F函數對應表，有效取得或算出對應於輸入值之輸出值。例如，可藉由僅應用一個密碼函數變更引數，而執行各種密碼處理。

【實施方式】

以下，詳細說明本發明之密碼處理裝置、密碼處理方法、以及電腦程式。說明依據以下項目進行。

1.SPN型Feistel結構

2.對具有兩個資料序列之Feistel結構的擴散矩陣切換機構(DSM)之設定構成

3.對擴展型Feistel結構(GFN：Generalized Feistel Network)之擴散矩陣切換機構(DSM)之設定構成

4.應用不同線性轉換矩陣之不同回合函數之表格裝設的處理構成

5.密碼處理裝置之構成例

[1. SPN型Feistel結構]

首先，就SPN(Substitution Permutation Network，取代-排列網路)型Feistel結構加以說明。作為公用密鑰區塊密碼之設計而眾所周知之Feistel結構，具有藉由稱為回合函數之基本處理單元之重複，而將明文轉換為密文之結構。

參照圖1，就Feistel結構之基本構成加以說明。圖1中，

表示包含具有r回合之回合數=r之兩個資料序列的Feistel結構例。再者，回合數r係設計階段中設置之參數，其係例如可相應輸入之密鑰長度進行變更之值。

圖1所示之Feistel結構中，使作為密碼化對象輸入之明文長度為2 mn位元。其中，m、n均為整數。最初，將2 mn位元之明文分割為mn位元之兩個輸入資料P[0]101、P[1]102後，作為輸入值。圖示之例係將輸入值分割為2個之構成，即資料序列數(分割數)=2之構成例。

Feistel結構係由稱為回合函數之基本處理單元之重複進行表現，各回合中所含之資料轉換函數稱為回合函數(F函數)120。圖1之構成中，表示使回合函數120重複r段之構成例。

例如，於第一回合中，mn位元之輸入資料X與自無圖示之密鑰排程部(密鑰生成部)輸入之mn位元之回合密鑰$RK_1$103輸入至F函數120中，於回合函數(F函數)120中經資料轉換處理後，輸出mn位元之資料Y。輸出係於邏輯互斥或部104中與來自另一個前段之輸入資料(第一段之情形時，輸入資料P_L)進行邏輯互斥或運算後，將mn位元之運算結果輸出至下一個回合函數中。該處理僅以經決定之回合數(r)重複應用回合函數(F函數)使密碼化處理結束，輸出密文之分割資料C[0]、C[1]。各回合中執行之回合函數(F函數)為同一構成之Feistel結構之解密處理係亦可使插入回合密鑰之順序相反，故無需構成反函數。

就作為各回合之函數設定之回合函數(F函數)120之構

成，參照圖2加以說明。圖2(a)係表示一個回合中對回合函數(F函數)120進行輸入及輸出的圖，圖2(b)係詳細表示回合函數(F函數)120之構成的圖。回合函數(F函數)120，如圖2(b)所示，具有連接有非線性轉換層(S層)與線性轉換層(P層)之所謂SP型構成。

圖2所示之回合函數(F函數)120係具有輸入輸出位元長為m×n(m、n：整數)位元設定的函數。SP型F函數內部中，首先執行密鑰資料K_i與資料X_i之邏輯互斥或，其次應用非線性轉換層(S層)，繼而應用線性轉換層(P層)。

具體而言，非線性轉換層(S層)係排列有m個稱為取代盒(S-box)121之n位元輸入n位元輸出之非線性轉換表格者，mn位元資料以n位元為單位分割，並輸入至各自相應取代盒(S-box)121中，將資料轉換。各取代盒中，例如執行應用有轉換表格之非線性轉換處理。

線性轉換層(P層)由線性轉換部122構成，線性轉換部122輸入來自取代盒121之作為輸出資料之mn位元輸出值Z，並對該輸入執行線性轉換，輸出mn位元之結果。線性轉換部122執行輸入位元位置之切換處理等線性轉換處理，輸出mn位元之輸出值Y。該輸出值Y與來自前段之輸入資料一併進行邏輯互斥或後，成為下一回合之F函數輸入值。

再者，以下說明之本實施例之構成中，作為線性轉換層(P層)之線性轉換部122中執行之線性轉換定義為應用$GF(2^n)$上所定義之mn×mn之矩陣進行之線性轉換，又，將

第i回合中所含之矩陣稱為M_i。

設為回合數r之SPN型Feistel結構如圖3所示。n-bit之明文P被1/2分割為P[0]與P[1]，P[0]中應用輸入有回合密鑰RK_1之回合函數F_0，並將其結果與P[1]進行邏輯互斥或運算(EXOR)。使該結果為下一個回合之左輸入，並使P[0]為右輸入。其後重複應用規定次數(r次)之回合函數，最終獲得輸出C。該構成係所有回合中回合函數(F函數)均相同者。

回合函數F_0內中，首先輸入於回合函數中之資料與回合密鑰進行邏輯互斥或運算(EXOR)。使其結果為X(n/2-bit)。X分割為m個之s-bit資料。成為使其分別為x_1、x_2、...x_m之($X=(x_1||x_2||...||x_m)$)。再者，a||b表示a與b之序連資料。

各分割資料x_i分別輸入至s-bit輸入輸出之非線性轉換S即取代盒(S-box)中。使S-box之輸出分別為z_1、z_2、…、z_m($Z=z_1||z_2||\cdots||z_m$)。Z進而輸入至線性轉換部中，實施應用m×m矩陣M0之矩陣運算，最終獲得輸出Y。

如上所述，Feistel結構具有藉由作為資料轉換函數之回合函數(F函數)之簡單重複，而將明文轉換為密文之結構。然而，作為應用該Feistel結構之公用密鑰區塊密碼處理之問題點，存在密碼分析造成之密鑰洩漏。例如，存在由差分分析(亦稱差分解讀法或差分攻擊)或基於明文與對應密文之分析進行的線性分析(亦稱線性解讀法或線性攻擊)進行分析之虞。密碼分析易於進行密鑰分析，會導致

其密碼處理之安全性較低。

[2.對具有兩個資料序列之Feistel結構進行的擴散矩陣切換機構(DSM)之設定構成]

如前項說明般，應用有Feistel結構之密碼處理中，作為使對差分攻擊或線性攻擊之耐受性提高之構成，提出有應用有擴散矩陣切換機構(DSM：Diffusion Switching Mechanism，以下DSM)之構成。關於應用有該擴散矩陣切換機構(DSM)之密碼處理構成，例如揭示於日本專利特開2006-72054號中。DSM並非使Feistel結構之回合函數(F函數)部之線性轉換部中應用之矩陣在所有回合中相同，而是將至少兩個以上不同矩陣配置於各回合中。藉由該DSM，可提高對於差分攻擊或線性攻擊之耐受性。

關於該DSM，就其概要加以說明。於Feistel結構中，應用擴散矩陣切換機構(DSM)之情形時，構成Feistel結構之回合函數(F函數)部之線性轉換部(P層)中應用之矩陣為複數不同之矩陣。例如，並非將如圖1或圖3所示之r回合之Feistel結構之各回合中之應用矩陣設為全部相同之線性轉換矩陣，而是依據特定規則排列至少兩種以上之矩陣。

例如，圖4中表示實現擴散矩陣切換機構(DSM)的Feistel結構例，該擴散矩陣切換機構(DSM)於各回合之回合函數(F函數)之線性轉換層中配置兩個不同之線性轉換矩陣M_0、M_1。於圖4所示之Feistel結構例中，

F函數F_0表示執行應用有線性轉換矩陣M_0之線性轉換處理之回合函數(F函數)，

F函數F_1表示執行應用有線性轉換矩陣M_1之線性轉換處理之回合函數(F函數)。

兩個線性轉換矩陣M_0、M_1由不同矩陣構成。

再者，為實現擴散矩陣切換機構(DSM)，所應用之矩陣必須滿足特定條件。該條件之一係對分支數(Branch)之制約。以下，就該制約加以說明。

Feistel結構中之回合函數部之線性轉換中應用之複數不同矩陣M_0~M_n各自之分支數中，

如下所述對應用矩陣中分支數之最小值：B_1^D，與

與應用之複數矩陣之結合矩陣對應之分支數之最小值：B_2^D、B_3^D、B_2^L加以定義。

[數1]

$$B_1^D = \min_i(Branch_n(M_i))$$

$$B_2^D = \min_i(Branch_n([M_i \mid M_{i+2}]))$$

$$B_3^D = \min_i(Branch_n([M_i \mid M_{i+2} \mid M_{i+4}]))$$

$$B_2^L = \min_i(Branch_n([{}^tM_i^{-1} \mid {}^tM_{i+2}^{-1}]))$$

於上述式中，

M_i表示Feistel結構中之第i回合之線性轉換處理中應用之線性轉換矩陣，

$[M_i|M_{i+2}|\cdots]$表示藉由$M_i|M_{i+2}|\cdots$各矩陣之序連所得之結合矩陣，

${}^tM$表示矩陣M之轉置矩陣，M^{-1}表示矩陣M之反矩陣。

上述式中：B_2^D、B_3^D、B_2^L，具體而言表示Feistel結構中相隔一個結合有連續之2回合或3回合F函數中所含之矩陣

的矩陣分支數之最小值。

例如，眾所周知，可藉由以上述各分支數滿足以下條件，即

$B_2^D \geqq 3$，$B_3^D \geqq 3$，$B_2^L \geqq 3$，

之方式設定各矩陣，而使Feistel結構中，對於差分攻擊或線性攻擊之耐受性得以提昇。

再者，B_1^D、B_2^D、B_3^D、B_2^L中之各下標具有以下意義。

B_n^D之n表示結合之矩陣數，B_n^D之D表示用以具有對於差分攻擊(Differential Attack)之耐受性之條件，B_n^L之L表示用以具有對於線性攻擊(Linear Attack)之耐受性之條件。

如上所述，藉由應用各回合之回合函數(F函數)之線性轉換層中配置有兩個以上不同線性轉換矩陣之擴散矩陣切換機構(DSM)，而可提高對於差分攻擊或線性攻擊之耐受性。

圖4所示之構成中，Feistel結構應用兩個不同矩陣M_0、M_1，並由執行應用線性轉換矩陣M_0之線性轉換處理之回合函數(F函數)F_0，與執行應用線性轉換矩陣M_1之線性轉換處理之回合函數(F函數)F_1構成，但所應用之不同線性轉換矩陣之數量並非限定於2個，亦可為應用3、4‥種矩陣之構成。

圖5中表示應用三個矩陣M_0、M_1、M_2之Feistel結構例。圖5所示之Feistel結構例中，

F函數F_0表示執行應用線性轉換矩陣M_0之線性轉換處理之回合函數(F函數)，

F函數F_1表示執行應用線性轉換矩陣M_1之線性轉換處理之回合函數(F函數)，

F函數F_2表示執行應用線性轉換矩陣M_2之線性轉換處理之回合函數(F函數)。

三個線性轉換矩陣M_0、M_1、M_2由不同矩陣構成。

如上所述，擴散矩陣切換機構(DSM)係將執行不同線性轉換處理之複數不同線性轉換矩陣M_0、M_1、‥配置於各回合之回合函數(F函數)之線性轉換層執行回合函數者，並藉由該構成，提高對於差分攻擊或線性攻擊之耐受性。

[3.對擴展型Feistel結構(GFN：Generalized Feistel Network)所進行之擴散矩陣切換機構(DSM)之設定構成]

其次，就擴展型Feistel結構(GFN：Generalized Feistel Network)加以說明。參照圖1~圖5所說明之Feistel結構係將輸入資料P分割為兩個資料序列P[0]、P[1]而執行處理之構成。輸入資料之分割數稱為資料序列數(分割數)。參照圖1~圖5所說明之Feistel結構係資料序列數(分割數)d=2之設定。

應用有Feistel結構之密碼處理，可將資料序列數(分割數)d設定為3以上之數，資料序列數(分割數)設為3以上之任意數：d之Feistel結構定義為擴展型Feistel結構(GFN：Generalized Feistel Network)。上述擴展型Feistel結構(GFN)中，亦可應用擴散矩陣切換機構(DSM)，並可藉由應用擴散矩陣切換機構(DSM)，而提高對於密碼攻擊之耐受性。

圖6中表示包含具有擴散矩陣切換機構(DSM)之擴展型Feistel結構(GFN)的密碼化函數之構成例。圖6所示之例係具有使資料序列數(分割數)d為d=4之擴散矩陣切換機構(DSM)的擴展型Feistel結構(GFN)之密碼化函數之構成例。

具有擴散矩陣切換機構(DSM)之擴展型Feistel結構(GFN)，如上所述，係於Feistel結構之回合函數(F函數)部之線性轉換部中配置兩個以上不同矩陣，以使每個回合中能夠進行切換之構成者。藉由DSM，可提高對於差分攻擊或線性攻擊之耐受性。圖6所示之例中，F函數F_0與F函數F_1中，成為執行分別應用有不同線性轉換矩陣之資料轉換之構成。再者，該等F函數中所應用之線性轉換矩陣可藉由設定為滿足某特定之條件之矩陣，而大幅度提高對於差分攻擊或線性攻擊之耐受性。關於該構成，本案申請者在先前申請之日本專利特願2006-206376號中已有詳細說明。

圖6所示之密碼化函數之構成中，輸入為明文P，明文P分割為P[0]、P[1]、P[2]、P[3]之四個資料序列(分割數=4)，各回合中依次執行應用有F函數F_0、或F函數F_1之資料轉換，且輸出構成密文C之C[0]、C[1]、C[2]、C[3]，作為r回合之轉換結果。各回合之F函數F_0、或F函數F_1中，輸入有作為根據由未圖示之密鑰排程部供給之萬能密鑰(主密鑰)生成之擴展密鑰構成要素的回合密鑰(副密鑰)之$RK_i[0]$、$RK_i[1]$，並應用於資料轉換。再者，密鑰$RK_i[n]$之i表示回合，n表示同一回合中之回合密鑰之識別符。

如圖6所示，具有擴散矩陣切換機構(DSM)之擴展型Feistel結構(GFN)中，各回合之轉換部分中，執行取代各資料序列之調換處理。如圖6所示，調換函數211係於各回合之轉換時，應用於各資料序列之輸出，設定與各資料序列之輸出對應之下一回合中之輸入序列。

圖6中，使資料序列如圖6上段所示，自左為資料序列0、1、2、3時，藉由調換函數211，如下所述切換居先回合之4個序列之輸出與輸入序列對後續回合之的置換。

居先回合之資料序列0之輸出作為後續回合中之資料序列3之輸入而設定。

居先回合之資料序列1之輸出作為後續回合中之資料序列0之輸入而設定。

居先回合之資料序列2之輸出作為後續回合中之資料序列1之輸入而設定。

居先回合之資料序列3之輸出作為後續回合中之資料序列2之輸入而設定。

執行如此序列置換處理之函數係密碼化處理中應用之調換函數。

具有資料序列數(分割數)d=3以上之任意數之擴展型Feistel結構(GFN)，於各回合中重複如下處理，執行一個以上之回合函數，其後，進行序列切換處理，並執行後續之回合函數。

具有如此資料序列數(分割數)d=3以上之任意數之擴展型Feistel結構(GFN)中，亦可藉由將回合函數(F函數)中應

用之線性轉換矩陣設為滿足某特定條件之不同矩陣，而大幅提高對於差分攻擊或線性攻擊之耐受性。

[4.應用有不同線性轉換矩陣之不同回合函數之表格裝設的處理構成]

如上所述之採用有擴散矩陣切換機構(DSM)之Feistel結構或應用有擴展型Feistel結構之密碼處理構成，具有可大幅度提高對於差分攻擊或線性攻擊之耐受性之優點，但另一方面，存在如下所述之問題。即，

必須裝設設定不同矩陣之不同回合函數(F函數)，

必須設置預先規定複數回合函數並依據序列進行切換之新的控制機構，

因此，構成密碼處理裝置之情形時，所需構成會增加，導致阻礙裝置小型化，使成本上升。又，存在伴隨切換控制處理速度下降之問題。

以下，就解決上述問題之構成加以說明。即，應用有不同線性轉換矩陣之不同回合函數之表格裝設的處理構成。

作為具有回合函數(F函數)之公用密鑰密碼之裝設構成，可實現應用有軟體、硬體之各種構成。作為F函數之處理構成，需要作為非線性轉換部之S-box與作為線性轉換部之矩陣運算部，可分別實現各種邏輯電路之硬體構成、或使用有表格轉換表之構成。當要求高速動作之情形時，最佳的是稱為表格(查表)裝設之方法。

查表(表格)裝設係如下裝設方法，於並未進行實際運算狀態下，使用表格(置換表)將對應於各種輸入之預先計算

結束之運算結果保持於記憶體空間，並藉由參照表格，獲得需要求出之輸出值。例如，需要進行

$f(x)=x^3$

之計算之情形時，因包含具有如下數值之所謂ftab之表格(置換表)，即使未進行實際之x^3計算，亦可藉由參照ftab之內容，獲得x^3之結果。

ftab[0]=0(=0^3)，

ftab[1]=1(=1^3)，

ftab[2]=8(=2^3)，

ftab[3]=27(=3^3)，

ftab[4]=64(=4^3)，

..

上述者係表格ftab之例，其具有輸入值存在0、1、2、3、4時，取得0、1、8、27、64作為輸出之構成。

如上所述，F函數應用查表(表格)裝設構成，並預先準備對應於所需之各F函數輸入值的輸出值作為表格，儲存於密碼處理裝置之記憶體中。可使各F函數之表格構成為能夠根據表示記憶體之表格儲存位置之各位址而獲得。根據該方法，可易於進行F函數之置換而不會降低執行速度。將其應用後，可藉由自外部給予偶數段之F函數表格之位址，而無需使用函數，便可變更密碼化函數與解密函數。

例如，參照圖7，說明用以根據16-bit輸入輸出之F函數輸入求出輸出的表格構成。圖7(a)所示之回合函數(F函數)

構成為包含兩個S-box301、302與一個線性轉換部303。該構成中，將輸入X(16-bit)以每8-bit一分為兩，使之成為x_1、x_2。其次，分別將x_1、x_2輸入至執行8-bit輸入輸出之非線性轉換處理之S-box301、302中，獲得輸出z_1、z_2。對該等z_1、z_2，於線性轉換部303中實施線性轉換，其結果獲得y_1、y_2，將該等序連，獲得最終輸出Y。例如，如下計算線性轉換部303中之線性轉換。

[數2]

$$\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} a_{0,0} & a_{0,1} \\ a_{1,0} & a_{1,1} \end{pmatrix} \begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$$

$$y_1 = a_{0,0} \cdot z_1 \oplus a_{0,1} \cdot z_2$$

$$y_2 = a_{1,0} \cdot z_1 \oplus a_{1,1} \cdot z_2$$

上述S-box中之非線性處理、或線性轉換部中之矩陣運算，可設為藉由邏輯電路等由輸入值求出輸出。

即，構成執行下述運算作為S-box中之非線性處理運算之邏輯電路，

$z_1=S(x_1)$

$z_2=S(x_2)$

再者，構成執行下述運算作為線性轉換部中之運算之邏輯電路，

$y_1=a_{0,0}z_1(EXOR)a_{0,1}z_2$

$y_2=a_{1,0}z_1(EXOR)a_{1,1}z_2$

可為應用邏輯電路求出結果之構成。然而，若構成邏輯電路，則存在裝設面積變大，又，處理速度亦下降之問題。

因此，對於高速化而言，最佳的是預先計算運算部分，以表格保持對應於各種輸入之輸出值，並藉由表格參照，獲得輸出之處理。例如，圖7所示之回合函數中，可利用圖7(b)所示之表格。

於該例中，使t為相當於對於兩個S-box301、302之輸入值之變數，並應用以下兩個表格$TAB_0[t]$、$TAB_1[t]$。

$TAB_0[t]=(a_0 \cdot {}_0S(t)||a_1 \cdot {}_0S(t))$

$TAB_1[t]=(a_0 \cdot {}_1S(t)||a_1 \cdot {}_1S(t))$

輸入值[t]係相當於對於兩個S-box301、302之輸入值x_1、x_2之8位元資料，並藉由$TAB_0[t]$、$TAB_1[t]$自表格取得之資料，即，

$(a_0 \cdot {}_0S(t)||a_1 \cdot {}_0S(t))$

$(a_0 \cdot {}_1S(t)||a_1 \cdot {}_1S(t))$

該等分別為16位元資料。

根據藉由$TAB_0[t]$、$TAB_1[t]$而取得之16位元資料，求出最終回合函數之輸出Y。輸出Y係可藉由對$TAB_0[]$中插入x_1所得之結果與$TAB_1[]$中插入x_2所得之結果進行EXOR之處理，即，

$Y=TAB[x_1](EXOR)TAB[x_2]$

而算出。

若更詳細記述上述處理，則如下所述。

$Y=(y_1||y_2)=(a_{0,0}S(x_1)||a_{1,0}S(x_1))(EXOR)(a_{0,1}S(x_2)||a_{1,1}S(x_2))$。

應用利用該表格之方法之情形時，各1次執行表格$TAB_0[]$與表格$TAB_1[]$之各表格參照處理，求出對應於輸入x_1、x_2之輸出$TAB_0[x_1]$、$TAB_0[x_2]$。即，

$TAB_0[x_1]=(a_{0,0}S(x_1)||a_{1,0}S(x_1))$

$TAB_1[x_2]=(a_{0,1}S(x_2)||a_{1,1}S(x_2))$

其次，對該等兩個表格取得值$TAB_0[x_1]$、$TAB_1[x_2]$，執行1次邏輯互斥或運算(EXOR)。

藉由該等處理，可獲得一個回合函數之處理結果。即，作為處理，僅進行2次表格參照與1次邏輯互斥或運算(EXOR)。藉此，若可充分高速執行表格參照，則可十分高速地進行F函數處理。

於本發明中，提出於採用先前說明之擴散矩陣切換機構(DSM)之Feistel結構或應用擴展型Feistel結構之密碼處理中之回合運算中，應用上述表格參照處理之構成。如先前說明所示，擴散矩陣切換機構(DSM)係由於適當使用應用有複數不同線性轉換矩陣之不同回合函數(F函數)，故與使用單一F函數之方法相比，飛躍性地提高安全性之方式。該方式中，使用複數不同之F函數，根據其數量，安全性之參數或裝設上之特性有所變化。

於使用擴散矩陣切換機構(DSM)之情形時，必須每個回合應用不同回合函數，故需要回合函數(F函數)之切換控制。作為一個裝設構成例，例如利用有具有三個不同線性轉換矩陣之三個不同回合函數(F函數)的構成中，設為準

備稱為F_0、F_1、F_2之三個F函數。

根據該裝設構成，藉由回合函數(F函數)之選擇控制，實現各種密碼處理。例如，構成為藉由利用先前參照圖3說明之僅一個回合函數(F函數)F_0的SPN型Feistel結構進行密碼處理之情形時，於所有回合中呼叫應用F函數F_0。

又，構成為依據利用有具有先前參照圖4說明之兩個不同線性轉換矩陣M_0、M_1之兩個F函數F_0、F_1的DSM應用Feistel結構進行密碼處理之情形時，於各回合中，依據預先規定之序列，呼叫應用兩個F函數F_0、F_1。

又，構成為依據利用有具有先前參照圖5說明之三個不同線性轉換矩陣M_0、M_1、M_2之三個F函數F_0、F_1、F_2的DSM應用Feistel結構進行密碼處理之情形時，於各回合中，依據預先規定之序列，呼叫應用三個F函數F_0、F_1、F_2。

如上所述，本體之密碼化部即使不進行變更，亦可以一個程式執行三個密碼化函數。

如上所述，若可適時置換F函數，則可實現各種應用，因此尤其期望的是DSM中可易於置換F函數。

作為用以解決該問題之最簡單方法，考慮如將F函數部作為函數自外部輸入之形態。該方法係預先製作執行複數F函數部之函數，將該等輸入至密碼化函數，藉此實現F函數之切換。然而，該方法必須以密碼化函數多次呼叫複數F函數。可認為通常一次執行時間非常短之區塊密碼中，密碼化函數內多次呼叫其他函數(該情形時為F函數)，會

導致執行速度大幅度下降，其影響巨大。因此，更期望的是並不將F函數部作為函數進行切換。

作為解決上述問題之構成，就裝設分別對應於應用不同線性轉換矩陣之不同回合函數(F函數)之表格的處理構成，加以說明。即，預先裝置之記憶體空間內，儲存與應用不同線性轉換矩陣之不同回合函數(F函數)對應之輸出值取得用之表格。當依據應用有上述擴散矩陣切換機構(DSM)之Feistel結構執行密碼處理之情形時，於各回合中適當切換利用所利用之表格。即，藉由僅置換所利用之表格，而實現F函數置換。

更具體而言，例如作為執行密碼處理之密碼化函數之輸入資訊，設定各回合中應用之回合函數(F函數)對應表之取得用記憶體位址。密碼化函數執行回合函數之情形時，應用各回合對應之記憶體位址，自記憶體取得對應於各回合中執行之回合函數(F函數)之表格，根據特定之輸入值取得表格設定值。若藉由該處理僅置換表格、即記憶體之位址，則等同於置換F函數，可實現高速處理。即，實際處理係僅改變表格之位址，因此執行速度完全不會降低。

參照圖8、圖9，就利用有對應於複數不同回合函數(F函數)之複數表格之密碼處理構成，加以說明。圖8係表示本實施例之密碼處理裝置400之一構成例的圖。密碼處理裝置400包含例如執行應用有上述SPN型Feistel結構之密碼處理，依據應用有擴散矩陣切換機構(DSM)之Feistel結構執行密碼處理等之資料處理部410，及儲存有與應用有不同

線性轉換矩陣M_0、M_1、…之回合函數(F函數)F_0、F_1…對應之表格的記憶體420。

記憶體420保持有與應用有不同線性轉換矩陣M_0、M_1，…之回合函數(F函數)F_0、F_1…對應之表格，亦即相應各輸入值儲存與不同F函數F_0、F_1…之輸入值對應之輸出值或算出輸出值所需之中間值之複數F函數對應表421、422‥42n。

圖9中，表示儲存於記憶體420之複數F函數對應表421、422‥42n之例。F函數對應表421係對應於第一F函數(回合函數)之表格，並保持對應地設定有相對於第一F函數之各輸入值、對應於輸入值之輸出值或算出輸出值所需之中間值。F函數對應表422係對應於第二F函數(回合函數)之表格，並保持對應地設定有相對於第二F函數之各輸入值、對應於輸入值之輸出值或算出輸出值所需之中間值。以下，同樣地n個F函數之對應表儲存於記憶體420中。

再者，儲存於表格中之輸入值可作為相對於整個F函數之輸入值，亦可作為相對於F函數內之各S-box之輸入值等F函數輸入值之部分構成值。至於輸出值可作為F函數之輸出值，亦可作為用以算出輸出值之中間值。即，儲存於記憶體420中之F函數對應表，可作為與相對於各F函數之輸入值或輸入值之構成資料、與F函數之輸出值或中間值或該等之構成資料保持對應的表格。

該等各表格係可應用存取用位址而讀取之構成，並設定有對應於各表格之位址，例如

第一F函數對應表位址=[FF000001]

第二F函數對應表位址=[FFF01234]

等各表格之讀取位址，圖8所示之回合函數執行部411應用與各回合中應用之F函數對應之位址，執行表格讀取。

圖8所示之資料處理部410，包含執行回合函數之回合函數執行部411，將應用於各回合中應用之F函數對應表存取之各表格對應之記憶體位址提供給回合函數執行部411的記憶體位址提供部412，及儲存有密碼處理之順序資訊之處理順序資訊儲存部413。

處理順序資訊儲存部，例如依據應用有先前說明之擴散矩陣切換機構(DSM)之Feistel結構執行密碼處理之情形時，預先儲存各回合中執行之F函數之順序資訊，而記憶體位址提供部412依據該順序資訊，取得各回合中需要參照之F函數對應表之記憶體位址，並將其提供給回合函數執行部411。

回合函數執行部411，自記憶體位址提供部412接受與基於執行之密碼順序之每個回合中執行之F函數對應的表格存取用位址，並依據接受位址，執行記憶體420之存取，取得各回合中需要應用之F函數對應表，並且根據表格參照，獲得對應於輸入值之輸出值(或中間值)。回合函數執行部411，依據對應於各回合而變更之位址，僅取得各回合中應用之表格，且亦可逐次設定每個回合之F函數對應表之位址作為固定密碼函數中應用之引數，故可僅藉由應用一個密碼函數變更引數，而執行各種密碼處理。即，無

需不同F函數之呼叫處理，便可高速獲得各回合運算(F函數)之處理結果。又，該構成中，無需對應於各回合函數之邏輯電路等，便可實現裝置小型化、裝設成本之削減。

再者，執行應用有先前參照圖6說明之資料序列數可設定為3以上之任意數之擴展型Feistel結構之密碼處理的構成中，有時一個回合中可並列執行複數回合函數(F函數)。因此，執行應用有擴展型Feistel結構之密碼處理之構成之情形時，回合函數執行部411較好的是構成為可並列執行複數回合函數(F函數)。回合函數執行部411，並列執行與並列執行之回合函數對應之各個F函數對應表之參照處理。再者，處理速度雖會下降，但亦可構成為順序存取記憶體。

再者，若使用如圖8所示之記憶體中儲存之F函數對應表之參照切換構成，則可僅藉由記憶體存取用之位址變更，而執行各回合中應用之表格變更，因此可實現表格利用順序之柔軟變更。例如，應用有先前參照圖5說明之三個不同矩陣M_0、M_1、M_2之Feistel結構之密碼處理中，圖5所示之例中設定為

F函數之應用順序=

$F_0 \rightarrow F_2 \rightarrow F_1 \rightarrow F_1 \rightarrow F_2 \cdots$

但亦可例如如下述般變更該順序。

F_0之位置中設定F_1，

F_1之位置中設定F_2，

F_2之位置中設定F_0。

上述F函數之利用順序之變更可僅藉由各回合中應用之位址變更而實現。

上述變更例中，各回合之F函數利用順序成為

$F_1 \rightarrow F_0 \rightarrow F_2 \rightarrow F_2 \rightarrow F_0 \cdots$。

實現如此順序所需之處理僅變更各回合中應用之F函數呼叫位址之順序，故而可易於進行變更。基於如此不同F函數利用順序之密碼處理具備不同於變更前之F函數利用順序之輸入輸出，且安全性而言，可構成等價之密碼化函數。

再者，擴散矩陣切換機構(DSM)因應用之不同回合函數(F函數)之數量不同，安全性參數會產生變化。通常，使用較多不同回合函數(F函數)者之安全性高。當構成為複數F函數對應表儲存於記憶體中進行利用之情形時，亦可想像需要參照之表格無法插入至可高速存取之記憶體空間(例如，1次快取記憶體)上，因此較好的是構成為將可相應於處理順序儲存最多之必須參照之表格的記憶體區域設為可高速存取之記憶體空間。

如圖8所示，本發明之密碼處理裝置400係執行Feistel型公用密鑰區塊密碼處理之密碼處理裝置，並包含選擇性應用至少兩種以上之不同之F函數作為回合函數，執行複數回合之回合運算的資料處理部410，及儲存有與分別對應於兩種以上之各個不同F函數之輸入值與輸出值或中間值保持對應之複數F函數對應表的記憶體420，而資料處理部410中，依據預先規定之密碼處理順序，取得對應於各回

合中應用之F函數的F函數對應表之存取用位址，並藉由應用有取得位址之記憶體420之存取，讀取對應於各回合F函數之F函數對應表421~42n，根據表格參照取得相對於輸入值之輸出值或中間值，獲得基於各F函數之資料轉換結果。

再者，資料處理部410係執行基於Feistel結構之密碼處理之構成，該Feistel具有擴散矩陣切換機構(DSM：Diffusion Switching Mechanism)，而該擴散矩陣切換機構選擇性應用設定至少2個以上不同矩陣結構作為應用於各回合F函數中之線性轉換處理之轉換矩陣之至少2個以上不同F函數，例如基於依據設為將密碼處理對象資料分割為2個之資料序列數(分割數)d=2之Feistel結構，或者設為資料序列數(分割數)d≧3之擴展型Feistel結構執行密碼處理。

資料處理部410執行預先設定之密碼函數，並於執行密碼函數時，於每個回合中適當切換與各回合中應用之F函數對應的F函數對應表之存取用位址，並自記憶體420讀取對應於各回合F函數之F函數對應表，再根據表格參照取得相對於輸入值之輸出值或中間值，獲得基於各F函數之資料轉換結果。

再者，儲存於記憶體420中之F函數對應表421~42n係使相對於各F函數之輸入值或輸入值之構成資料與F函數之輸出值或中間值、或該等之構成資料保持對應的F函數對應表。

如上所述，藉由如此構成，資料處理部410可依據對應

於各回合而變更之位址取得表格，執行基於各回合F函數之資料轉換處理，若逐次設定每個回合之F函數對應表之位址作為固定之密碼函數中應用之引數，則可僅藉由應用一個密碼函數變更引數，而執行各種密碼處理。即，無需不同F函數之呼叫處理，便可高速獲得各回合運算(F函數)之處理結果。又，該構成中，無需對應於各回合函數之邏輯電路等，便可實現裝置小型化、裝設成本之削減。

[5.密碼處理裝置之構成例]

最後，圖10中表示作為執行依據上述實施例之密碼處理之密碼處理裝置的IC模組700之構成例。上述處理例如可執行於PC、IC卡、讀寫器、其他各種資訊處理裝置中，圖10所示之IC模組700可構成於該等各種設備中。

圖10所示之CPU(Central processing Unit，中央處理單元)701係密碼處理之開始或結束時執行資料之收發控制、各構成部間之資料傳輸控制、其他各種程式的處理器。記憶體702包含CPU 701執行之程式，或者儲存運算參數等固定資料之ROM(Read-Only-Memory，唯讀記憶體)，CPU 701處理中執行之程式，及程式處理中適當變化之參數儲存區域，作為工作區域使用之RAM(Random Access Memory，隨機存取記憶體)等。又，記憶體702用作密碼處理所需之密鑰資料，或密碼處理中應用之轉換表格(置換表)或應用於轉換矩陣之資料等之儲存區域。又，如參照圖8、圖9說明所示，記憶體702用作用以獲得對應於上述不同F函數之輸出值的F函數對應表之儲存區域。

如上所述，保持有複數F函數對應表，該等F函數對應表與各輸入值保持對應地儲存有與應用有不同線性轉換矩陣M_0、M_1、...之回合函數(F函數)F_0、F_1...對應之表格，即算出基於不同F函數F_0、F_1...之輸入值之輸出值所需之數值。再者，資料儲存區域較好的是構成為具有抗侵入結構之記憶體。

密碼處理部703基於例如依據上述Feistel結構、或擴展型Feistel結構之公用密鑰區塊密碼處理演算法執行密碼處理，解密處理。再者於此，表示有將密碼處理機構作為個別模組之例，但亦可構成為並不設置上述獨立之密碼處理模組，而例如將密碼處理程式儲存於ROM中，由CPU 701讀取ROM儲存程式進行執行。

隨機數產生器704於密碼處理所需之密鑰生成等中執行必須之隨機數產生處理。

收發部705係執行與外部之資料通信之資料通信處理部，例如執行與讀寫器等IC模組之資料通信，執行IC模組內生成之密文輸出，或者來自外部讀寫器等設備之資料輸入等。

該IC模組700之密碼處理部703例如執行資料序列數d=2之Feistel型密碼處理，或使資料序列數d為d≧3之整數之擴展型Feistel型密碼處理。又，執行基於Feistel結構之密碼處理，該Feistel具有擴散矩陣切換機構(DSM：Diffusion Switching Mechanism)，而該擴散矩陣切換機構選擇性應用設定有至少2個以上不同矩陣結構之至少2個以上不同F

函數。再者，於密碼處理時，如參照圖8、圖9說明所示，於各回合中逐次切換用以取得獲得對應於不同F函數之輸出值的F函數對應表之位址，執行記憶體存取，取得對應於各F函數輸入值之輸出值或中間值，執行回合運算。藉由該處理，無需利用各種密碼函數，便可藉由利用將記憶體存取用位址設為引數之一個密碼函數，而基於各種密碼順序執行處理。

以上，一面參照特定之實施例，一面詳細解釋本發明。然而，業者須知可於不脫離本發明宗旨之範圍內，進行該實施例之修正或代用。即，由於以例示形態揭示本發明，故並非限定性解釋。為判斷本發明之宗旨，須參酌申請專利範圍之項目。

再者，說明書中所說明之系列處理係可藉由硬體或軟體、或者兩者之複合構成而執行。由軟體執行處理之情形時，可將記錄有處理順序之程式安裝於編入專用硬體中之電腦內記憶體後執行，或者可將程式安裝於能夠執行各種處理之通用電腦內執行處理。

例如，程式係可預先記錄於作為記錄媒體之硬碟或ROM(Read Only Memory，唯讀記憶體)中。或者，程式可暫時或永久儲存(記錄)於軟碟、CD-ROM(Compact Disc Read Only Memory，緊密光碟-唯讀記憶體)、MO(Magneto optical，磁光碟)碟、DVD(Digital Versatile Disc，數位多用途光碟)、磁碟、半導體記憶體等可移動記錄媒體中。如此可移動記錄媒體可作為所謂封裝軟體提供。

再者，程式除自如上所述之可移動記錄媒體安裝於電腦以外，亦可自下載網站，無線傳輸至電腦中，或者介由LAN(Local Area Network，區域網路)、網際網路之所謂網路，有線傳輸至電腦中，電腦可接收如此傳輸而至之程式，並安裝於內置之硬碟等記錄媒體。

再者，揭示於說明書之各種處理不僅可按照揭示內容以時序進行執行，而且亦可相應執行處理之裝置處理能力或者需要同作或單獨進行執行。又，本說明書中，所謂系統係指複數裝置之邏輯集合構成，並非限定於各構成之裝置安裝於同一機架內。

[產業上之可利用性]

如上所述，根據本發明之一實施例構成，於藉由選擇性應用有至少兩種以上不同F函數作為回合函數之回合運算執行密碼處理的構成中，將與對應於各個F函數之輸入值與輸出值或中間值保持對應的複數F函數對應表儲存於記憶體內，並依據預先規定之密碼處理順序，應用對應於各回合F函數之表格存取用位址，自記憶體中讀取F函數對應表，並基於表格參照，取得相對於輸入值之輸出值或中間值，獲得基於各F函數之資料轉換結果。根據本構成，可依據對應於各回合而變更之位址，取得各F函數對應表，有效取得或算出對應於輸入值之輸出值。例如，可僅藉由應用一個密碼函數變更引數，而執行各種密碼處理。

【圖式簡單說明】

圖1係說明Feistel結構之基本構成的圖。

圖2(a)、2(b)係說明作為回合函數部設定之F函數之構成的圖。

圖3係表示使回合數為r之SPN型Feistel結構例的圖。

圖4係表示實現各回合之回合函數(F函數)之線性轉換層中配置兩個不同線性轉換矩陣M_0、M_1之擴散矩陣切換機構(DSM)之Feistel結構例的圖。

圖5係表示應用三個矩陣M_0、M_1、M_2之Feistel結構例的圖。

圖6係表示包含具有擴散矩陣切換機構(DSM)之擴展型Feistel結構(GFN)之密碼化函數之構成例的圖。

圖7(a)、7(b)係說明用以自F函數之輸入求出輸出之表格構成的圖。

圖8係對利用有對應於複數不同回合函數(F函數)之複數表格之密碼處理構成加以說明的圖。

圖9係對為了實現利用有對應於複數不同回合函數(F函數)之複數表格之密碼處理構成而儲存於記憶體中之表格加以說明的圖。

圖10係表示作為執行本發明之密碼處理之密碼處理裝置之IC模組之構成例的圖。

【主要元件符號說明】

104	邏輯互斥或部
120	回合函數(F函數)
121、301、302	取代盒(S-box)
122、303	線性轉換部

211	調換函數
400	密碼處理裝置
410	資料處理部
411	回合函數執行部
412	記憶體位址提供部
413	處理順序資訊儲存部
420、702	記憶體
421、422、42n	F函數對應表
700	IC模組
701	CPU(中央處理單元)
703	密碼處理部
704	隨機數產生器
705	收發部
F、F0、F1、F2	回合函數
Ki	密鑰資料
M0、M1	線性轉換矩陣
S-box	取代盒
P[0]101、P[1]102	輸入資料
RKi[0]、RKi[1]...RKi[n]	回合密鑰
X1、X2、...Xi	資料

五、中文發明摘要：

本發明係提供一種有效執行應用複數不同F函數之密碼處理的構成。於執行藉由選擇性應用不同F函數之回合運算而成之密碼處理的構成中，將對應於各F函數之輸入值與輸出值或中間值賦予對應的複數F函數對應表儲存於記憶體內，依據預先規定之密碼處理順序，應用對應於各回合F函數的位址，自記憶體讀取F函數對應表，根據表格參照，取得相對於輸入值之輸出值或中間值，獲得依據各F函數之資料轉換結果。

六、英文發明摘要：

十一、圖式：

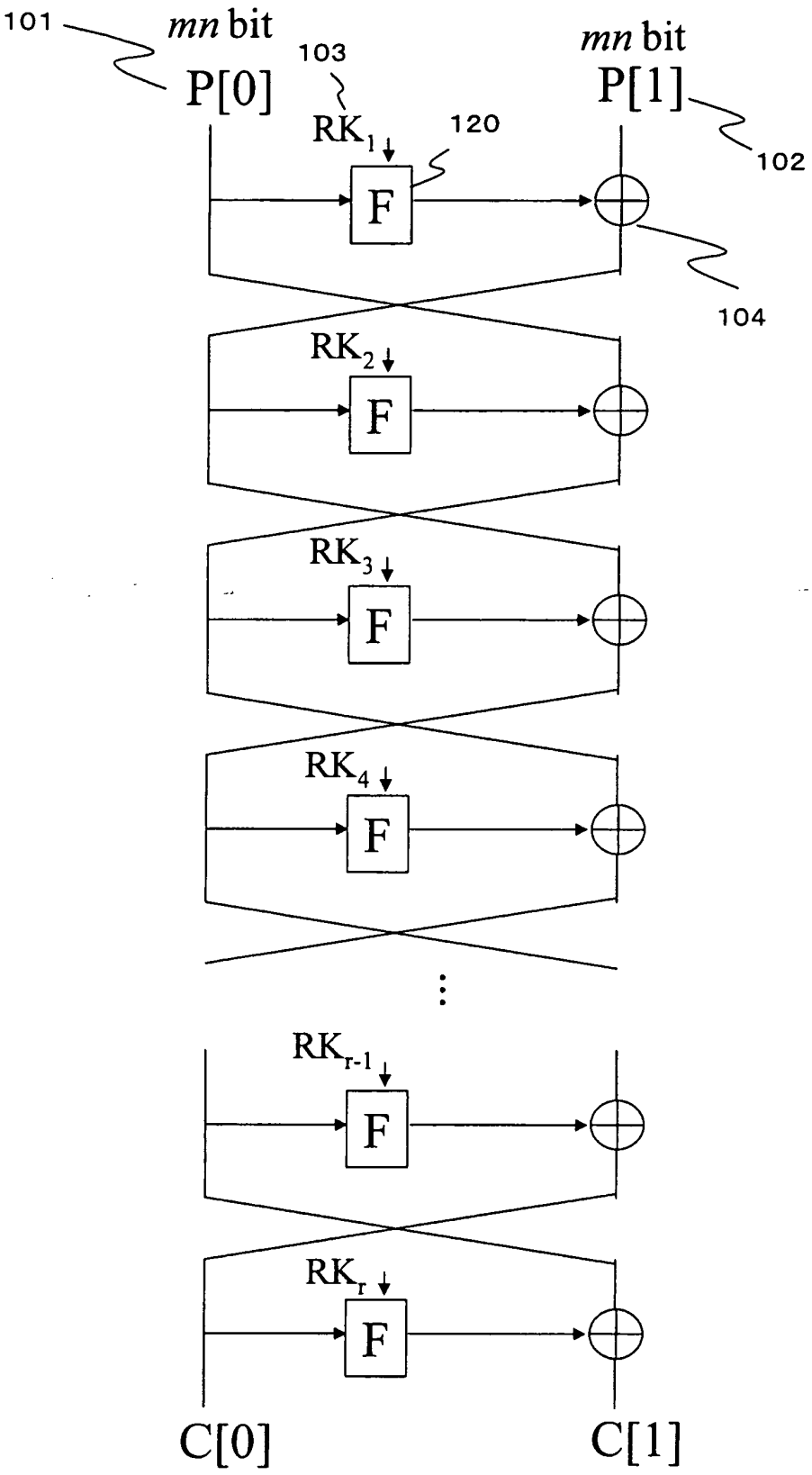

101
mn bit
P[0]
103
RK1
120
mn bit
P[1]
102
F
104
RK2
F
RK3
F
RK4
F
RKr-1
F
RKr
F
C[0]
C[1]

圖1

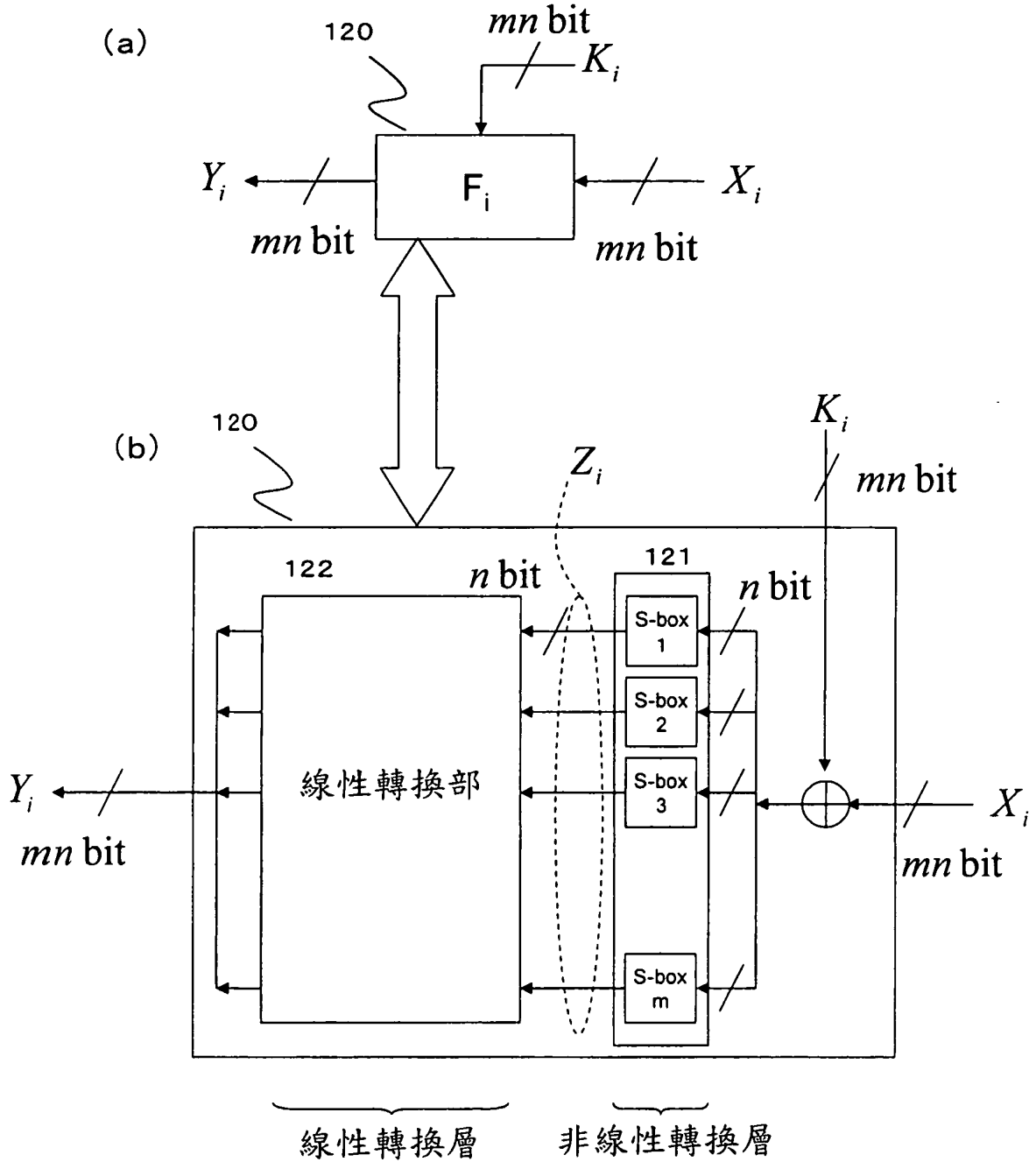

(a)
120
mn bit
K_i
Y_i
F_i
X_i
mn bit
mn bit
(b)
120
Z_i
K_i
mn bit
122
n bit
121
n bit
S-box 1
S-box 2
S-box 3
S-box m
線性轉換部
Y_i
mn bit
X_i
mn bit
線性轉換層
非線性轉換層

圖2

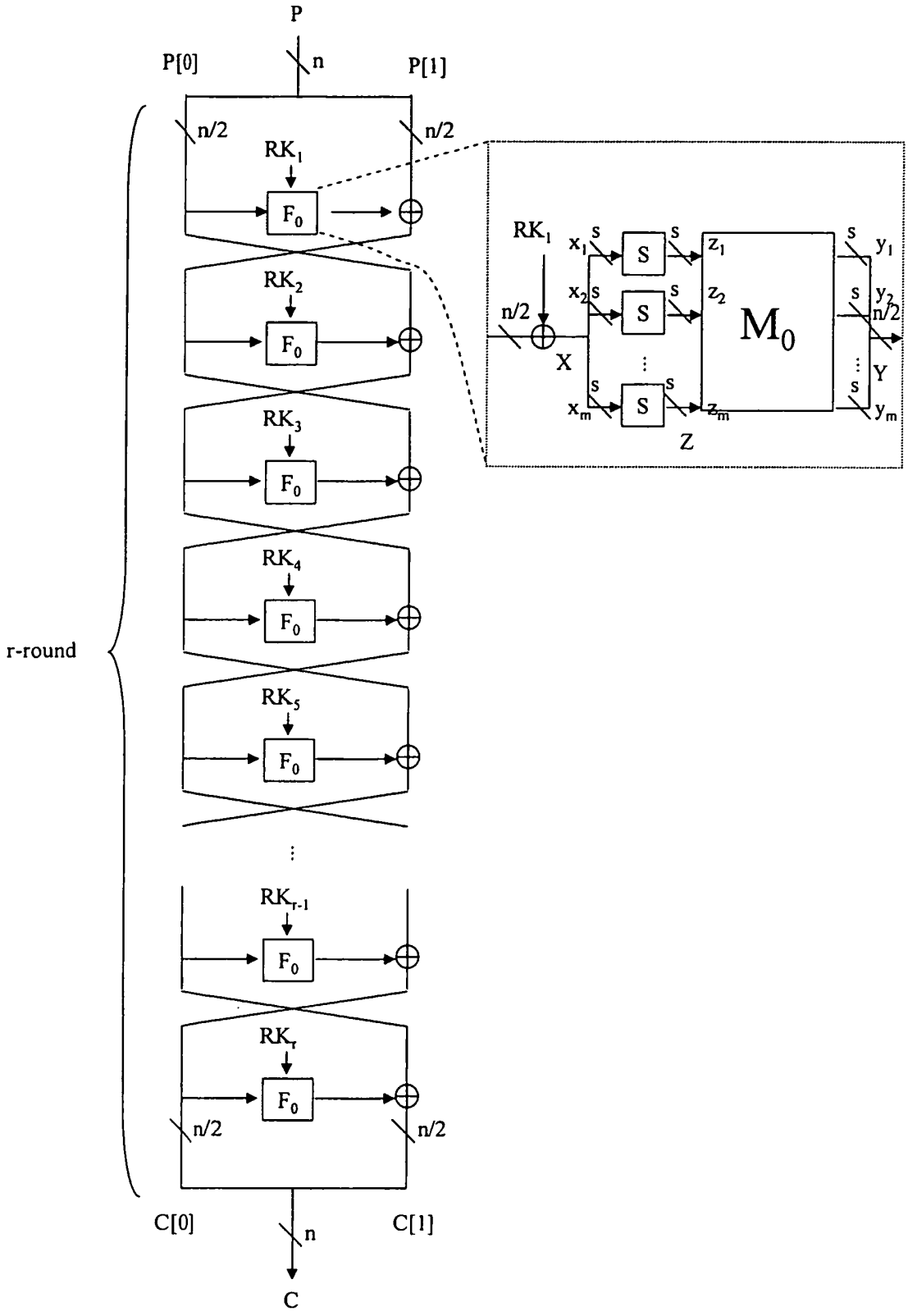

P
P[0]
n
P[1]
n/2
n/2
RK1
F0
RK2
RK3
RK4
RK5
RKr-1
RKr
r-round
n/2
n/2
C[0]
n
C[1]
C
RK1
n/2
X
x1
x2
xm
S
z1
z2
zm
M0
Z
y1
y2
n/2
Y
ym

圖3

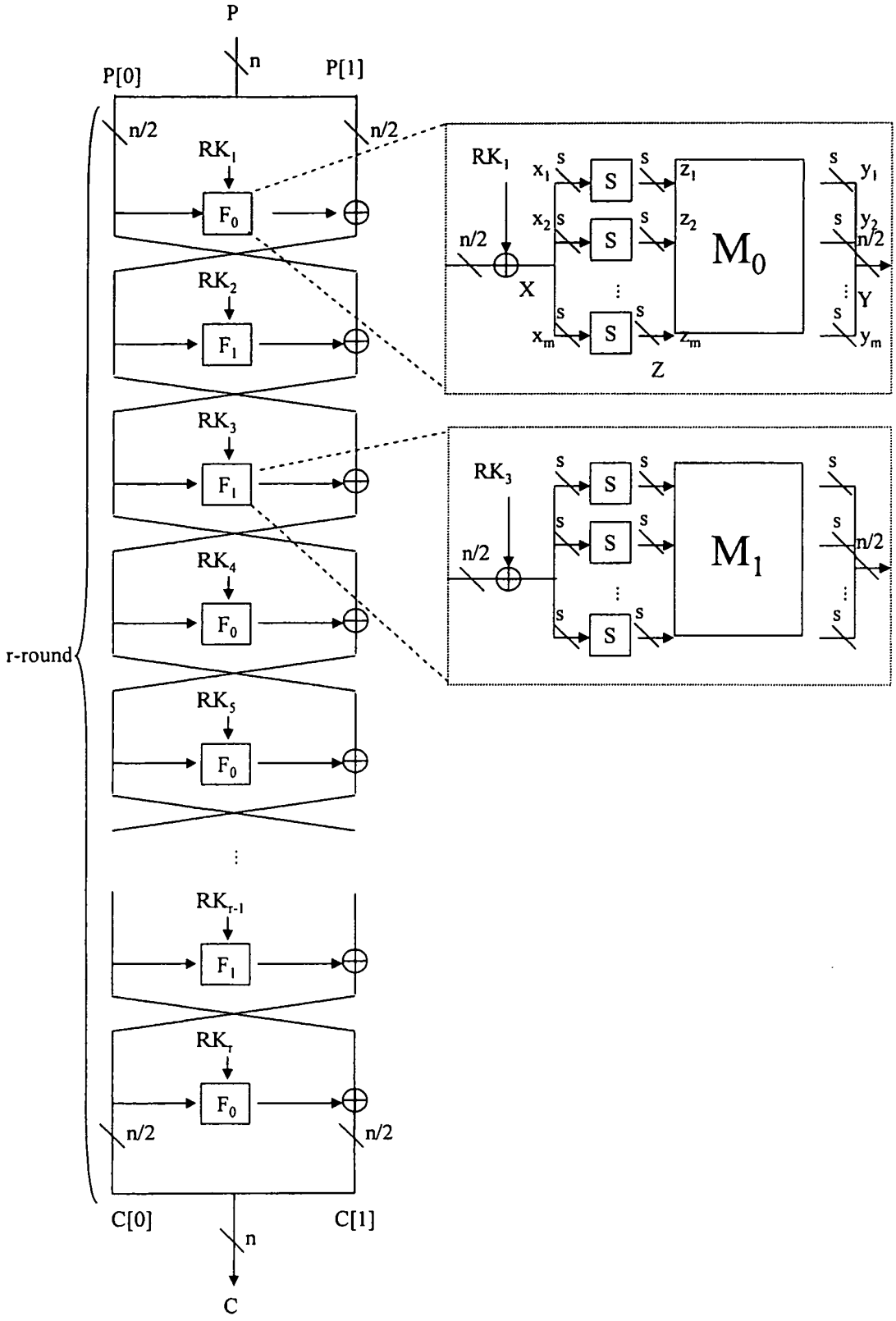

P
n
P[0]
P[1]
n/2
n/2
RK1
F0
RK2
F1
RK3
F1
RK4
F0
RK5
F0
r-round
RKr-1
F1
RKr
F0
n/2
n/2
C[0]
C[1]
n
C
RK1
x1
x2
xm
S
z1
z2
zm
M0
y1
y2
yn
X
Z
Y
RK3
M1

圖4

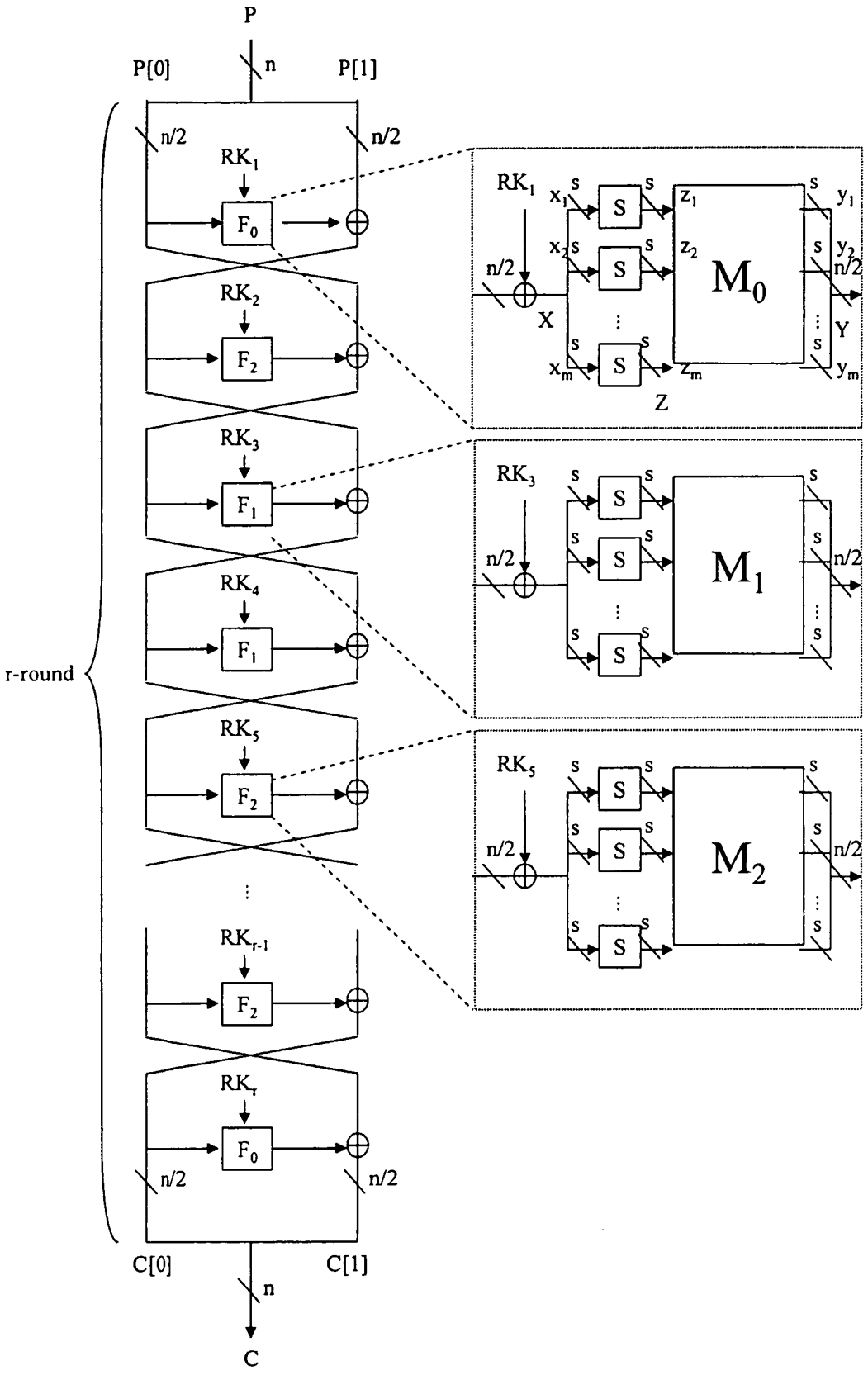

P
P[0]
n
P[1]
n/2
n/2
RK1
F0
RK2
F2
RK3
F1
RK4
F1
RK5
F2
RKr-1
F2
RKr
F0
n/2
n/2
r-round
C[0]
n
C[1]
C
RK1
x1
x2
xm
S
z1
z2
zm
M0
y1
y2
ym
n/2
X
Y
Z
RK3
M1
RK5
M2

圖5

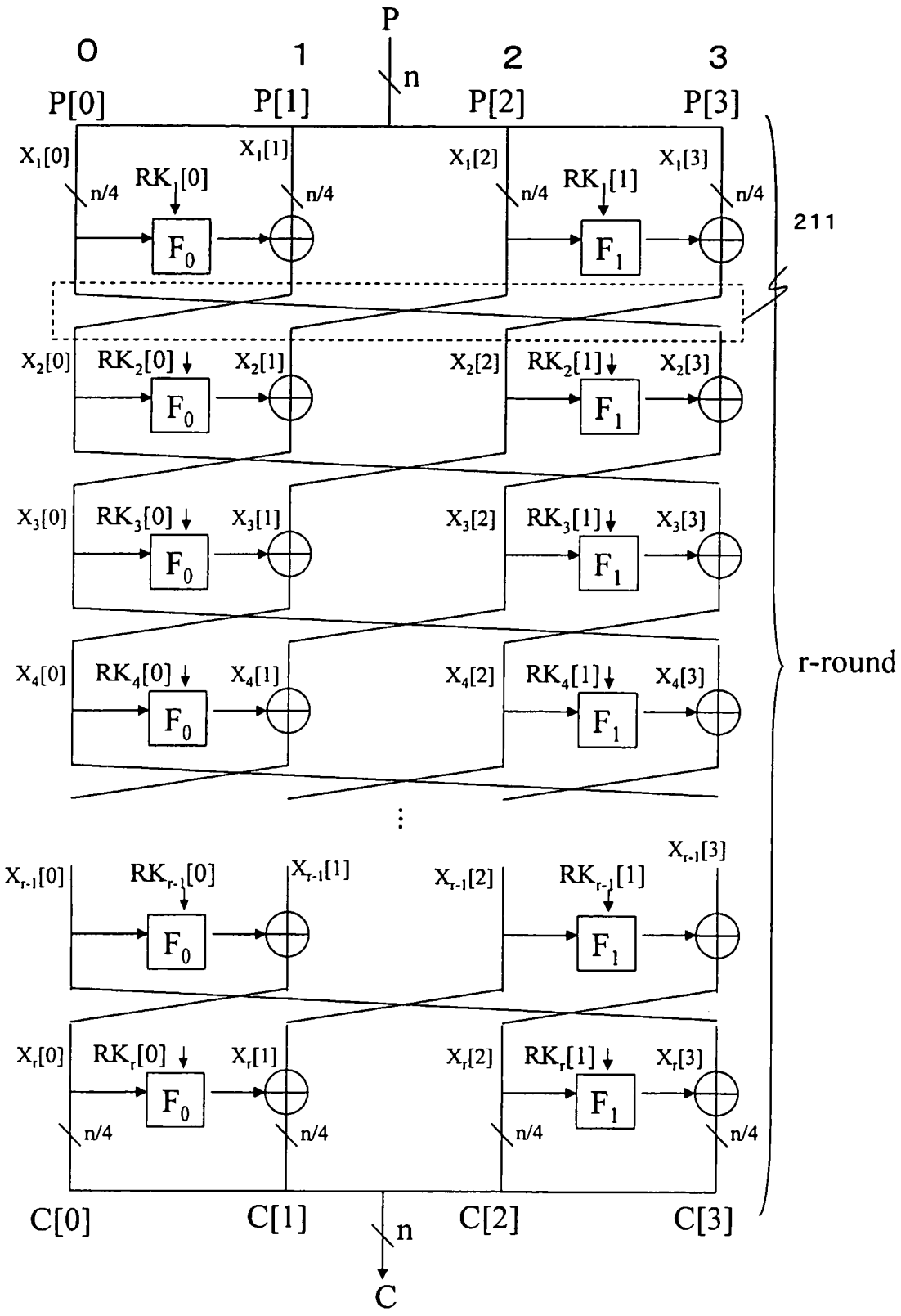
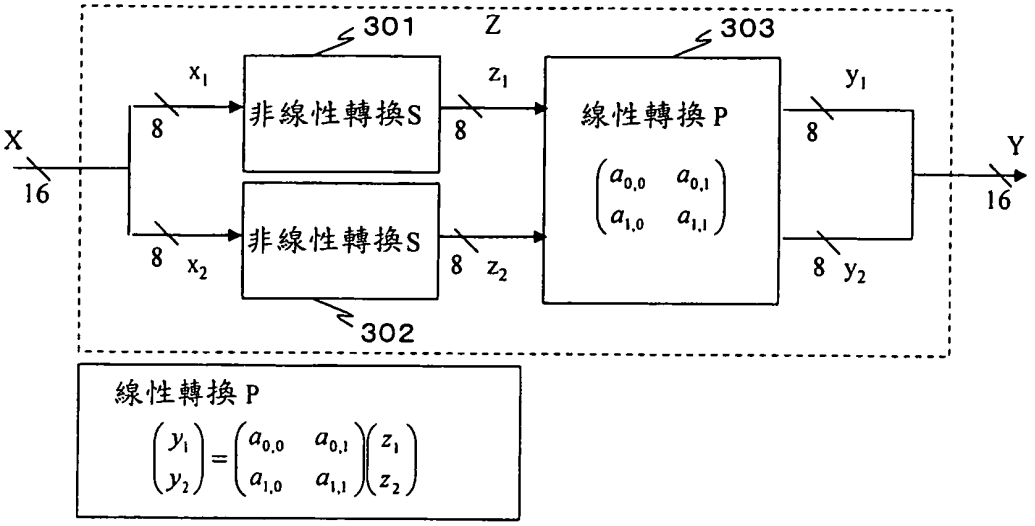

P
0
1
2
3
n
P[0]
P[1]
P[2]
P[3]
$X_1[0]$
$X_1[1]$
$X_1[2]$
$X_1[3]$
$RK_1[0]$
$RK_1[1]$
n/4
F_0
F_1
211
$X_2[0]$
$X_2[1]$
$X_2[2]$
$X_2[3]$
$RK_2[0]$
$RK_2[1]$
$X_3[0]$
$X_3[1]$
$X_3[2]$
$X_3[3]$
$RK_3[0]$
$RK_3[1]$
$X_4[0]$
$X_4[1]$
$X_4[2]$
$X_4[3]$
$RK_4[0]$
$RK_4[1]$
r-round
$X_{r-1}[0]$
$X_{r-1}[1]$
$X_{r-1}[2]$
$X_{r-1}[3]$
$RK_{r-1}[0]$
$RK_{r-1}[1]$
$X_r[0]$
$X_r[1]$
$X_r[2]$
$X_r[3]$
$RK_r[0]$
$RK_r[1]$
C[0]
C[1]
C[2]
C[3]
C

圖6

(a) 回合函數（F函數）



(b) 表格構成

事前製作、保持如下所述之8－bit輸入16－bit輸出之表格$TAB_0[t]$、$TAB_1[t]$

$$TAB_0[t] = \overbrace{(a_{0,0}\,S(t) \,\|\, a_{1,0}\,S(t))}^{16\text{-bit}}$$
$$TAB_1[t] = (a_{0,1}\,S(t) \,\|\, a_{1,1}\,S(t))$$

F函數處理

$$Y = TAB_0[x_1] \,(+)\, TAB_1[x_2]$$

圖7

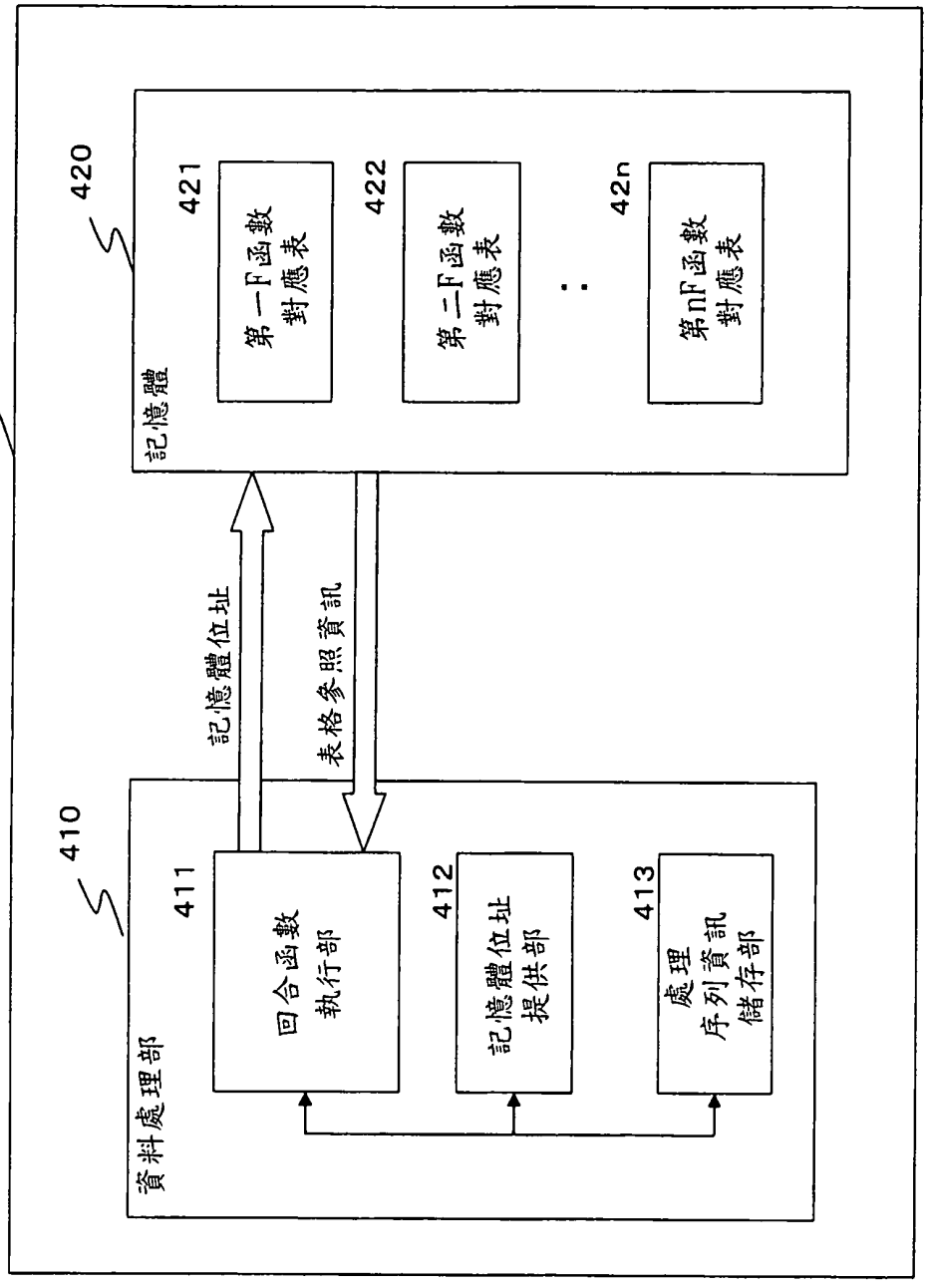

400
420
421
第一F函數
對應表
422
第二F函數
對應表
42n
第nF函數
對應表
記憶體
記憶體位址
表格參照資訊
410
411
回合函數
執行部
412
記憶體位址
提供部
413
處理
序列資訊
儲存部
資料處理部

圖8

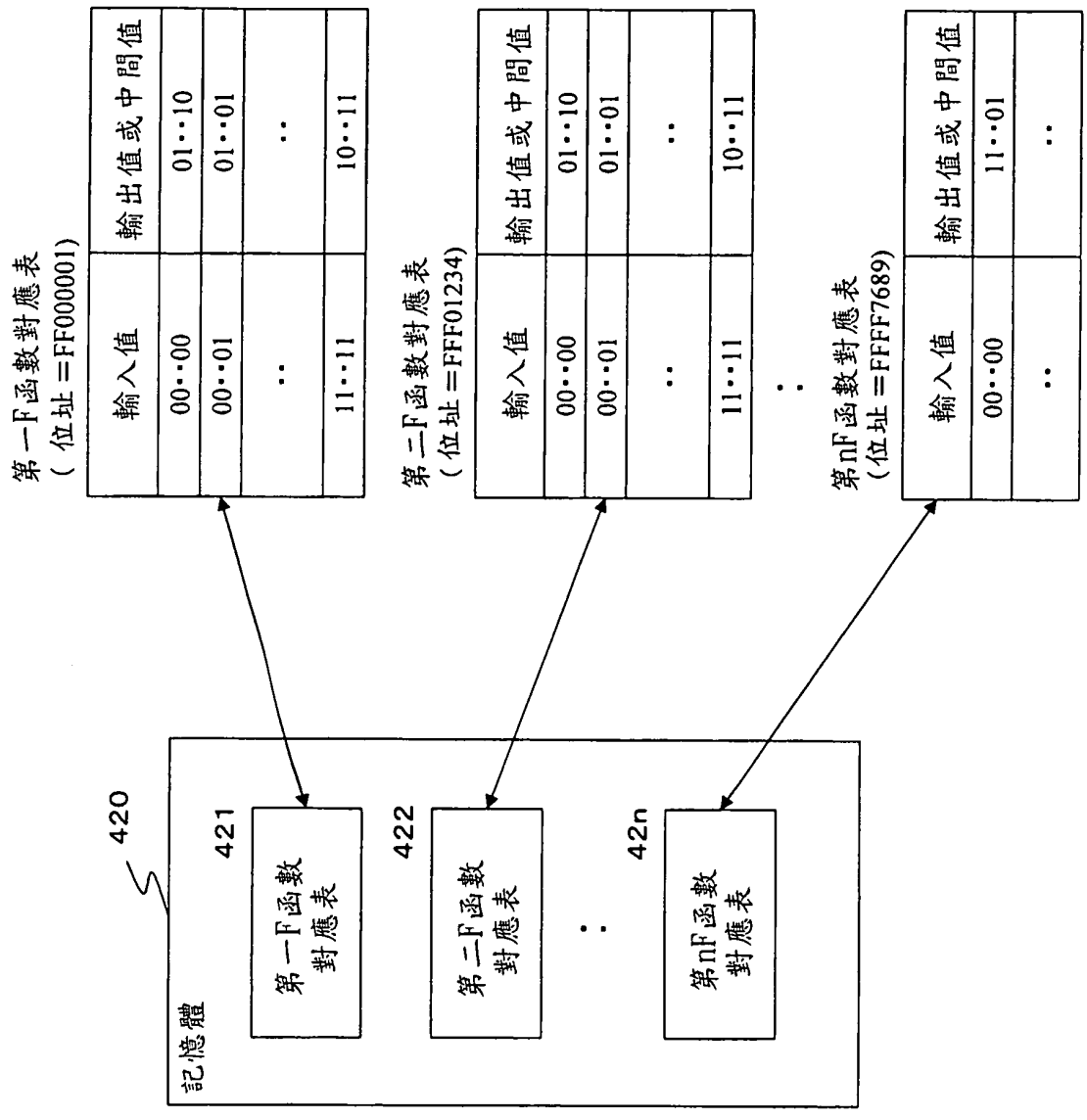

第一F函數對應表
（位址=FF000001）
輸入值
輸出值或中間值
00‥00
01‥10
00‥01
01‥01
‥
‥
11‥11
10‥11
第二F函數對應表
（位址=FFF01234）
輸入值
輸出值或中間值
00‥00
01‥10
00‥01
01‥01
‥
‥
11‥11
10‥11
第nF函數對應表
（位址=FFFF7689）
輸入值
輸出值或中間值
00‥00
11‥01
‥
‥
420
記憶體
421
第一F函數對應表
422
第二F函數對應表
42n
第nF函數對應表

圖9

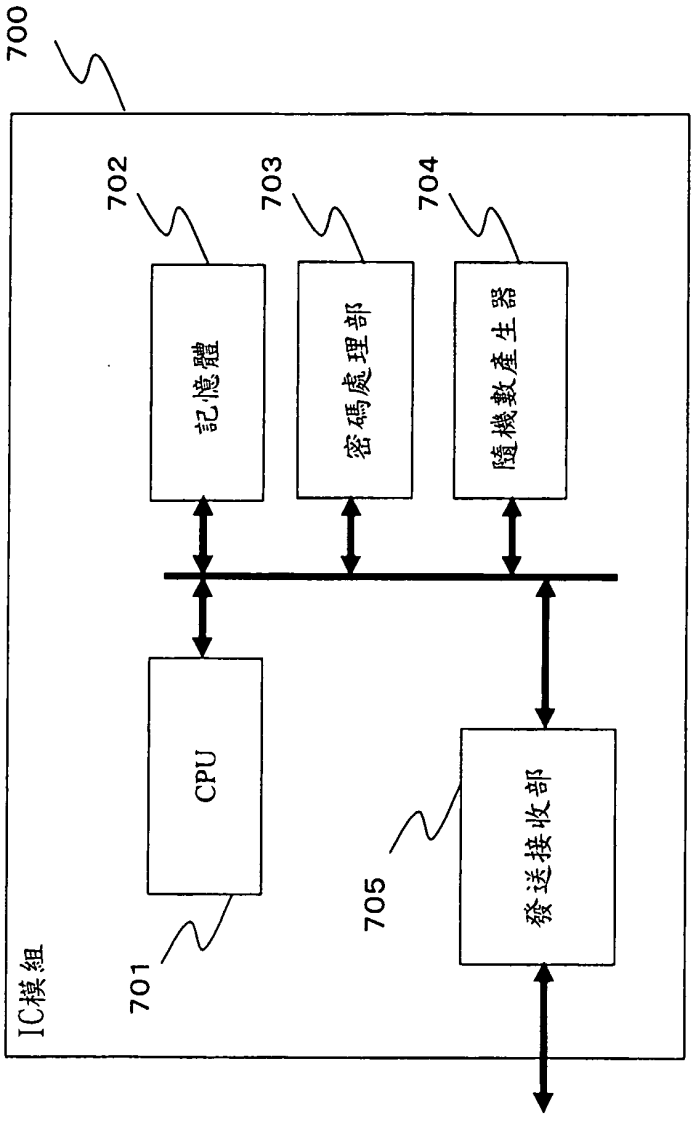


圖10

七、指定代表圖：

(一)本案指定代表圖為：第（ 8 ）圖。

(二)本代表圖之元件符號簡單說明：

400	密碼處理裝置
410	資料處理部
411	回合函數執行部
412	記憶體位址提供部
413	處理序列資訊儲存部
420	記憶體
421、422、42n	F函數對應表

八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

（無）

I380659

發明專利說明書

中文說明書替換頁(101年6月)

（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：96132640

H04L 9/06 (2006.01)

※ 申請日期：96.8.31 ※IPC 分類：G09C1/00 (2006.01)

一、發明名稱：（中文/英文）

密碼處理裝置、密碼處理方法以及密碼處理電腦程式產品、解密處理裝置、解密處理方法以及解密處理電腦程式產品

二、申 請 人：（共 1 人）

姓名或名稱：（中文/英文）

日商新力股份有限公司
SONY CORPORATION

代表人：（中文/英文）

中鉢 良治
CHUBACHI, RYOJI

住居所或營業所地址：（中文/英文）

日本東京都港區港南1丁目7番1號
1-7-1 KONAN, MINATO-KU, TOKYO, 108-0075, JAPAN

國 籍：（中文/英文）

日本 JAPAN

十、申請專利範圍：

1. 一種密碼處理裝置，其特徵在於：其係執行Feistel型公用密鑰區塊密碼處理者，且包含：

資料處理部，其係將包含線性轉換部及非線性轉換部之F函數作為回合函數而反覆執行之資料處理部，其係選擇性應用至少兩種以上不同F函數，執行複數回合之回合運算；及

記憶體，其儲存有複數F函數對應表，該等F函數對應表係將對應於上述兩種以上不同F函數各個的輸入值與輸出值或中間值賦予對應；

上述資料處理部係下述結構：

依據預先規定之密碼處理順序(sequence)，取得與各回合中應用之F函數對應的F函數對應表之存取用位址，並藉由應用取得位址之記憶體存取，讀取對應於各回合F函數的F函數對應表，根據表格參照，取得相對於輸入值之輸出值或中間值，獲得依據各F函數之資料轉換結果；

上述資料處理部係下述結構：

執行依據具有擴散矩陣切換機構(DSM：Diffusion Switching Mechanism)的Feistel結構之密碼處理，上述擴散矩陣切換機構係選擇性應用設定有至少2個以上不同矩陣作為各回合F函數中應用於線性轉換處理的轉換矩陣之至少2個以上不同F函數。

2. 如請求項1之密碼處理裝置，其中上述資料處理部係下

述結構：

執行基於Feistel結構之密碼處理，上述Feistel結構係依據將密碼處理對象資料2分割之資料序列數(分割數)d=2之設定，執行密碼處理。

3. 如請求項1之密碼處理裝置，其中上述資料處理部係下述結構：

執行基於擴展型Feistel結構之密碼處理，上述擴展型Feistel結構係依據將密碼處理對象資料分割為3個以上之資料序列數(分割數)d≧3之設定，執行密碼處理。

4. 如請求項1之密碼處理裝置，其中上述資料處理部係下述結構：

執行預先設定之密碼函數，並於執行該密碼函數時，於各回合適當地切換與各回合中應用之F函數對應的F函數對應表之存取用位址，讀取對應於各回合F函數的F函數對應表，並根據表格參照，取得相對於輸入值之輸出值或中間值，獲得依據各F函數之資料轉換結果。

5. 如請求項1之密碼處理裝置，其中上述記憶體係下述結構：

儲存有將對於各F函數之輸入值或輸入值之構成資料、及F函數之輸出值或中間值或該等構成資料賦予對應之F函數對應表。

6. 一種密碼處理方法，其特徵在於：其係於密碼處理裝置中，執行Feistel型公用密鑰區塊密碼處理者，且包含：

於資料處理部中，將包含線性轉換部及非線性轉換部

之F函數作為回合函數而反覆執行之資料處理步驟，其係選擇性應用至少兩種以上不同F函數，執行複數回合之回合運算之資料處理步驟；

上述資料處理步驟包含下述步驟：

依據預先規定之密碼處理順序，取得與各回合中應用之F函數相對應之F函數對應表之存取用位址；

執行應用上述取得位址之記憶體存取，自儲存有將對應於上述兩種以上不同F函數各個之輸入值與輸出值或中間值賦予對應之複數F函數對應表的記憶體中讀取對應於各回合F函數之F函數對應表；及

參照自記憶體所讀取之表格，取得相對於F函數輸入值之輸出值或中間值，獲得依據各F函數之資料轉換結果；

上述資料處理步驟包含下述步驟：

執行依據具有擴散矩陣切換機構(DSM：Diffusion Switching Mechanism)的Feistel結構之密碼處理，上述擴散矩陣切換機構係選擇性應用設定有至少2個以上不同矩陣作為各回合F函數中應用於線性轉換處理的轉換矩陣之至少2個以上不同F函數。

7. 一種密碼處理電腦程式產品，其特徵在於：其係於密碼處理裝置中，使Feistel型公用密鑰區塊密碼處理執行者，且包含：

於資料處理部中，將包含線性轉換部及非線性轉換部之F函數作為回合函數而反覆執行之資料處理步驟，其

係選擇性應用至少兩種以上不同F函數，執行複數回合之回合運算的資料處理步驟；

上述資料處理步驟係使下述步驟執行之步驟：

依據預先規定之密碼處理順序，取得與各回合中應用之F函數相對應之F函數對應表之存取用位址；

使應用上述取得位址之記憶體存取執行，自儲存有將與上述兩種以上不同F函數各個對應之輸入值與輸出值或中間值賦予對應之複數F函數對應表的記憶體中讀取對應於各回合F函數之F函數對應表；及

使參照自記憶體中所讀取之表格，取得相對於F函數輸入值之輸出值或中間值，取得依據各F函數之資料轉換結果；

上述資料處理步驟包含下述步驟：

執行依據具有擴散矩陣切換機構(DSM：Diffusion Switching Mechanism)的Feistel結構之密碼處理，上述擴散矩陣切換機構係選擇性應用設定有至少2個以上不同矩陣作為各回合F函數中應用於線性轉換處理的轉換矩陣之至少2個以上不同F函數。

8. 一種解密處理裝置，其特徵在於：其係執行Feistel型公用密鑰區塊密碼處理者，且包含：

資料處理部，其係將包含線性轉換部及非線性轉換部之F函數作為回合函數而反覆執行之資料處理部，其係選擇性應用至少兩種以上不同F函數，執行複數回合之回合運算；及

記憶體，其儲存有複數F函數對應表，該等F函數對應表係將對應於上述兩種以上不同F函數各個的輸入值與輸出值或中間值賦予對應；

上述資料處理部係下述結構：

依據預先規定之解密處理順序(sequence)，取得與各回合中應用之F函數對應的F函數對應表之存取用位址，並藉由應用取得位址之記憶體存取，讀取對應於各回合F函數的F函數對應表，根據表格參照，取得相對於輸入值之輸出值或中間值，獲得依據各F函數之資料轉換結果；

上述資料處理部係下述結構：

執行依據具有擴散矩陣切換機構(DSM：Diffusion Switching Mechanism)的Feistel結構之解密處理，上述擴散矩陣切換機構係選擇性應用設定有至少2個以上不同矩陣作為各回合F函數中應用於線性轉換處理的轉換矩陣之至少2個以上不同F函數。

9. 如請求項8之解密處理裝置，其中上述資料處理部係下述結構：

執行基於Feistel結構之解密處理，上述Feistel結構係依據將解密處理對象資料2分割之資料序列數(分割數)d=2之設定，執行解密處理。

10. 如請求項8之解密處理裝置，其中上述資料處理部係下述結構：

執行基於擴展型Feistel結構之解密處理，上述擴展型

Feistel結構係依據將解密處理對象資料分割為3個以上之資料序列數(分割數)d≧3之設定，執行解密處理。

11. 如請求項8之解密處理裝置，其中上述資料處理部係下述結構：

執行預先設定之解密函數，並於執行該解密函數時，於各回合適當地切換與各回合中應用之F函數對應的F函數對應表之存取用位址，讀取對應於各回合F函數的F函數對應表，並根據表格參照，取得相對於輸入值之輸出值或中間值，獲得依據各F函數之資料轉換結果。

12. 如請求項8之解密處理裝置，其中上述記憶體係下述結構：

儲存有將對於各F函數之輸入值或輸入值之構成資料、及F函數之輸出值或中間值或該等構成資料賦予對應之F函數對應表。

13. 一種解密處理方法，其特徵在於：其係於解密處理裝置中，執行Feistel型公用密鑰區塊密碼處理者，且包含：

於資料處理部中，將包含線性轉換部及非線性轉換部之F函數作為回合函數而反覆執行之資料處理步驟，其係選擇性應用至少兩種以上不同F函數，執行複數回合之回合運算之資料處理步驟；

上述資料處理步驟包含下述步驟：

依據預先規定之解密處理順序，取得與各回合中應用之F函數相對應之F函數對應表之存取用位址；

執行應用上述取得位址之記憶體存取，自儲存有將對

應於上述兩種以上不同F函數各個之輸入值與輸出值或中間值賦予對應之複數F函數對應表的記憶體中讀取對應於各回合F函數之F函數對應表；及

參照自記憶體所讀取之表格，取得相對於F函數輸入值之輸出值或中間值，獲得依據各F函數之資料轉換結果；

上述資料處理步驟包含下述步驟：

執行依據具有擴散矩陣切換機構(DSM：Diffusion Switching Mechanism)的Feistel結構之解密處理，上述擴散矩陣切換機構係選擇性應用設定有至少2個以上不同矩陣作為各回合F函數中應用於線性轉換處理的轉換矩陣之至少2個以上不同F函數。

14. 一種解密處理電腦程式產品，其特徵在於：其係於解密處理裝置中，使Feistel型公用密鑰區塊密碼處理執行者，且包含：

於資料處理部中，將包含線性轉換部及非線性轉換部之F函數作為回合函數而反覆執行之資料處理步驟，其係選擇性應用至少兩種以上不同F函數，執行複數回合之回合運算的資料處理步驟；

上述資料處理步驟係使下述步驟執行之步驟：

依據預先規定之解密處理順序，取得與各回合中應用之F函數相對應之F函數對應表之存取用位址；

使應用上述取得位址之記憶體存取執行，自儲存有將與上述兩種以上不同F函數各個對應之輸入值與輸出值

或中間值賦予對應之複數F函數對應表的記憶體中讀取對應於各回合F函數之F函數對應表；及

使參照自記憶體中所讀取之表格，取得相對於F函數輸入值之輸出值或中間值，取得依據各F函數之資料轉換結果；

上述資料處理步驟包含下述步驟：

執行依據具有擴散矩陣切換機構(DSM：Diffusion Switching Mechanism)的Feistel結構之解密處理，上述擴散矩陣切換機構係選擇性應用設定有至少2個以上不同矩陣作為各回合F函數中應用於線性轉換處理的轉換矩陣之至少2個以上不同F函數。