200830233

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：96131712

※ 申請日期：96.8.27　　※IPC 分類：G09C1/00 (2006.01)
H04L 9/06(2006.01)

一、發明名稱：（中文/英文）

資料轉換裝置、資料轉換方法及電腦程式

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

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2006-238227

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】

本發明係關於一種資料轉換裝置、資料轉換方法及電腦程式。進一步詳細而言係關於一種進行可應用於例如共同鍵區塊密碼處理或雜湊函數等之非線性轉換處理之資料轉換裝置、資料轉換方法及電腦程式。

【先前技術】

今日，伴隨著網路通信、電子商務交易發展，通信中之安全確保遂成為重要問題。密碼技術為安全確保之一種方法，現在正實際進行使用各種加密方法之通信。

例如於IC卡等小型裝置中埋入密碼處理模組，於IC卡與作為資料讀取寫入裝置之讀寫機間進行資料收發，以進行認證處理或收發資料之加密、解密之系統已實用化。

存在有各種密碼處理運算法，若予以大致分類可分類為：將加密鍵與解密鍵設定為不同鍵，例如設定作為公開鍵與私密鍵之公開鍵密碼方式；及將加密鍵與解密鍵設定作為共同鍵之共同鍵密碼方式。

共同鍵密碼方式亦存在有各種運算法，其一係以共同鍵為基調來產生複數鍵，使用所產生之複數鍵來重複執行區塊單位(64位元、128位元等)之資料轉換處理之方式。共同鍵區塊密碼方式係應用此種鍵產生方式及資料轉換處理之代表性運算法。

作為代表性之共同鍵區塊密碼之運算法，據知例如過去有美國標準密碼之DES(Data Encryption Standard：資料加

密標準)運算法，及現在之美國標準密碼之AES(Advanced Encryption Standard：先進加密標準)運算法等。

如此之共同鍵區塊密碼之運算法主要藉由具有重複執行輸入資料轉換之回合函數(round function)執行部之密碼處理部，及產生在回合函數部之各回合應用之回合鍵之鍵排程部所構成。鍵排程部係根據私密鍵之主鍵(master key)，首先產生位元數增加之擴張鍵，並根據所產生之擴張鍵來產生在密碼處理部之各回合函數部應用之回合鍵(副鍵)。

作為執行此種運算法之具體構造，據知為具有線性轉換部及非線性轉換部之重複執行回合函數之構造。例如代表性之構造為Feistel構造。Feistel構造係具有藉由單純重複作為資料轉換函數之回合函數(F函數)，來將明文轉換為密文之構造。於回合函數(F函數)中執行線性轉換處理及非線性轉換處理。此外，作為記載有關應用Feistel構造之密碼處理之文獻，有例如非專利文獻1、非專利文獻2。

該共同鍵區塊密碼處理或例如雜湊函數等係藉由非線性轉換處理來執行資料轉換。對於非線性轉換可應用稱為S盒(S-box)之非線性轉換函數。S盒為區塊密碼或雜湊函數之構成要素，為決定其安全性或安裝性能非常重要之函數。S盒一般為n位元輸入、m位元輸出之非線性轉換函數。輸出入位元數為相同數目且輸出入1對1地對應之S盒稱為雙射型S盒。

對於密碼處理之非線性轉換應用S盒之情況時，所應用之S盒之性質會對於密碼之安全性造成甚大影響。亦即，

據知有例如差分解析、線性解析等各種密碼攻擊，藉由此種密碼攻擊解析鍵或運算法之難度越高，則安全性越高。依區塊密碼或雜湊函數所利用之S盒之性質，此安全性係大相逕庭。

例如應用於密碼運算法全體或密碼處理之回合函數本身嚴密之安全性評估，係由於其輸出入尺寸甚大(例如64位元、128位元等)而一般較為困難。然而，S盒之輸出入尺寸一般較小。例如為8位元輸出入程度，可進行嚴密之安全性評估。據知為了提高密碼運算法全體之安全性，對於S盒至少會要求如下特性。

(1)最大差分確率充分小

(2)最大線性確率充分小

(3)進行布耳多項式表現時之布耳代數次數充分大

(4)將輸出入表現為多項式時之項數充分多

主要分別為(1)決定對於差分攻擊之耐受度，(2)決定對於線性攻擊之耐受度，(3)決定對於高階差分攻擊之耐受度，(4)決定對於內插攻擊之耐受度。並且，為了提高安全性，重點在於S盒之輸出入之位元相關低，或使輸入變化1位元時之輸出變化為1/2程度等。

而且，S盒除了要求安全性，亦要求高安裝性能。例如於藉由軟體來執行密碼處理或雜湊函數之安裝架構中，安裝通常於記憶體保持表示對於輸入之輸出之表，藉由查表(表安裝)之方法來執行非線性轉換之架構，因此其安裝性能不甚取決於S盒之內部構造。然而，於硬體安裝中，構

成用以根據例如輸入值來算出特定輸出之電路。此電路架構係依所應用之S盒，其架構會大幅變化，並對於電路規模造成影響。

[非專利文獻1]K. Nyberg, "Generalized Feistel networks (一般化Feistel網路)", 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(不依賴任何未驗證假說來建構安全可證之區塊密文)。CRYPTO 1989: 461-480。

【發明內容】

[發明所欲解決之問題]

本發明係有鑑於上述問題點所實現者，其目的在於改良執行在密碼處理或雜湊函數等所利用之非線性轉換處理之S盒之架構，以提供一種提高對於各種密碼攻擊之耐受性之架構，亦即提供一種提高安全性之資料轉換裝置、資料轉換方法及電腦程式。

[解決問題之技術手段]

本發明之第一面係在於：

一種資料轉換裝置，其特徵為包含：

第一段非線性轉換部，其係包含執行分割輸入資料後之各個分割資料之非線性轉換處理之複數小型非線性轉換部；

線性轉換部，其係輸入所有來自構成前述第一段非線性轉換部之複數小型非線性轉換部之輸出，並執行線性轉換；及

第二段非線性轉換部，其係包含執行分割前述線性轉換部之輸出資料後之各個分割資料之非線性轉換處理之複數小型非線性轉換部；

前述線性轉換部係

藉由具有與前述輸入資料之位元尺寸相同尺寸之要素之矩陣運算來執行資料轉換，且於矩陣為m×m矩陣之情況下，執行應用至少具有m以上分支數之高分支數矩陣之資料轉換處理之架構。

並且，於本發明之資料轉換裝置之一實施態樣中，其特徵為：於前述輸入資料為n位元資料之情況下，前述第一非線性轉換部係包含分別輸入為輸入資料之n位元資料之分割資料之n/k位元，並輸出作為非線性轉換處理結果之n/k位元之k個小型非線性轉換部；前述線性轉換部係輸入前述k個小型非線性轉換部所輸出之總計n位元之資料，並藉由應用高分支數矩陣之資料轉換處理，來產生n位元之輸出之架構；前述第二非線性轉換部係具有分別輸入為從前述線性轉換部輸出之n位元資料之分割資料之n/k位元，並輸出作為非線性轉換處理結果之n/k位元之k個小型非線性轉換部之架構。

並且，於本發明之資料轉換裝置之一實施態樣中，其特徵為：前述線性轉換部係執行應用執行最佳擴散轉換

ODM(Optimal Diffusion Mappings)處理之MDS(Maximum Distance Separable：最大距離可分隔)矩陣之資料轉換處理之架構。

並且，於本發明之資料轉換裝置之一實施態樣中，其特徵為：前述線性轉換部係於前述輸入資料為n位元資料之情況下，執行應用藉由於GF(2)上定義之n次不可約多項式p(x)所定義之擴張體$GF(2^n)$上之矩陣之資料轉換處理之架構。

並且，於本發明之資料轉換裝置之一實施態樣中，其特徵為：前述資料轉換裝置係執行n位元輸出入之非線性轉換處理之S盒(S-box)；前述第一段非線性轉換部及前述第二段非線性轉換部所含之複數小型非線性轉換部，係由執行位元數比n位元少之非線性轉換處理之小型S盒所構成。

並且，於本發明之資料轉換裝置之一實施態樣中，其特徵為：前述資料轉換裝置係執行伴隨非線性轉換處理之密碼處理之架構。

並且，於本發明之資料轉換裝置之一實施態樣中，其特徵為：前述密碼處理為共同鍵區塊密碼處理。

並且，本發明之第二面係在於：

一種資料轉換方法，其特徵為：其係於資料轉換裝置中執行者；且包含：

第一段非線性轉換步驟，其係於第一段非線性轉換部應用複數小型非線性轉換部，執行分割輸入資料後之各個分割資料之非線性轉換處理；

線性轉換步驟，其係於線性轉換部，輸入所有來自構成前述第一段非線性轉換部之複數小型非線性轉換部之輸出，並執行線性轉換；及

第二段非線性轉換步驟，其係於第二段非線性轉換部應用複數小型非線性轉換部，執行分割前述線性轉換部之輸出資料後之各個分割資料之非線性轉換處理；

前述線性轉換步驟係

藉由具有與前述輸入資料之位元尺寸相同尺寸之要素之矩陣運算來執行資料轉換之架構，且於矩陣為m×m矩陣之情況下，執行應用至少具有m以上分支數之高分支數矩陣之資料轉換處理之步驟。

並且，本發明之第三面係在於：

一種電腦程式，其特徵為：其係於資料轉換裝置中使資料轉換處理執行者；且包含：

第一段非線性轉換步驟，其係於第一段非線性轉換部應用複數小型非線性轉換部，使分割輸入資料後之各個分割資料之非線性轉換處理執行；

線性轉換步驟，其係於線性轉換部，輸入所有來自構成前述第一段非線性轉換部之複數小型非線性轉換部之輸出，並使線性轉換執行；及

第二段非線性轉換步驟，其係於第二段非線性轉換部應用複數小型非線性轉換部，使分割前述線性轉換部之輸出資料後之各個分割資料之非線性轉換處理執行；

前述線性轉換步驟係

藉由具有與前述輸入資料之位元尺寸相同尺寸之要素之矩陣運算來執行資料轉換之架構，且於矩陣為m×m矩陣之情況下，使應用至少具有m以上分支數之高分支數矩陣之資料轉換處理執行之步驟。

此外，本發明之電腦程式係例如可對於可執行各種程式碼之電腦系統藉由以電腦可讀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提供之電腦程式。藉由以電腦可讀形式提供此種程式，可於電腦系統上實現與程式相應之處理。

本發明進一步之其他目的、特徵或優點藉由根據後述之本發明實施例或附圖之更詳細說明當可明瞭。此外，本說明書中，系統係指複數裝置之邏輯性集合架構，各架構之裝置不限於位在同一殼體內。

[發明之效果]

若根據本發明之一實施例之架構，由於例如於共同鍵密碼處理或雜湊函數等處理中所執行之非線性轉換處理，係應用藉由複數小S盒(S-box)來執行非線性轉換之第一段非線性轉換部、輸入來自第一段非線性轉換部之所有輸出並執行線性轉換之線性轉換部、及由執行線性轉換部之輸出資料分割後之各個分割資料之非線性轉換處理之複數小型非線性轉換部所組成之第二段非線性轉換部，來進行資料轉換之架構，且線性轉換部應用進行最佳擴散轉換之矩陣來執行資料轉換而構成，因此不過度增大從資料輸入至輸出之要徑(critical path)即可實現適當之資料擴散，可實現

對於各種密碼攻擊之耐受度強之安全性高之資料轉換。

【實施方式】

以下，說明有關本發明之資料轉換裝置、資料轉換方法及電腦程式之詳細。說明係按照以下項目來進行。

1.共同鍵區塊密碼之概要

2.密碼攻擊之概要

3.有關組合複數小型S盒而成之非線性轉換處理架構

(3-1)有關組合複數小型S盒而成之非線性轉換處理架構之有效性

(3-2)有關組合以往型之複數小型S盒而成之非線性轉換處理架構及問題點

(3-3)有關組合本發明之複數小型S盒而成之非線性轉換處理架構

4.密碼處理裝置之架構例

[1.共同鍵區塊密碼之概要]

首先，說明有關本發明可應用之共同鍵區塊密碼之概要。於本說明書中，共同鍵區塊密碼(以下記作區塊密碼)係指以下所定義者。

區塊密碼係輸入明文P及鍵K，並輸出密文C。明文及密文之位元長稱為區塊尺寸，於此以n表示。n可取定任意整數值，通常係對各區塊密碼運算法而預先決定1個值。區塊長為n之區塊密碼亦可稱為n位元區塊密碼。

鍵之位元長係以k表示。鍵可取定任意整數值。共同鍵區塊密碼運算法係對應1個或複數之鍵尺寸。例如可能有

對應某區塊密碼運算法A為區塊尺寸n=128，鍵之位元長k=128，或k=192或k=256之各種鍵尺寸之架構。

明文[P]、密碼[C]、鍵[K]之各位元尺寸係如下所示。

明文P：n位元

密文C：n位元

鍵K：k位元

於圖1表示對應k位元之鍵長之n位元共同鍵區塊密碼運算法E之圖。如圖1所示，共同鍵區塊密碼處理部E10係輸入n位元之明文P及k位元之鍵K，並執行預先決定之密碼運算法，輸出n位元之密文C。此外，於圖1僅表示從明文產生密文之加密處理。從密文產生明文之解密處理一般使用密碼處理部E10之反函數。但依密碼處理部E10之構造，於解密處理中亦可應用相同之共同鍵區塊密碼處理部E10，並可藉由鍵輸入順序等之序列變更來實現解密處理。

參考圖2來說明有關圖1所示之共同鍵區塊密碼處理部E10之內部架構。區塊密碼可分為兩部分來思考。其一為輸入鍵K，藉由某設定之步驟來擴張輸入鍵K之位元長，並輸出擴張鍵K'(位元長k')之鍵排程部11；以及接受明文P及從鍵排程部11輸入之擴張鍵K'，並輸入明文P，執行應用擴張鍵K'之密碼處理，並執行用以產生密文C之資料轉換之密碼處理部12。此外，如先前所說明，依密碼處理部12之構造，亦會有亦可對於將密文回復成明文之資料解密處理應用密碼處理部12之情況。

接著，參考圖3來說明有關圖2所示之密碼處理部12之詳

細架構。如圖3所示，密碼處理部12係具有重複執行應用回合函數執行部20之資料轉換之架構。亦即，密碼處理部12可分割為回合函數執行部20之處理單位。回合函數執行部20係作為輸入而接受前段之回合函數執行部之輸出X_i、及根據擴張鍵所產生之回合鍵RK_i之2種資料，於內部執行資料轉換處理，並將輸出資料X_{i+1}輸出至下一回合函數執行部。此外，於第一回合，輸入係明文或對於明文之初始化處理資料。而且，最終回合之輸出為密文。

於圖3所示之例中，密碼處理部12係具有r個回合函數執行部20，且重複r次之回合函數執行部之資料轉換以產生密文之架構。回合函數之重複次數稱為回合數。圖示之例中，回合數為r。

各回合函數執行部之輸入資料X_i係加密中途之n位元資料，某回合之回合函數之輸出X_{i+1}係供給作為下一回合之輸入。各回合函數執行部之另一輸入資料係使用根據從鍵排程所輸出之擴張鍵K'之資料。此輸入於各回合函數執行部並應用於回合函數執行之鍵係稱為回合鍵。圖中，應用於i回合之回合鍵表示作為RK_i。擴張鍵K'係構成作為例如r回合份之回合鍵RK_1~RK_r之連結資料。

圖3所示之架構係從密碼處理部12之輸入側看來，第一個回合之輸入資料設為X_0，從第i個回合函數輸出之資料設為X_i，回合鍵設為RK_i而表示之密碼處理部12之架構。此外，依此密碼處理部12之構造，可成為例如將所應用之回合鍵之應用序列設定成與加密處理相反，將密文輸入於

密碼處理部12，藉此可輸出解密文之架構。

圖3所示之密碼處理部12之回合函數執行部20可採取各種型態。回合函數可依其密碼運算法所採用之構造(structure)來分類。作為代表性構造存在有：

(甲)SPN(Substitution Permutation Network：取代置換網路)構造；

(乙)Feistel構造；

(丙)延伸Feistel構造。

以下，參考圖4~圖6來說明有關此等之具體架構。

(甲)SPN構造回合函數

首先，參考圖4來說明有關作為回合函數執行部20之一架構例之SPN構造回合函數。SPN構造回合函數執行部20a係具有連接有非線性轉換層(S層)及線性轉換層(P層)之所謂SP型之架構。如圖4所示，其藉由對於n位元之輸入資料全部執行與回合鍵之互斥或(XOR)運算之互斥或運算部21、輸入互斥或運算部21之運算結果並執行輸入資料之非線性轉換之非線性轉換處理部22、及輸入非線性轉換處理部22之非線性轉換處理結果並執行對於輸入資料之線性轉換處理之線性轉換處理部23等所構成。線性轉換處理部23之線性轉換結果輸出至下一回合。於最終回合成為密文。此外，於圖4所示之例中，表示互斥或運算部21、非線性轉換處理部22、線性轉換處理部23之處理順序，但此等處理部之順序不受限定，以其他序列來進行處理之架構亦可。

(乙)Feistel構造

接著，參考圖5來說明作為回合函數執行部20之一架構例之Feistel構造。如圖5所示，Feistel構造係將從前面回合之輸入(於第一回合為輸入文)之n位元輸入資料分割為n/2位元之兩個資料，於各回合一面置換一面執行處理。

於應用具有Feistel構造之回合函數執行部20b之處理中，如圖示，一方之n/2位元資料及回合鍵輸入於F函數部30。F函數部30係與上述SPN構造相同，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型之架構。

來自前面回合之n/2位元資料及回合鍵輸入於F函數部30之互斥或運算部31，並進行互斥或(XOR)處理。並且，將此結果資料輸入於非線性轉換處理部32，並執行非線性轉換，且進一步於線性轉換處理部33輸入此非線性轉換結果，執行線性轉換。此線性轉換結果係作為F函數處理結果資料而輸出。

並且，將此F函數輸出及從前面回合輸入之另一個n/2位元輸入，輸入於互斥或運算部34，執行互斥或運算(XOR)，並將執行結果設定作為下一回合之F函數之輸入。此外，設定於圖示之第i回合之F函數輸入之n/2位元係應用於與下一回合之F函數輸出之互斥或運算。如此，Feistel構造係執行一面於各回合交互地置換輸入，一面應用F函數之資料轉換處理。

(丙)延伸Feistel構造

接著，參考圖6來說明有關回合函數執行部20之一架構

例之延伸Feistel構造。首先，參考圖5所說明之Feistel構造係將n位元之明文分割為二，各區分為n/2位元來執行處理。亦即，分割數：d=2之處理。此外，此分割數亦稱為資料系列數。

延伸Feistel構造係此資料系列數(分割數)d設定為3以上之任意整數。可定義因應資料系列數(分割數)d值之各種延伸Feistel構造。圖6所示之例中，資料系列數(分割數)d=4，對於各系列輸入有n/4位元之資料。於各回合中，執行1個以上之作為回合函數之F函數。圖示之例係於1回合中藉由2個F函數部進行回合運算之架構例。

F函數部41，42之架構係與先前參考圖5所說明之F函數部30之架構相同，成為執行回合鍵與輸入值之互斥或運算、及非線性轉換處理、線性轉換處理之架構。此外，輸入於各F函數部之回合鍵係調整為輸入位元與位元數一致。圖示之例中，輸入於各F函數部41，42之回合鍵為n/4位元。此等鍵係進一步將構成擴張鍵之回合鍵予以位元分割而產生。此外，資料系列數(分割數)設為d時，輸入於各系列之資料為n/d位元，輸入於各F函數之鍵之位元數亦調整為n/d位元。

此外，圖6所示之延伸Feistel構造係資料系列數(分割數)設為d，各回合中同時執行d/2之F函數之架構例，但延伸Feistel構造可為於各回合中執行1個以上、d/2以下之F函數之架構。

如參考圖4~圖6所說明，共同鍵區塊密碼之密碼處理部

12之回合函數執行部20可採取如下構造：

(甲)SPN(Substitution Permutation Network：取代置換網路)構造；

(乙)Feistel構造；

(丙)延伸Feistel構造。

此等回合函數執行部全都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型之架構。亦即，具有執行非線性轉換處理之非線性轉換處理部、及執行線性轉換處理之線性轉換處理部。以下，說明有關此等轉換處理架構。

(非線性轉換處理部)

參考圖7來說明有關非線性轉換處理部之具體例。如圖7所示，具體而言，非線性轉換處理部50係排列有m個稱為S盒(S-box)51之s位元輸入s位元輸出之非線性轉換表，ms位元之輸入資料各分割為s位元，輸入於分別相對應之S盒(S-box)51而被轉換資料。於各S盒51執行例如應用轉換表之非線性轉換處理。

若增大輸入之資料尺寸，安裝上之成本傾向變高。為了避免此，多半如圖7所示，採取將處理對象資料X分割為複數單位，對於各個施以非線性轉換之架構。例如輸入尺寸設為ms位元時，分割為各s位元之m個資料，並對於m個S盒(S-box)51分別輸入s位元，執行應用例如轉換表之非線性轉換處理，合成此等各S位元輸出m個而獲得ms位元之非線性轉換結果。

(線性轉換處理部)

參考圖8來說明有關線性轉換處理部之具體例。線性轉換處理部係將輸入值之例如來自S盒之輸出資料之ms位元之輸出值，作為輸入值X輸入，對於此輸入施以線性轉換，並輸出ms位元之結果。線性轉換處理係執行例如輸入位元位置之置換處理等線性轉換處理，並輸出ms位元之輸出值Y。線性轉換處理係例如對於輸入應用線性轉換矩陣，以進行輸入位元位置之置換處理。此矩陣之一例為圖8所示之線性轉換矩陣。

於線性轉換處理部所應用之線性轉換矩陣之要素為擴張體：$GF(2^8)$之體要素或GF(2)之要素等，一般可作為應用各種表現之矩陣來構成。圖8係表示具有ms位元輸出入，並藉由在$GF(2^S)$上定義之m×m矩陣所定義之線性轉換處理部之一架構例。

[2.密碼攻擊之概要]

作為對於上述共同鍵區塊密碼之密碼攻擊，亦即作為所應用之鍵之解析或運算法之解析方法，據知有各種方法。以下，說明有關此密碼攻擊之概要。依序說明有關以下各攻擊。

(2-1)差分攻擊

(2-2)線性攻擊

(2-3)高階差分攻擊

(2-4)內插攻擊

(2-1)差分攻擊

作為共同鍵密碼之攻擊法之一，存在有差分解讀法(Differential Cryptanalysis)。關於差分解讀法係於例如文獻「E. Biham, A. Shamir, "Differential Cryptanalysis of DES-like Cryptosystems(類DES加密之差分解讀法), "Journal of Cryptology, Vol. 4, No. 1, pp. 3-72, 1991.」中有描述。

此攻擊法係對於某密碼觀測稱為差分值之資料之傳播，於該差分值之傳播以高確率發生之情況時可攻擊，亦即可推測出鍵之攻擊法。此稱為差分值之資料之傳播確率稱為差分確率。

對於n位元輸出入之函數f，定義輸入為x(n位元)，輸入差分值為Δx(n位元)，輸出差分值為Δy(n位元)時，如下定義對於函數f之輸入差分值Δx、輸出差分值Δy之差分確率$DP_f(\Delta x、\Delta y)$。

[數1]

$$DP_f(\Delta x,\Delta y)=\frac{\#\{x\in\{0,1\}^n \mid f(x)\oplus f(x\oplus\Delta x)=\Delta y\}}{2^n}$$

而且，如下定義對於函數f之最大差分確率MDP_f。

[數2]

$$MDP_f=\max_{\Delta x\neq 0,\Delta y} DP_f(\Delta x,\Delta y)$$

此等值係藉由函數f唯一地求出之值，最大差分確率MDP_f大之函數f係對於差分攻擊脆弱之函數。故，設計密碼時，宜設計儘可能縮小MDP_f之函數f。

(2-2)線性攻擊

並且，作為共同鍵密碼之攻擊法之一，存在有線性解讀法(Linear Cryptanalysis)。關於線性解讀法係於例如文獻「M. Matsui, "Linear Cryptanalysis Method for DES Cipher(DES密文用之線性解讀法), "EUROCRYPT'93, LNCS 765, pp. 386-397, 1994.」中有描述。

此攻擊法係對於某密碼，觀測輸入之特定位元之互斥或與輸出之特定位元之互斥或間之相關，於找到強力之相關關係之情況時可攻擊，亦即可推測出鍵之攻擊法。此輸出入之特定位元之相關係數稱為線性確率。

對於n位元輸出入之函數f，定義輸入為x(n位元)，輸入遮罩值為Γx(n位元)，輸出遮罩值為Γy(n位元)時，如下定義對於函數f之輸入遮罩值Γx、輸出遮罩值Γy之線性確率$LP_f(\Gamma x、\Gamma y)$。

[數3]

$$LP_f(\Gamma x,\Gamma y)=\left(2\cdot\frac{\#\{x\in\{0,1\}^n \mid x\bullet\Gamma x=f(x)\bullet\Gamma y\}}{2^n}-1\right)^2$$

其中，於上式中，[・]表示n位元向量彼此之內積運算。

[數4]

$$x\bullet y=\oplus_{i=1}^{n}(x_i\cdot y_i)$$

而且，如下定義對於函數f之最大線性確率MLP_f。

[數5]

$$MLP_f = \max_{\Gamma x, \Gamma y \neq 0} LP_f(\Gamma x, \Gamma y)$$

此等值係藉由函數f唯一地求出之值，最大線性確率MLP_f大之函數f係對於線性攻擊脆弱之函數。故，設計密碼時，宜設計儘可能縮小MLP_f之函數f。

(2-3)高階差分攻擊

並且，作為共同鍵密碼之攻擊法之一，存在有高階差分攻擊法(Higher Order Differential Attack)。關於高階差分攻擊法係於例如文獻「L. R. Knudsen, "Truncated and Higher Order Differentials(截斷式及高階差分), "FSE'94, LNCS 1008, pp. 196-211」中有描述。

此攻擊法係利用密碼運算法所具有之代數性質之攻擊法，於以明文之所有位元將密文表現為布耳多項式時，在其布耳代數次數相對於明文之特定位元變得比某次數小之情況時可攻擊，亦即可推測出鍵之攻擊法。

(2-4)內插攻擊

並且，作為共同鍵密碼之攻擊法之一，存在有內插攻擊法(Interpolation Attack)。關於內插攻擊係於例如文獻「T. Jakobsen and L. R. Knudsen, "The Interpolation Attack on Block Cipher(區塊密文之內插攻擊), "FSE'97, LNCS 1267, pp. 28-40, 1997」中有描述。

此攻擊法係利用密碼運算法所具有之代數性質之攻擊法，在將加密函數表現作為多項式函數時其項數少之情況時，藉由復原包含鍵值之加密函數來進行攻擊之攻擊法。

[3.有關組合複數小型S盒而成之非線性轉換處理架構]

(3-1)有關組合複數小型S盒而成之非線性轉換處理架構之有效性

如上述，共同鍵區塊密碼係藉由回合函數之重複來進行密碼處理之架構。此共同鍵區塊密碼處理係重複執行回合函數之架構，於回合函數中執行線性轉換處理及非線性轉換處理。於非線性轉換處理中，例如參考圖7所說明，執行應用S-box(S盒)之非線性轉換處理。除了上述共同鍵區塊密碼處理以外，例如於雜湊函數等之資料轉換中，亦可對於非線性轉換處理應用S盒。

如先前所說明，此S盒之輸出入尺寸一般較小，可進行嚴密之安全性評估，為了提高密碼或雜湊運算法全體之安全性，作為對於S盒所要求之特性，據知有以下特性。

(1)最大差分確率充分小

(2)最大線性確率充分小

(3)進行布耳多項式表現時之布耳代數次數充分大

(4)將輸出入表現為多項式時之項數充分多

主要分別為(1)決定對於差分攻擊之耐受度，(2)決定對於線性攻擊之耐受度，(3)決定對於高階差分攻擊之耐受度，(4)決定對於內插攻擊之耐受度。並且，為了提高安全性，重點在於S盒之輸出入之位元相關低，或使輸入變化1位元時之輸出變化為1/2程度等。

而且，S-box除了要求安全性，亦要求高安裝性能。例如於藉由軟體來執行密碼處理或雜湊函數之安裝架構中，安裝通常於記憶體保持表示對於輸入之輸出之表，藉由查

表(表安裝)之方法來執行非線性轉換之架構，因此其安裝性能不甚取決於S-box之內部構造。然而，於硬體安裝中，構成用以根據例如輸入值來算出特定輸出之電路。此電路架構係依所應用之S-box，其架構會大幅變化，並對於電路規模造成影響。

為了維持密碼運算法或雜湊運算法之安全性，作為對於S-box所要求之特性，如前述有以下特性：

(1)最大差分確率充分小

(2)最大線性確率充分小

(3)進行布耳多項式表現時之布耳代數次數充分大

(4)將輸出入表現為多項式時之項數充分多

作為效率良好地產生符合此要求之S-box之方法，使用擴張體上之冪積函數之方法係廣為人知。若以此方法適當選擇擴張體之次數與冪積之乘數，可產生特性非常良好之S-box。

實際上設定n位元輸出入S-box之輸入為x，輸出為y，其分別為擴張體$GF(2^n)$之元素之情況時，

y=f(x)以下式賦予之情況時，

[數6]

$$y = x^{2^t+1}$$

(t為任意整數)

$$y = x^{-1}$$

據知於最大差分確率、最大線性確率之點可構成最佳之S-box。

作為以此方法構成之S-box之例，可舉出在AES、Camellia、MISTY中應用之S-box等。

由於AES或Camellia之S-box亦可作為$GF((2^4)^2)$上之反原函數來構成S-box，因此從安全性觀點考量，其特性非常良好，進一步可謂亦具有非常高之硬體安裝性能。

然而，近年來，關於此種S-box，亦被指出利用其特徵性之代數性質之攻擊法、或關於其太過平均之擴散性之問題點等。

有鑑於此點而思慮未具特徵性之代數性質之S-box之構成法，即思慮為了使其不具明顯之代數構造，藉由以隨機或依據其之方法來選擇要素之方法，以產生S-box之方法。

若以此方法來產生S-box，於大多數之情況下會不具特徵性之代數構造，並且未進行如擴張體上之冪積函數之平均擴散，因此可謂對於如上述問題取得對策。

然而，由於n位元輸出入之雙射S-box之數目存在有2^n階乘個，因此於實際上隨機產生n位元輸出入之S-box並逐一檢查其特性之方法中，若n增大某程度，則難以有效率地產生特性良好之S-box。

而且，完全隨機選擇S-box之要素之情況時，由於以硬體安裝時，主要亦僅可使用稱為表安裝之方法，因此安裝效率大幅降低。

因此問題而嘗試隨機產生具有小尺寸輸出入之S-box，並組合其等複數個來產生更大之S-box。例如：

CRYPTON ver. 0.5、

CRYPTON ver. 1.0、

Whirlpool、

FOX等

其S-box等可視為根據此種方法所產生之S-box。以下，說明有關此等之具體架構例及其問題點。

(3-2)有關組合以往型之複數小型S盒而成之非線性轉換處理架構及問題點

以下，針對以下各架構來說明有關組合以往型之複數小型S盒而成之非線性轉換處理架構及問題點。

(a)CRYPTON ver. 0.5、

(b)CRYPTON ver. 1.0、

(c)Whirlpool、

(d)FOX

(a)CRYPTON ver. 0.5

例如CRYPTONver. 0.5之S-box係具有圖9所示之構造。S-box[S40]101、S-box[S41]102、S-box[S42]103為4位元輸出入之S-box，具有組合此等3個S-box與互斥或運算部111~113，將輸入8位元進行非線性轉換而獲得輸出8位元之架構。此外，於圖示之S-box之標示[$S4_n$]，4表示4位元輸出入之S盒，n為S-box之識別符。S-box[$S4_0$]101、S-box[$S4_1$]102、S-box[$S4_2$]103均為4位元輸出入之S-box，且

為執行分別不同之非線性轉換處理之不同之S-box。

由於此構造係採用所謂3段Feistel構造，因此布耳代數次數變低，並且要徑甚長。亦即，成為從輸入至獲得最終輸出為止，必須通過3個小S-box之架構。因此，具有安裝性能不甚高之特徵。

(b)CRYPTON ver. 1.0

而且，CRYPTON ver. 1.0之S-box係具有圖10所示之構造。由S-box[$S4_0$]121、S-box[$S4_1$]122、執行S-box[$S4_1$]122之逆向轉換之S-box[$S4_1^{-1}$]123、執行S-box[$S4_0$]121之逆向轉換之S-box[$S4_0^{-1}$]124、及藉由位元運算來執行線性轉換處理之位元運算部131, 132所構成。

於S-box[$S4_0$]121將輸入8位元之高位4位元執行非線性轉換後，進行輸入於位元運算部131之線性轉換，將其結果輸入於S-box[$S4_1^{-1}$]123並輸出非線性轉換結果。關於低位4位元，於S-box[$S4_1$]122執行非線性轉換後，進行輸入於位元運算部131之線性轉換，將其結果輸入於S-box[$S4_0^{-1}$]123並輸出非線性轉換結果。

由於此構造必須從1位元要素8x8矩陣，亦即從64位元之空間選擇中途使用之位元運算部131之位元運算，因此其選擇變難。亦即，於非線性轉換要求基本上從非線性轉換對象之輸入8位元，作為與各輸入8位元相對應之非線性轉換結果之輸出8位元而獲得未有偏離之輸出之架構，具有難以選擇用以使得中段之位元運算部131, 132所應用之矩陣成為符合此要求之矩陣之問題。

(c)Whirlpool

而且，Whirlpool之S-box係具有圖11所示之構造。其具有使用S-box[$S4_0$]141，144、執行S-box[$S4_0$]之逆向轉換之S-box[$S4_0^{-1}$]142，145、及執行S-box[$S4_1$]143，藉由互斥或運算部151~153來結合此等S-box之架構。

此構造中，所需之小S-box之數目多達5個，並且要徑甚長。亦即，其為從輸入達到最終輸出為止，必須通過3個小S-box之架構，具有安裝性能不甚高之問題。

(d)FOX

並且，FOX之S-box係具有圖12所示之架構。其具有使用3種4位元輸出入S-box161~163及4位元輸出入或電路171，172，並藉由互斥或運算部來連接此等之架構。

此構造中，所需之小S-box之數目少至3個，但全體而言互斥或運算部(XOR)之數目多，要徑亦長。為了從輸入至獲得最終輸出，必須通過3個小S-box。因此，具有安裝性能不甚高之問題。

(3-3)有關組合本發明之複數小型S盒而成之非線性轉換處理架構

接著，說明有關組合本發明之複數小型S盒而成之非線性轉換處理架構。如上述，關於組合複數小型S盒而成之非線性轉換處理架構，已提案有複數類型，但分別具有要徑長之問題點或線性轉換矩陣之設定困難等問題點。

首先，說明有關理解按照以下本發明之非線性轉換處理架構所需之以下用語。

(a)分支數及最佳擴散層

(b)擴張體上之矩陣運算

(a)分支數及最佳擴散層

首先，說明有關分支數及最佳擴散轉換(Optimal Diffusion Mappings)。

對於從n×a位元資料對於n×b位元資料之映射

θ：{0, 1}na→{0, 1}nb

如下定義分支數Bn(θ)。

[數7]

$$B_n(\theta) = \min_{\alpha \neq 0}\{hw_n(\alpha) + hw_n(\theta(\alpha))\}$$

其中，$\min_{\alpha \neq 0}\{X_\alpha$表示$\}$符合$\alpha \neq 0$之所有$X_\alpha$中之最小值，$hw_n(Y)$係於每n位元區劃位元行Y而表示時，遞迴n位元之資料並非全部均為0(非零)之要素之函數。此時，分支數B(θ)為b＋1之映射θ定義為最佳擴散轉換(Optimal Diffusion Mappings)。而且，以下定義符合ODM之矩陣為MDS(Maximum Distance Separable：最大距離可分隔)矩陣。

(b)擴張體上之矩陣運算

由在基礎體GF(2)上定義之n次不可約多項式p(x)所做成之擴張體$GF(2^n)$上所進行之矩陣運算，係稱為擴張體上之矩陣運算。

例如：

[數8]

$$\begin{pmatrix} y_0 \\ y_1 \end{pmatrix} = \begin{pmatrix} a_{0,0} & a_{0,1} \\ a_{1,0} & a_{1,1} \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \end{pmatrix}$$

思考上述矩陣運算。

於上述矩陣運算中，輸出y_0, y_1分別表現如下：

$y_0=a_{0,0}x_0+a_{0,1}x_1$

$y_1=a_{1,0}x_0+a_{1,1}x_1$

此時，$a_{0,0}$、x_0等該類變數全部視為擴張體GF(2^n)上之元素，運算全部在擴張體GF(2^n)上進行。以此方法進行矩陣運算之方法稱為擴張體上之矩陣運算。

關於本發明之非線性轉換處理架構係實現解決上述組合以往之複數小型S盒而成之非線性轉換處理架構中之問題點，亦即解決要徑長之問題點、或線性轉換矩陣之設定困難等問題點之非線性轉換處理架構。

於本發明之架構中，為了效率良好地產生難以在擴張體GF(2^n)上進行簡單表現，且具有高度安裝性能(特別是硬體)之n位元輸出入之雙射S-box，而於小S-box之組合位置組合具有與分支數高之小S-box之輸出入尺寸相同尺寸之要素之矩陣運算，以實現作為大S-box之非線性轉換處理架構。具體而言，分支數高之矩陣運算係表示對於m×m矩陣具有分支數m以上之矩陣。

作為分支數高之矩陣係選擇例如執行前述最佳擴散轉換之MDS(Maximum Distance Separable：最大距離可分隔)矩陣。MDS矩陣為構成矩陣之任意小矩陣為正則矩陣之矩陣。此外，若正則矩陣為具有反矩陣之矩陣，矩陣設為

A，反矩陣設為A^{-1}，則：

$AA^{-1}=A^{-1}A=E$

其中，E為單位矩陣，

具有上式成立之反矩陣A^{-1}之矩陣A為正則矩陣。

於圖13表示作為有關本發明之一實施例之非線性轉換處理架構之n位元輸出入S-box之架構例。圖13所示之架構係由4個n/2位元輸出入之雙射S-box201~204、及由在擴張體$GF(2^{n/2})$定義之2x2MDS(Maximum Distance Separable：最大距離可分隔)矩陣所組成之線性轉換處理部211所構成之執行n位元輸出入之非線性轉換處理之架構。

輸入n位元係高位各n/2位元、低位各n/2位元，分別輸入於n/2位元輸出入之雙射S-box[S_0]201、S-box[S_1]202，並於各S-box進行非線性轉換處理後，輸入於在擴張體$GF(2^{n/2})$定義之2x2MDS矩陣所組成之線性轉換處理部211，根據MDS矩陣進行線性轉換處理後，線性轉換結果之n位元之高位各n/2位元、低位各n/2位元分別輸入於n/2位元輸出入之雙射S-box[S_2]203、S-box[S_3]204，於各S-box進行非線性轉換處理而獲得作為輸出結果之n位元之架構。

若利用於圖13所示之線性轉換處理部211中應用如MDS矩陣之分支數高之擴散轉換矩陣，則保證前段之小S-box[S_0]201、S-box[S_1]202之輸出會對於後段之小S-box[S_2]203、S-box[S_3]204之輸入均衡地配置，因此可產生全體特性良好之大S-box。而且，線性轉換處理部211中應

用之相當於擴散轉換矩陣之MDS矩陣之要素尺寸係由小S-box之輸出入尺寸(n/2)唯一地決定，因此即使大S-box之輸出入尺寸(n)變大，可選擇之矩陣空間仍有限，因此可容易地檢查該矩陣之分支數。

由於圖13所示之架構之線性轉換處理部211中應用之作為擴散轉換矩陣之MDS矩陣之要素尺寸為n/2位元，且為2×2矩陣，因此要素數為4個，即使調查全矩陣，該數目仍為$2^{n/2\times4}$種程度，因此可容易調查全矩陣。其中，矩陣運算係由在GF(2)上定義之n次不可約多項式p(x)所做成之擴張體$GF(2^n)$上之矩陣運算。

若以此方法產生S-box，則據判由於可實現簡易之代數表現限於圖13所示之架構中之輸出入尺寸n/2位元小之S-box201~204，因此在擴張體$GF(2^n)$上之要素看似隨機。故，可判斷難以在$GF(2^n)$上進行單純之代數表現。而且，可期待不會如在擴張體上之冪積般平均地擴散。

並且，若適當選擇矩陣，則能以簡易運算及短路徑來構成，因此相較於以n位元隨機地產生之S-box、或組合以往之小S-box所構成之S-box，可謂安裝效率甚高。

參考圖14~圖17，來說明有關應用圖13所示之架構來執行具體之8位元輸出入之非線性轉換之S-box之架構例。

圖14(a)、圖15(a)所示之架構相同，其表示作為應用圖13所示之架構來執行具體之8位元輸出入之非線性轉換之S-box之一架構例之8位元S-box300之架構之圖。圖14(b)係表示圖14(a)所示之8位元S-box300之構成要素之4個4位元

輸出入S-box301~304之轉換表。使用此表之數值為16進位。該表係表示對於輸入：x=0~F(16進位)之各S-box301~304之輸出值。而且，於圖15(c)表示作為圖15(a)(=圖14(a))所示之線性轉換處理部311而使用分支數高之擴散轉換，具體而言使用最佳擴散轉換[ODM]之MDS矩陣(matrix)311之具體例。

說明有關圖14(a)所示之執行8位元輸出入之非線性轉換之S-box之處理。首先，8位元S-box300之輸入之x(8位元)分割為1/2，亦即每4位元分割為x[0], x[1]。接著，分別將x[0]對於4位元輸出入之S-box[$S4_0$]301輸入，將x[1]對於4位元輸出入之S-box[$S4_1$]302輸入，獲得作為各S-box301, 302之非線性轉換結果之輸出w[0], w[1]。S-box[$S4_0$]301、S-box[$S4_1$]302係隨機選擇之4位元S-box，非線性轉換係作為按照圖14(b)之表之轉換處理來執行。

此外，S-box[$S4_0$]301、S-box[$S4_1$]302係符合最大差分確率充分低或最大線性確率充分低等S-box所應符合之所有性質之S-box。而且，由於此等S-box為4位元輸出入，因此實際上可尋找符合此性質之S-box。

S-box[$S4_0$]301、S-box[$S4_1$]302之輸出w[0], w[1]係輸入於藉由最佳擴散轉換[ODM]之MDS矩陣(matrix)來執行線性轉換之線性轉換處理部311，並作為藉由MDS矩陣(matrix)所獲得之線性轉換結果而輸出z[0], z[1]。於線性轉換處理部311，藉由在GF(2)上定義之4次不可約多項式：$p(x)=x^4+x+1$所做成之擴張體$GF(2^4)$上之矩陣運算，

來執行線性轉換，並輸出z[0], z[1]。作為線性轉換處理部311之MDS矩陣(matrix)係根據，以GF(2)上之4次不可約多項式所定義之擴張體$GF(2^4)$上之元素作為要素所具有之2x2之4要素所組成之矩陣，來執行線性轉換處理。

於圖15(c)表示矩陣運算之具體處理。應用圖15(c)所示之2x2之MDS矩陣之情況時，根據輸入w[0], w[1]，如下算出輸出z[0], z[1]。

z[0]=w[0](XOR)w[1]x2

z[1]=w[0]x2(XOR)w[1]

分別將作為藉由最佳擴散轉換[ODM]之MDS矩陣(matrix)所獲得之線性轉換結果所獲得之8位元資料中之高位4位元z[0]，對於4位元輸出入之S-box[$S4_2$]303輸入，將低位4位元z[1]對於4位元輸出入之S-box[$S4_3$]304輸入，於此等4位元S-box執行非線性轉換，並獲得輸出y[0], y[1]。S-box[$S4_2$]303、S-box[$S4_3$]304係與S-box[$S4_0$]301、S-box[$S4_1$]302相同，為分別隨機選擇之特性良好之4位元S-box，其按照圖14(b)所示之表來執行資料轉換。最終將結合有S-box[$S4_2$]303、S-box[$S4_3$]304所輸出之4位元資料y[0]及y[1]之8位元資料，作為8位元入出之S-box300之最終輸出y(8位元)。

圖16(a)所示之架構與圖14(a)所示之架構相同，其為應用圖13所示之架構來執行具體之8位元輸出入之非線性轉換之8位元S-box320之一架構例；圖16(b)係表示圖16(a)所示之8位元S-box320之構成要素之4個4位元輸出入S-

box321~324之轉換表。使用此表之數值為16進位。該表係表示對於輸入：x=0~F(16進位)之各S-box321~324之輸出值。而且，於圖17(c)表示作為圖17(a)(=圖16(a))所示之線性轉換處理部331而使用最佳擴散轉換[ODM]之MDS矩陣(matrix)331之具體例。

圖16、圖17所示之架構例中，

4位元輸出入S-box321~324係按照圖16(b)所示之表來執行非線性轉換，

線性轉換處理部331係按照圖17(c)來進行轉換處理，

此等處理不同。

於線性轉換處理部331，藉由在GF(2)上定義之4次不可約多項式：$p(x)=x^4+x+1$所做成之擴張體$GF(2^4)$上之矩陣運算，來執行線性轉換，並輸出z[0], z[1]。作為線性轉換處理部311之MDS矩陣(matrix)係根據，以4次不可約多項式所定義之擴張體$GF(2^4)$上之2元素作為要素所具有之2x2之4要素所組成之矩陣，來執行線性轉換處理。

於圖17(c)表示矩陣運算之具體處理。應用圖17(c)所示之2x2之MDS矩陣之情況時，根據輸入w[0], w[1]，如下算出輸出z[0], z[1]。

z[0]=w[0](XOR)w[1]

z[1]=w[0](XOR)w[1]x2

由於圖14~圖17所示之例係執行8位元輸出入側之非線性轉換處理之S盒，任一者在線性轉換處理部311, 331中應用之MDS矩陣之要素尺寸為n/2位元，且為2x2矩陣，因此要

素數為4個，即使調查全矩陣，該數目仍為$2^{n/2\times4}$種程度，因此可容易調查全矩陣，如前述，若以此方法產生S-box，則據判由於可實現簡易之代數表現限於小S-box，因此在擴張體GF(2^n)上之要素看似隨機，可判斷難以在GF(2^n)上進行單純之代數表現。而且，不會如在擴張體上之冪積運算般平均地擴散。並且，於用以從輸入獲得輸出之路徑，小S-box僅有兩個，若適當選擇矩陣，則能以簡易運算及短路徑來構成，因此相較於以n位元隨機地產生之S-box、或組合以往之小S-box所構成之S-box，安裝效率變高。

圖13~圖17所示之架構例係將輸入n位元分割為二，將高位各n/2位元、低位各n/2位元分別輸入於n/2位元輸出入之S-box，而且將來自線性轉換處理部之輸出n位元之高位各n/2位元、低位各n/2位元，分別輸入於n/2位元輸出入之S-box[S_2]而獲得非線性轉換處理結果之架構，但分割輸入位元並輸入之小S-box之數目不限於2，其他數目亦可。於圖18表示利用將輸入n位元分割為四，進行每n/4位元之非線性轉換處理之小n/4位元輸出入S-box之n位元S-box400之架構例。

於圖18所示之n位元S-box400之架構係由8個n/4位元輸出入之雙射S-box401~408，及由作為分支數高之擴散轉換而在最佳擴散轉換[ODM]之擴張體GF($2^{n/4}$)定義之4×4MDS(Maximum Distance Separable：最大距離可分隔)矩陣所組成之線性轉換處理部421所構成，執行n位元輸出入

之非線性轉換處理之架構。

輸入n位元係各分割為n/4位元，分別輸入於n/4位元輸出入之雙射S-box[S_0]401、S-box[S_1]402、S-box[S_2]403、S-box[S_3]404，並於各S-box進行非線性轉換處理後，輸入於在擴張體GF($2^{n/4}$)定義之4x4MDS矩陣所組成之線性轉換處理部421，根據MDS矩陣進行線性轉換處理後，線性轉換結果之n位元之各n/4位元分別輸入於n/4位元輸出入之S-box[S_0]405、S-box[S_1]406、S-box[S_2]407、S-box[S_3]408，於各S-box進行非線性轉換處理而獲得作為輸出結果之n位元之架構。

於圖18所示之線性轉換處理部421中應用之擴散轉換亦為最佳擴散轉換[ODM]之MDS矩陣，保證前段之4個小S-box之輸出會對於後段之小S-box之輸入均衡地配置，因此可產生全體特性良好之大S-box。

歸納有關藉由按照上述本發明執行非線性轉換處理之S盒所構成之資料轉換裝置之架構。本發明之資料轉換裝置之特徵在於具有如下架構。亦即，其為具有：

第一段非線性轉換部，其係由執行輸入資料分割後之各個分割資料之非線性轉換處理之複數小型非線性轉換部(小S盒)所組成；

線性轉換部，其係輸入來自構成第一段非線性轉換部之複數小型非線性轉換部之所有輸出，並執行線性轉換；及

第二段非線性轉換部，其係由執行線性轉換部之輸出資料分割後之各個分割資料之非線性轉換處理之複數小型非

線性轉換部(小S盒)所組成；

線性轉換部係藉由具有與輸入資料之位元尺寸相同尺寸之要素之矩陣運算來執行資料轉換，且於矩陣為m×m矩陣之情況下，應用至少具有分支數m以上之高分支數之矩陣來執行資料轉換處理之架構。

具體而言，於輸入資料為n位元資料之情況下，第一非線性轉換部係由輸入作為輸入資料之n位元資料之分割資料之n/k位元之各個，並輸出作為非線性轉換處理結果之n/k位元之k個小型非線性轉換部所構成；線性轉換部係輸入k個小型非線性轉換部所輸出之總計n位元之資料，並藉由應用高分支數之矩陣之資料轉換處理，來產生n位元之輸出之架構；第二非線性轉換部係具有由輸入從線性轉換部輸出之作為n位元資料之分割資料之n/k位元之各個，並輸出作為非線性轉換處理結果之n/k位元之k個小型非線性轉換部之架構。

於此，線性轉換部係應用執行分支數m以上之擴散轉換之例如最佳擴散轉換ODM(Optimal Diffusion Mappings)之MDS(Maximum Distance Separable：最大距離可分隔)矩陣來執行資料轉換處理之架構，進一步具體而言係於輸入資料為n位元資料之情況時，應用由藉由在GF(2)上定義之n次不可約多項式p(x)所定義之擴張體$GF(2^n)$上之矩陣來執行資料轉換處理之架構。

此外，關於本發明之資料轉換裝置可作為如先前說明之執行共同鍵區塊密碼處理之裝置來具體實現，例如，

(甲)SPN(Substitution Permutation Network：取代置換網路)構造；

(乙)Feistel構造；

(丙)延伸Feistel構造；

可應用於應用以上構造來進行密碼處理之裝置中之非線性轉換部。此外，本發明之架構除了密碼處理以外，亦可於雜湊函數等進行非線性轉換之運算裝置中應用。

[4.密碼處理裝置之架構例]

最後，作為按照上述實施例來執行資料轉換處理之裝置例，於圖19表示作為密碼處理裝置之IC模組700之架構例。上述處理可於例如PC、IC卡、讀寫機及其他各種資訊處理裝置中執行，圖19所示之IC模組700可於此等各種機器中構成。

圖19所示之CPU(Central processing Unit：中央處理單元)701係執行密碼處理之開始或結束、資料收發之控制、各構成部間之資料傳輸控制及其他各種程式之處理器。記憶體702係由儲存CPU701所執行之程式或運算參數等固定資料之ROM(Read-Only-Memory：唯讀記憶體)、於CPU701之處理中執行之程式及程式處理中會適當變化之參數之儲存區、及作為工作區域來使用之RAM(Random Access Memory：隨機存取記憶體)等所組成。而且，記憶體702可作為密碼處理所需之鍵資料、於密碼處理中應用之轉換表(置換表)或應用於轉換矩陣之資料等之儲存區域來使用。此外，資料儲存區域宜構成作為具有防竊取構造

之記憶體。

密碼處理部703係按照應用例如上述各種密碼處理架構，亦即：

(甲)SPN(Substitution Permutation Network：取代置換網路)構造；

(乙)Feistel構造；

(丙)延伸Feistel構造；

此等各架構之任一構造之共同鍵區塊密碼處理運算法來執行密碼處理、解密處理，並進一步執行應用雜湊函數之運算處理等。

而且，密碼處理部703係執行與上述實施例相對應之非線性轉換處理之架構，亦即作為n位元輸出入S-box之架構，藉由執行輸出入位元比n小之非線性轉換之小S-box來執行非線性轉換，將其結果輸入於MDS矩陣等分支數高之擴散轉換矩陣，應用矩陣來執行轉換，將該轉換結果進一步應用執行輸出入位元比n小之非線性轉換之小S-box，來執行非線性轉換，以執行獲得n位元之非線性轉換結果之非線性轉換處理之架構。

此外，於此係表示密碼處理機構為個別模組之例，但亦可構成如不設置此獨立之密碼處理模組，例如將密碼處理程式儲存於ROM，並由CPU701讀出ROM儲存程式來執行。

隨機數產生器704係執行密碼處理所需之鍵產生等所需之隨機數之產生處理。

傳送接收部705係與外部執行資料通信之資料通信處理部，例如讀寫機等與IC模組執行資料通信，執行在IC模組內產生之密文之輸出，或執行來自外部讀寫機等機器之資料輸入等。

此IC模組700係具有執行應用作為按照上述實施例之非線性轉換處理部之S-box之處理，亦即應用具有參考圖13~圖18所說明之架構之S-box來執行非線性轉換處理之架構。

以上，參考特定實施例詳細解說有關本發明。然而，於未脫離本發明之要旨之範圍內，同業人士當然可施行該實施例之修正或取代。亦即，以例示之型態來揭示本發明，不應限定性地解釋。為了判斷本發明之要旨，應參酌申請專利範圍項。

此外，於說明書中所說明之一連串處理可藉由硬體、軟體或兩者之複合架構來執行。藉由軟體來執行處理之情況時，可將記錄有處理序列之程式安裝於組入專用硬體中之電腦內之記憶體來執行，或將程式安裝於可執行各種處理之泛用電腦來執行。

例如程式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)。或者，程式可預先暫時或永久儲存(記錄)於可撓式碟片、CD-ROM(Compact Disc Read Only Memory：微型碟片唯讀記憶體)、MO(Magneto optical：光磁性)碟片、DVD(Digital Versatile Disc：數位多功能碟片)、磁碟片、半導體記憶體

等可移除式記錄媒體。此種可移除式記錄媒體可作為所謂套裝軟體來提供。

此外，程式除了可從如上述之可移除式記錄媒體安裝於電腦以外，亦可從下載網頁無線傳輸至電腦，或經由LAN(Local Area Network：區域網路)、網際網路該類之網路，以有線傳輸至電腦，於電腦接收如此傳輸而來之程式，並安裝於內建之硬碟等記憶媒體。

此外，說明書所記載之各種處理不僅可按照記載，依時間序列來執行，亦可因應執行處理之裝置之處理能力或需要，同時或個別地執行。而且，本說明書中，系統係指複數裝置之邏輯性集合架構，各架構之裝置不限於位在同一殼體內。

[產業上之可利用性]

如上述，若根據本發明之一實施例之架構，由於例如將共同鍵區塊密碼或雜湊函數等處理中所執行之非線性轉換處理，應用藉由複數小S盒(S-box)來執行非線性轉換之第一段非線性轉換部、輸入來自第一段非線性轉換部之所有輸出並執行線性轉換之線性轉換部、及執行線性轉換部之輸出資料分割後之各個分割資料之非線性轉換處理之複數小型非線性轉換部所組成之第二段非線性轉換部，來進行資料轉換而構成，線性轉換部係應用進行最佳擴散轉換之矩陣來執行資料轉換之架構，因此不過度增大從資料輸入至輸出之要徑即可實現適當之資料擴散，可實現對於各種密碼攻擊之耐受度強之安全性高之資料轉換。

【圖式簡單說明】

圖1係表示共同鍵區塊密碼運算法之基本架構之圖。

圖2係說明有關圖1所示之共同鍵區塊密碼處理部E10之內部架構之圖。

圖3係說明有關圖2所示之密碼處理部12之詳細架構之圖。

圖4係說明有關作為回合函數執行部之一架構例之SPN構造回合函數之圖。

圖5係說明有關作為回合函數執行部之一架構例之Feistel構造之圖。

圖6係說明有關作為回合函數執行部之一架構例之延伸Feistel構造之圖。

圖7係說明有關非線性轉換處理部之具體例之圖。

圖8係說明有關線性轉換處理部之具體例之圖。

圖9係說明有關CRYPTON ver. 0.5之S-box之架構之圖。

圖10係說明有關CRYPTON ver. 1.0之S-box之架構之圖。

圖11係說明有關Whirlpool之S-box之架構之圖。

圖12係說明有關FOX之S-box之架構之圖。

圖13係表示作為有關本發明之一實施例之非線性轉換處理架構之n位元輸出入S-box之架構例之圖。

圖14(a)、14(b)係說明有關本發明之一實施例之執行具體之8位元輸出入之非線性轉換之S-box之架構例之圖。

圖15(a)、15(c)係說明有關本發明之一實施例之執行具

體之8位元輸出入之非線性轉換之S-box之架構例之圖。

圖16(a)、16(b)係說明有關本發明之一實施例之執行具體之8位元輸出入之非線性轉換之S-box之架構例之圖。

圖17(a)、17(c)係說明有關本發明之一實施例之執行具體之8位元輸出入之非線性轉換之S-box之架構例之圖。

圖18係說明作為有關本發明之一實施例之執行非線性轉換之S-box之架構例之圖。

圖19係表示作為有關本發明之裝置例之密碼處理裝置架構例之圖。

【主要元件符號說明】

10	共同鍵區塊密碼處理部E
11	鍵排程部
12	密碼處理部
20	回合函數執行部
20a, 20b	回合函數執行部
21, 34, 111~113, 151~153	互斥或(XOR)運算部
22, 32, 50	非線性轉換處理部
23, 33, 211, 421	線性轉換處理部
30, 41，42	F函數部
51, 161~163	S盒(S-box)
101, 121, 141, 144	S-box[$S4_0$]
102, 122, 143	S-box[$S4_1$]

103	S-box[$S4_2$]
123	S-box[$S4_1^{-1}$]
124, 142, 145	S-box[$S4_0^{-1}$]
131	位元運算部
171, 172	4位元輸出入或電路
201~204, 401~408	雙射S-box
300, 320	8位元S-box
301~304, 321~324	4位元輸出入S-box
311, 331	線性轉換處理部、MDS矩陣
400	n位元S-box
700	IC模組
701	CPU
702	記憶體
703	密碼處理部
704	隨機數產生器
705	傳送接收部
C	密文
K	鍵
K'	擴張鍵
P	明文
RK1~RKr	回合鍵
X	輸入值

X0~Xi~Xr	輸入資料、輸出資料
x[0], x[1], w[0], w[1]	輸入
Y	輸出值
y[0], y[1]	4位元資料
z[0], z[1]	輸出

五、中文發明摘要：

本發明實現一種安裝效率及安全性高之非線性轉換處理架構。本發明係執行應用第一段非線性轉換部、線性轉換部及第二段非線性轉換部之資料轉換，該第一段非線性轉換部係藉由複數小S盒(S-box)來執行非線性轉換，該線性轉換部係輸入所有來自第一段非線性轉換部之輸出，並執行應用進行最佳擴散轉換之矩陣之資料轉換，該第二段非線性轉換部係由執行分割線性轉換部之輸出資料後之各個分割資料之非線性轉換處理之複數小型非線性轉換部所組成。藉由本架構，不使要徑(critical path)過大而可實現適當之資料擴散，可實現安裝效率及安全性高之架構。

六、英文發明摘要：

十、申請專利範圍：

1. 一種資料轉換裝置，其特徵為包含：

第一段非線性轉換部，其係包含執行分割輸入資料後之各個分割資料之非線性轉換處理之複數小型非線性轉換部；

線性轉換部，其係輸入所有來自構成前述第一段非線性轉換部之複數小型非線性轉換部之輸出，並執行線性轉換；及

第二段非線性轉換部，其係包含執行分割前述線性轉換部之輸出資料後之各個分割資料之非線性轉換處理之複數小型非線性轉換部；

前述線性轉換部係

藉由具有與前述輸入資料之位元尺寸相同尺寸之要素之矩陣運算來執行資料轉換，且於矩陣為m×m矩陣之情況下，執行應用至少具有m以上分支數之高分支數矩陣之資料轉換處理之架構。

2. 如請求項1之資料轉換裝置，其中於前述輸入資料為n位元資料之情況下，

前述第一非線性轉換部係包含分別輸入作為輸入資料之n位元資料之分割資料之n/k位元，並輸出作為非線性轉換處理結果之n/k位元之k個小型非線性轉換部；

前述線性轉換部係輸入前述k個小型非線性轉換部所輸出之總計n位元之資料，並藉由應用高分支數矩陣之資料轉換處理，來產生n位元之輸出之架構；

前述第二非線性轉換部係具有分別輸入為從前述線性轉換部輸出之作為n位元資料之分割資料之n/k位元，並輸出作為非線性轉換處理結果之n/k位元之k個小型非線性轉換部之架構。

3. 如請求項1之資料轉換裝置，其中前述線性轉換部係執行應用執行最佳擴散轉換(ODM(Optimal Diffusion Mappings))處理之MDS(Maximum Distance Separable：最大距離可分隔)矩陣之資料轉換處理之架構。

4. 如請求項1之資料轉換裝置，其中前述線性轉換部係

於前述輸入資料為n位元資料之情況下，

執行應用藉由於GF(2)上定義之n次不可約多項式p(x)所定義之擴張體$GF(2^n)$上之矩陣之資料轉換處理之架構。

5. 如請求項1之資料轉換裝置，其中前述資料轉換裝置係

執行n位元輸出入之非線性轉換處理之S盒(S-box)；

前述第一段非線性轉換部及前述第二段非線性轉換部所含之複數小型非線性轉換部，係由執行位元數比n位元少之非線性轉換處理之小型S盒所構成。

6. 如請求項1至5中任一項之資料轉換裝置，其中前述資料轉換裝置係

執行伴隨非線性轉換處理之密碼處理之架構。

7. 如請求項6之資料轉換裝置，其中前述密碼處理為共同鍵區塊密碼處理。

8. 一種資料轉換方法，其特徵為：其係於資料轉換裝置中

執行者；且包含：

第一段非線性轉換步驟，其係於第一段非線性轉換部應用複數小型非線性轉換部，執行分割輸入資料後之各個分割資料之非線性轉換處理；

線性轉換步驟，其係於線性轉換部，輸入所有來自構成前述第一段非線性轉換部之複數小型非線性轉換部之輸出，並執行線性轉換；及

第二段非線性轉換步驟，其係於第二段非線性轉換部應用複數小型非線性轉換部，執行分割前述線性轉換部之輸出資料後之各個分割資料之非線性轉換處理；

前述線性轉換步驟係

藉由具有與前述輸入資料之位元尺寸相同尺寸之要素之矩陣運算來執行資料轉換之架構，且於矩陣為m×m矩陣之情況下，執行應用至少具有m以上分支數之高分支數矩陣之資料轉換處理之步驟。

9. 一種電腦程式，其特徵為：其係於資料轉換裝置使資料轉換處理執行者；且包含：

第一段非線性轉換步驟，其係於第一段非線性轉換部應用複數小型非線性轉換部，使分割輸入資料後之各個分割資料之非線性轉換處理執行；

線性轉換步驟，其係於線性轉換部，輸入所有來自構成前述第一段非線性轉換部之複數小型非線性轉換部之輸出，並使線性轉換執行；及

第二段非線性轉換步驟，其係於第二段非線性轉換部

應用複數小型非線性轉換部，使分割前述線性轉換部之輸出資料後之各個分割資料之非線性轉換處理執行；

前述線性轉換步驟係

藉由具有與前述輸入資料之位元尺寸相同尺寸之要素之矩陣運算來執行資料轉換之架構，且於矩陣為m×m矩陣之情況下，使應用至少具有m以上分支數之高分支數矩陣之資料轉換處理執行之步驟。

十一、圖式：

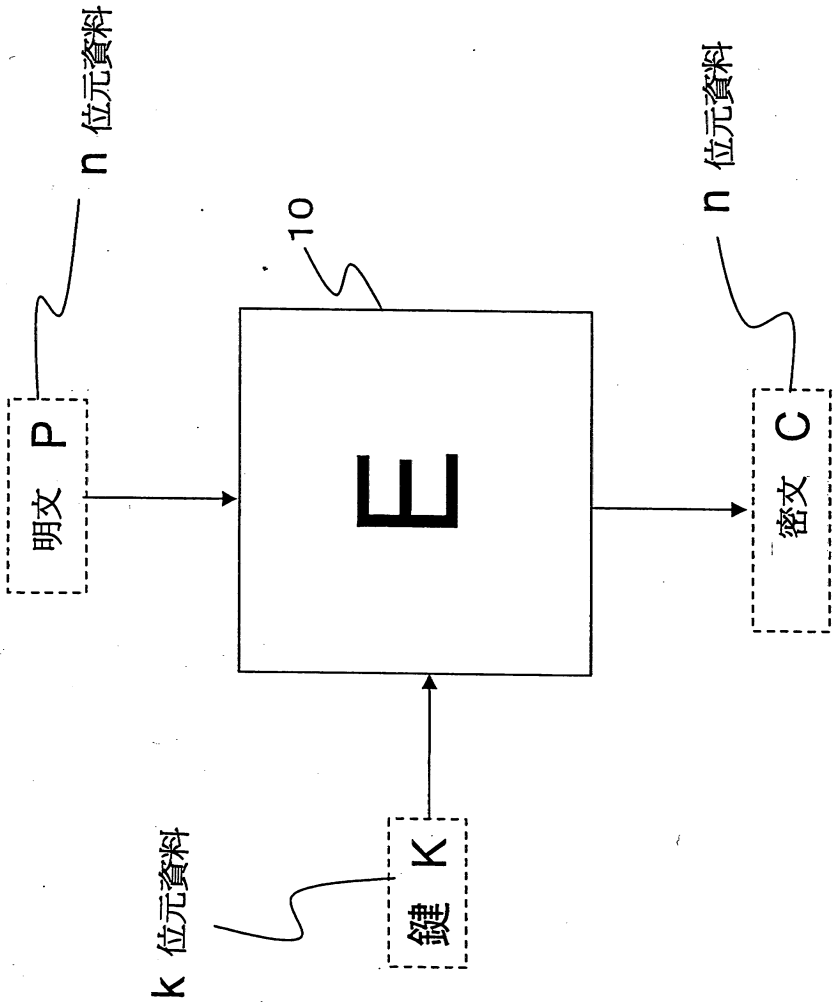


圖 1

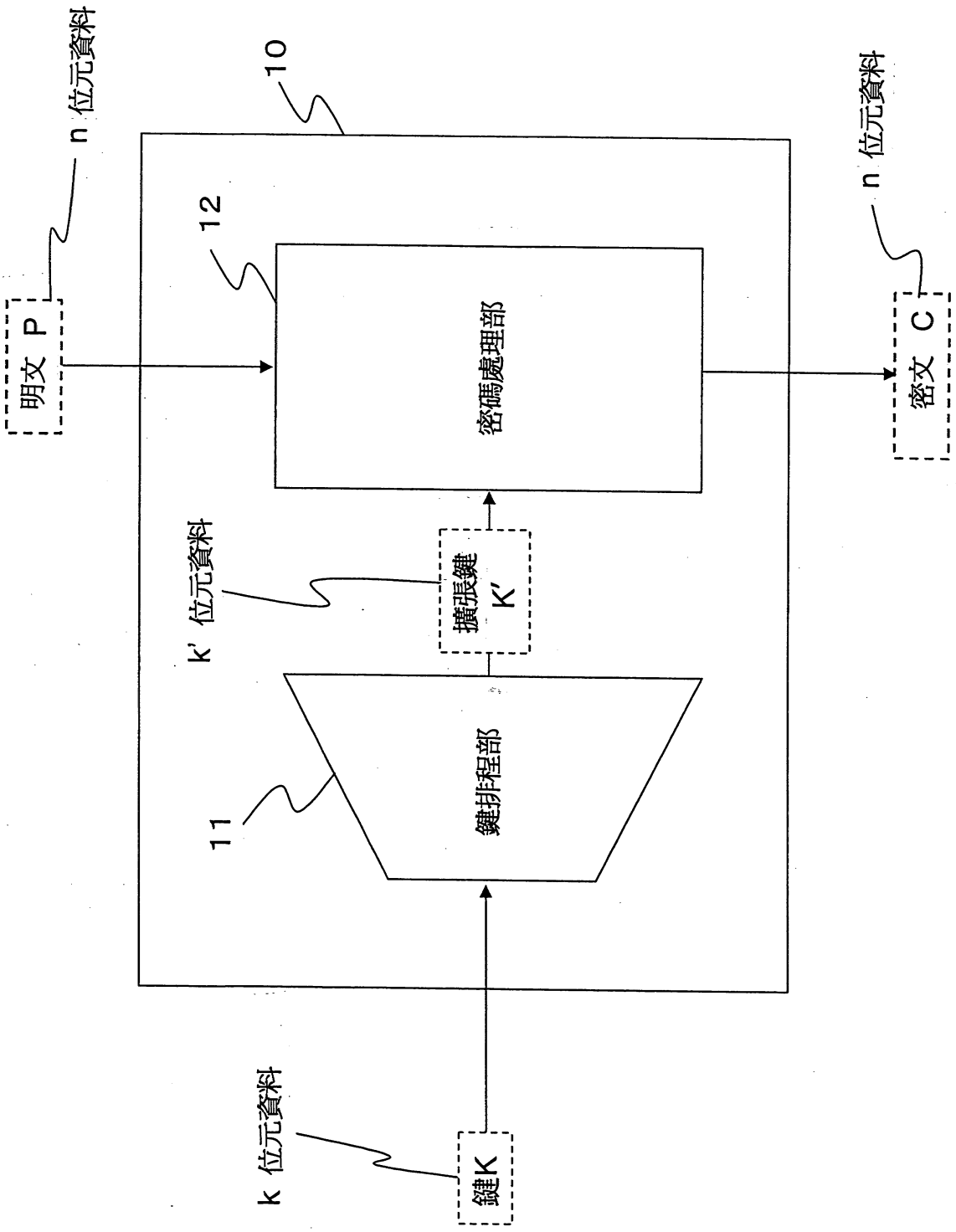


圖 2

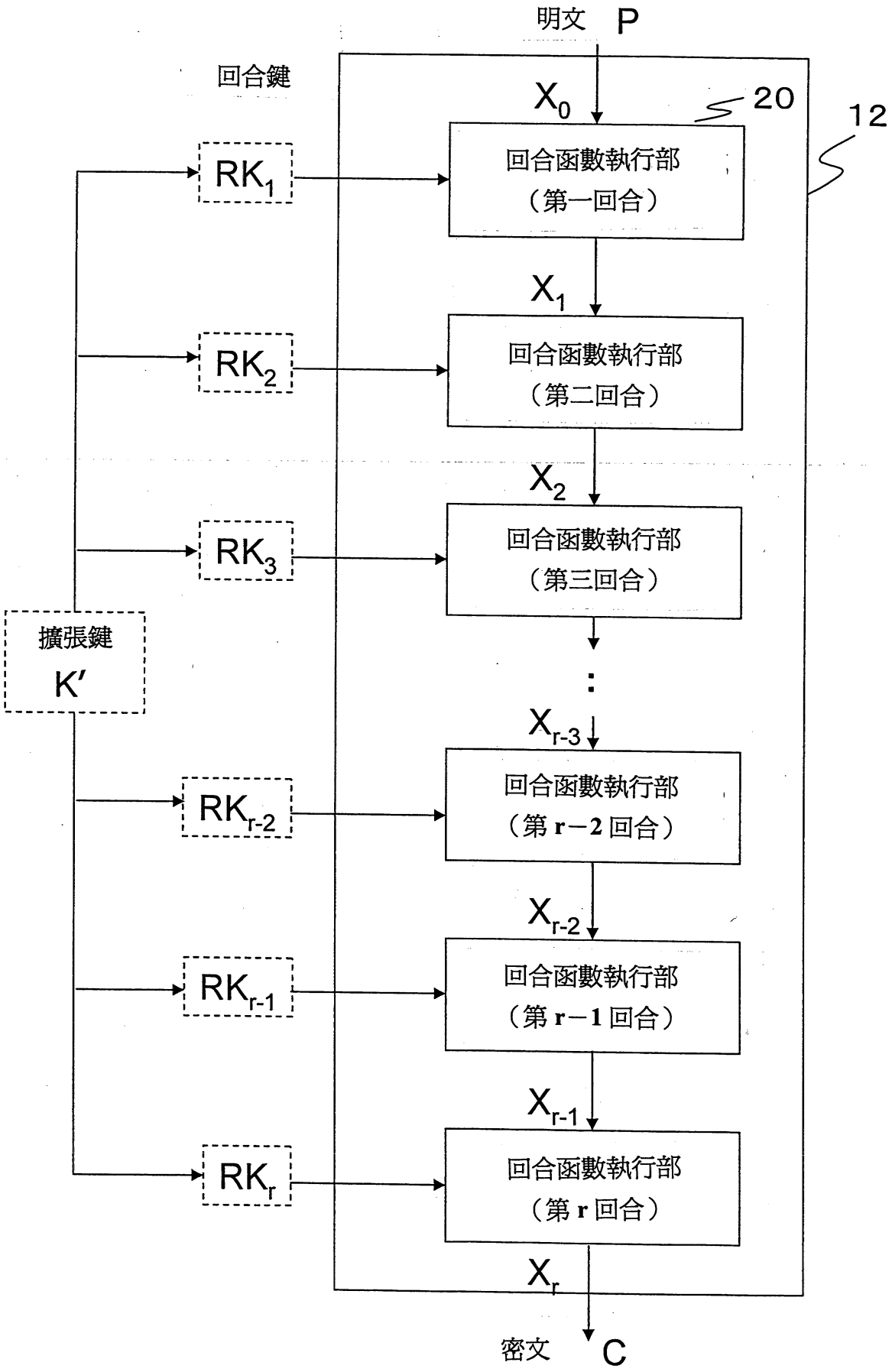

明文 P
回合鍵
X_0
20
12
回合函數執行部
（第一回合）
RK_1
X_1
回合函數執行部
（第二回合）
RK_2
X_2
回合函數執行部
（第三回合）
RK_3
擴張鍵
K′
:
X_{r-3}
回合函數執行部
（第 r−2 回合）
RK_{r-2}
X_{r-2}
回合函數執行部
（第 r−1 回合）
RK_{r-1}
X_{r-1}
回合函數執行部
（第 r 回合）
RK_r
X_r
密文 C

圖 3

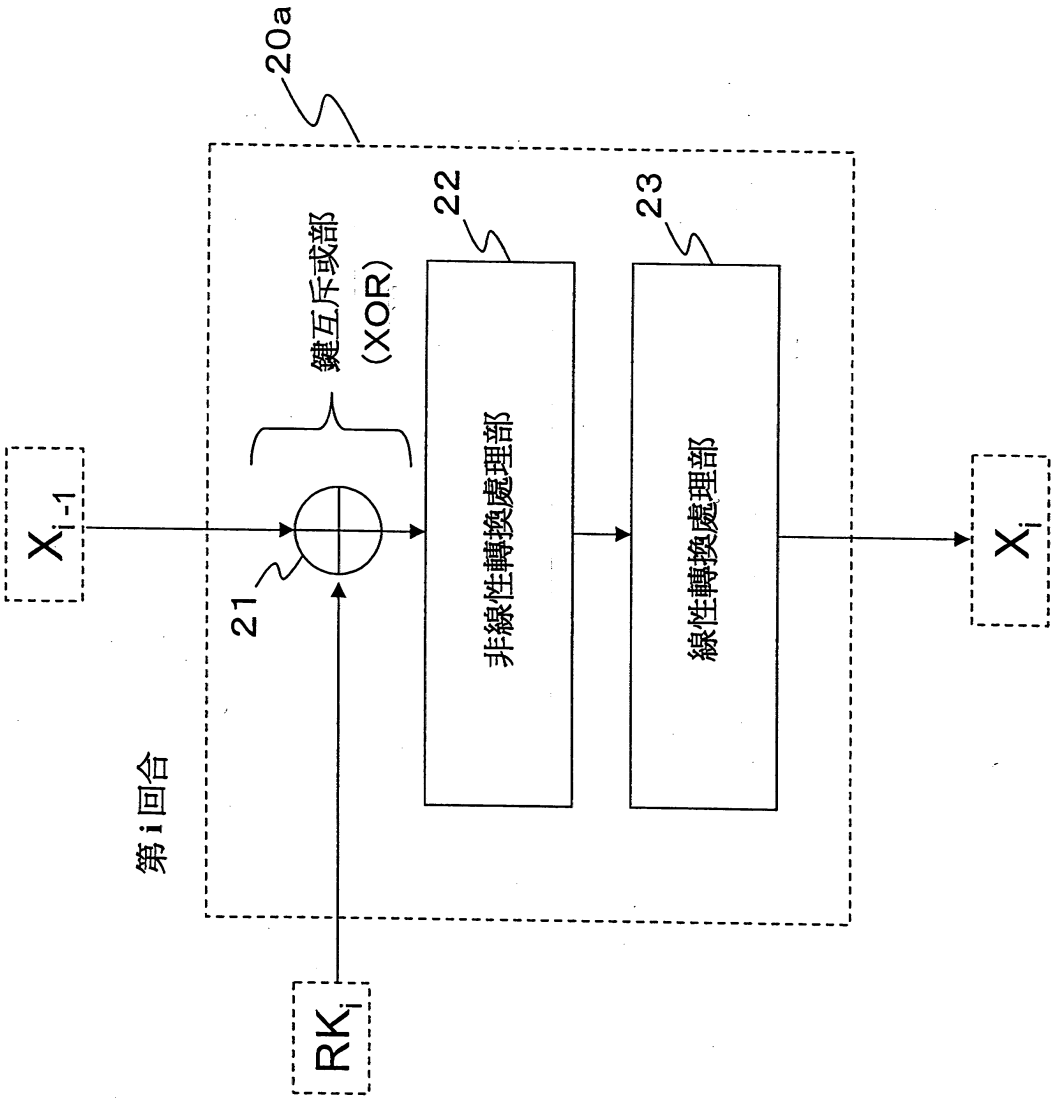


圖 4

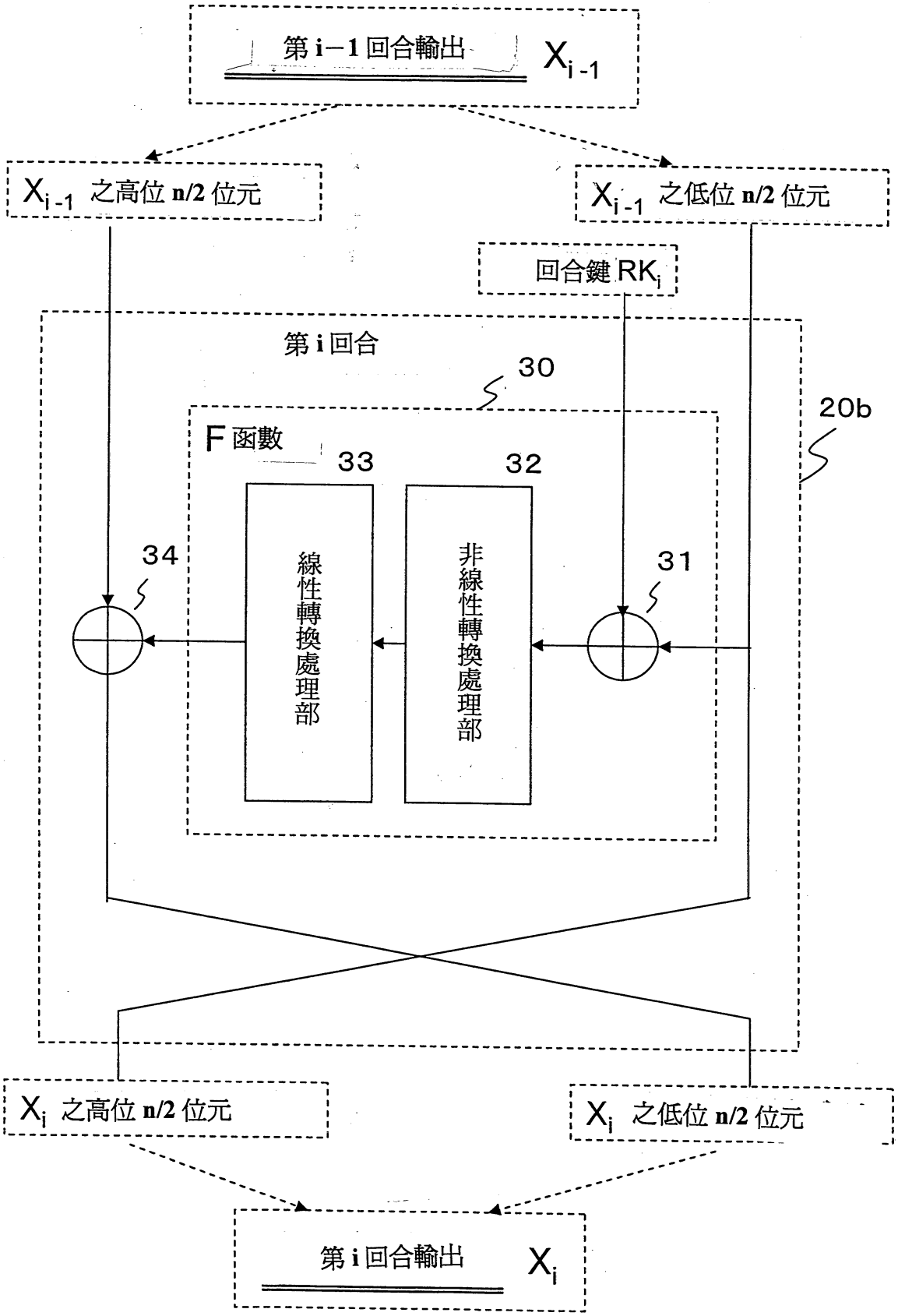

第 i−1 回合輸出
X_{i-1}
X_{i-1} 之高位 n/2 位元
X_{i-1} 之低位 n/2 位元
回合鍵 RK_i
第 i 回合
30
20b
F 函數
33
32
34
31
線性轉換處理部
非線性轉換處理部
X_i 之高位 n/2 位元
X_i 之低位 n/2 位元
第 i 回合輸出
X_i

圖 5

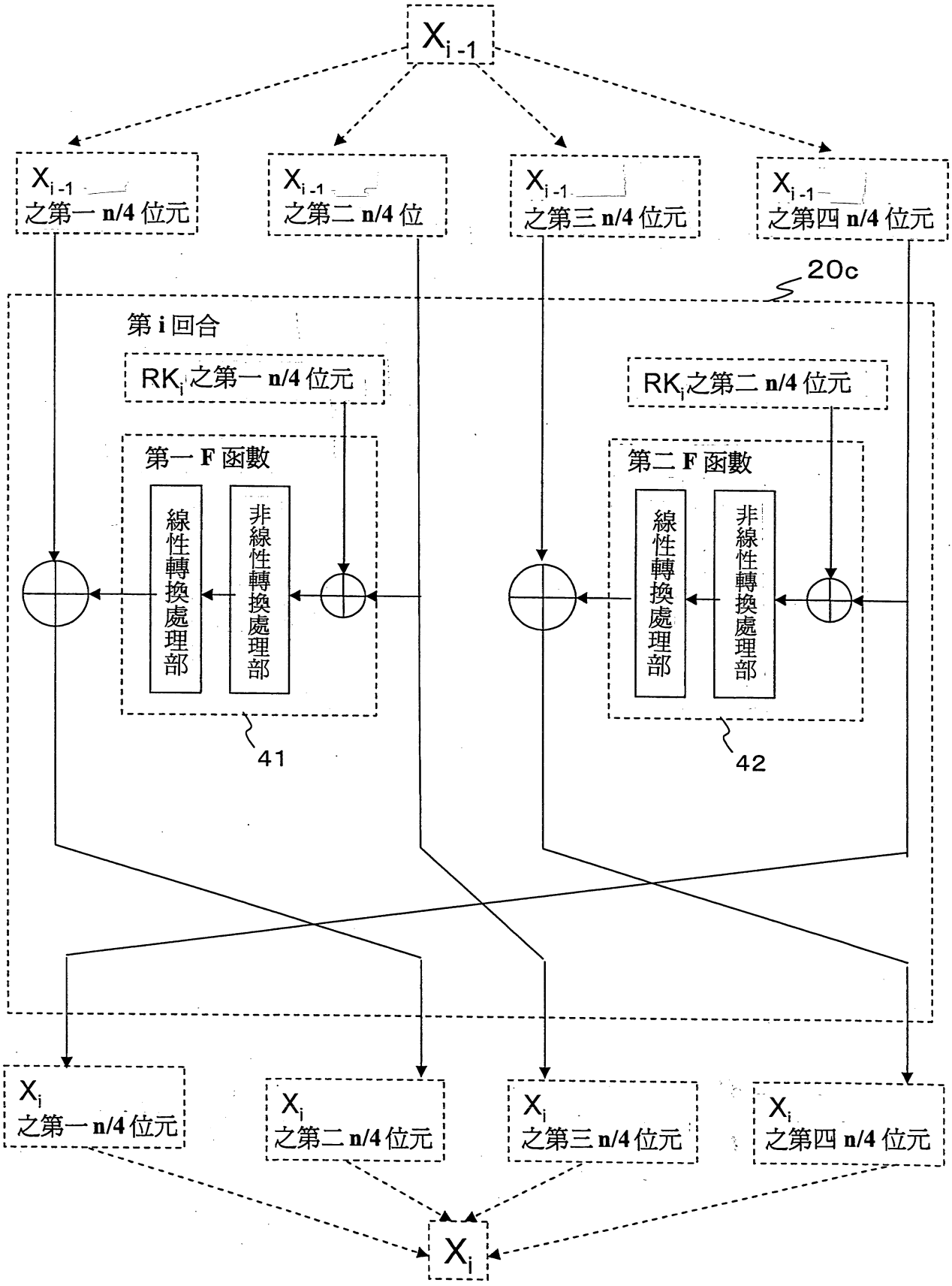

X_{i-1}
X_{i-1} 之第一 n/4 位元
X_{i-1} 之第二 n/4 位
X_{i-1} 之第三 n/4 位元
X_{i-1} 之第四 n/4 位元
20c
第 i 回合
RK_i 之第一 n/4 位元
RK_i 之第二 n/4 位元
第一 F 函數
第二 F 函數
線性轉換處理部
非線性轉換處理部
線性轉換處理部
非線性轉換處理部
41
42
X_i 之第一 n/4 位元
X_i 之第二 n/4 位元
X_i 之第三 n/4 位元
X_i 之第四 n/4 位元
X_i

圖 6

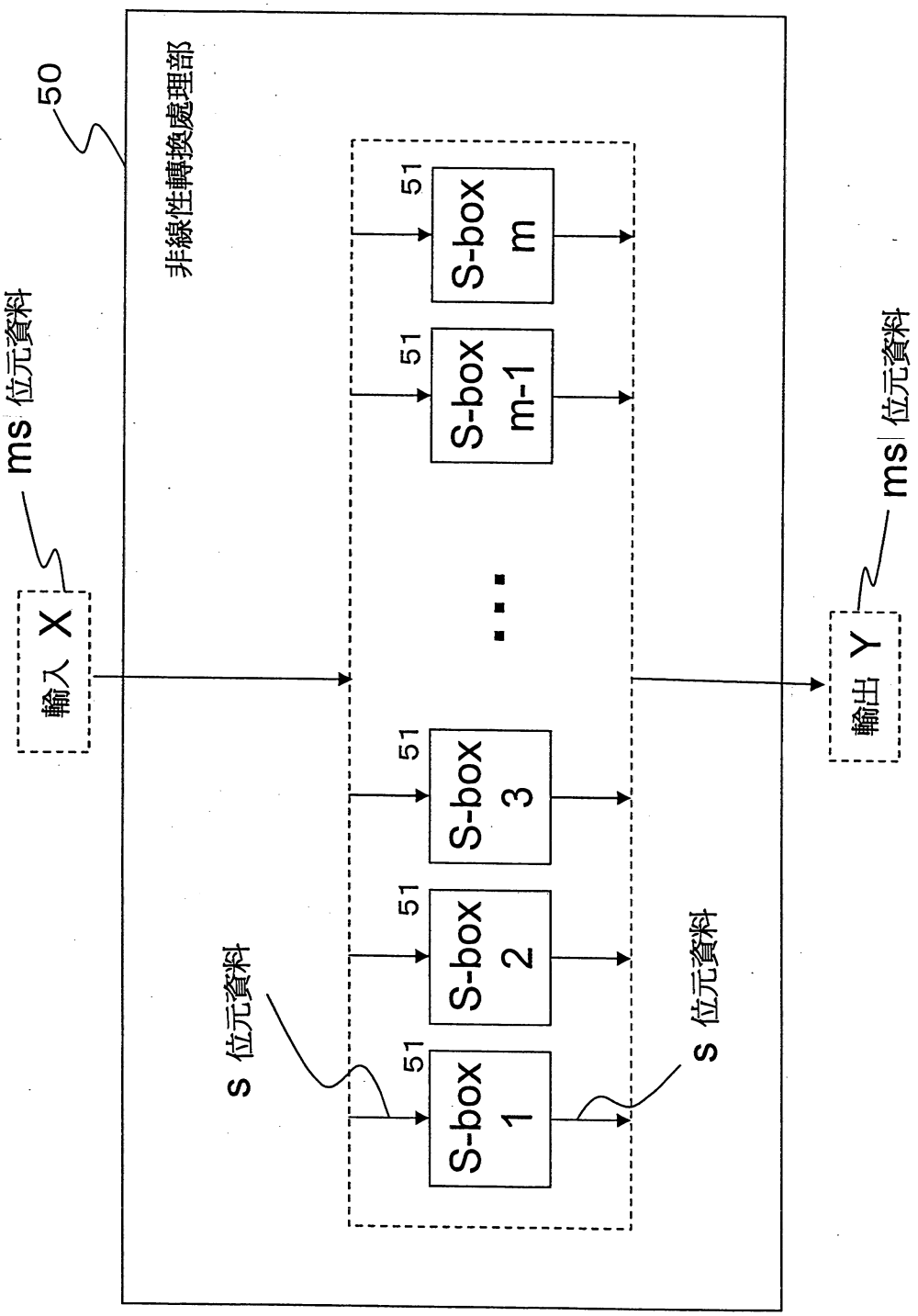

50
非線性轉換處理部
ms 位元資料
輸入 X
51
S-box 1
51
S-box 2
51
S-box 3
51
S-box m-1
51
S-box m
s 位元資料
s 位元資料
輸出 Y
ms 位元資料

圖 7

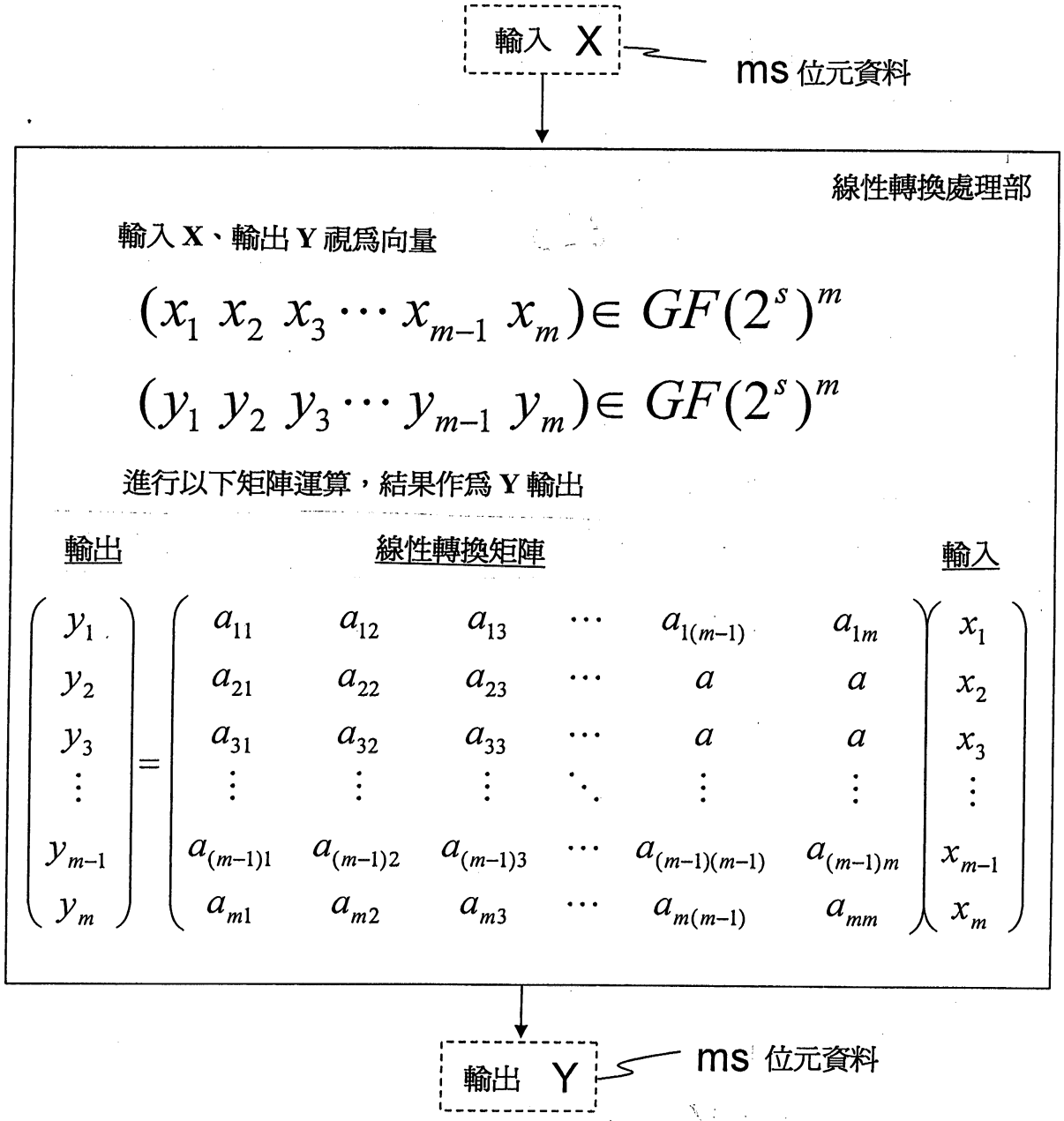

輸入 X
ms 位元資料
線性轉換處理部
輸入 X、輸出 Y 視爲向量
$(x_1\ x_2\ x_3 \cdots x_{m-1}\ x_m) \in GF(2^s)^m$
$(y_1\ y_2\ y_3 \cdots y_{m-1}\ y_m) \in GF(2^s)^m$
進行以下矩陣運算，結果作爲 Y 輸出
輸出
線性轉換矩陣
輸入
$\begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ \vdots \\ y_{m-1} \\ y_m \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1(m-1)} & a_{1m} \\ a_{21} & a_{22} & a_{23} & \cdots & a & a \\ a_{31} & a_{32} & a_{33} & \cdots & a & a \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{(m-1)1} & a_{(m-1)2} & a_{(m-1)3} & \cdots & a_{(m-1)(m-1)} & a_{(m-1)m} \\ a_{m1} & a_{m2} & a_{m3} & \cdots & a_{m(m-1)} & a_{mm} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_{m-1} \\ x_m \end{pmatrix}$
輸出 Y
ms 位元資料

圖 8

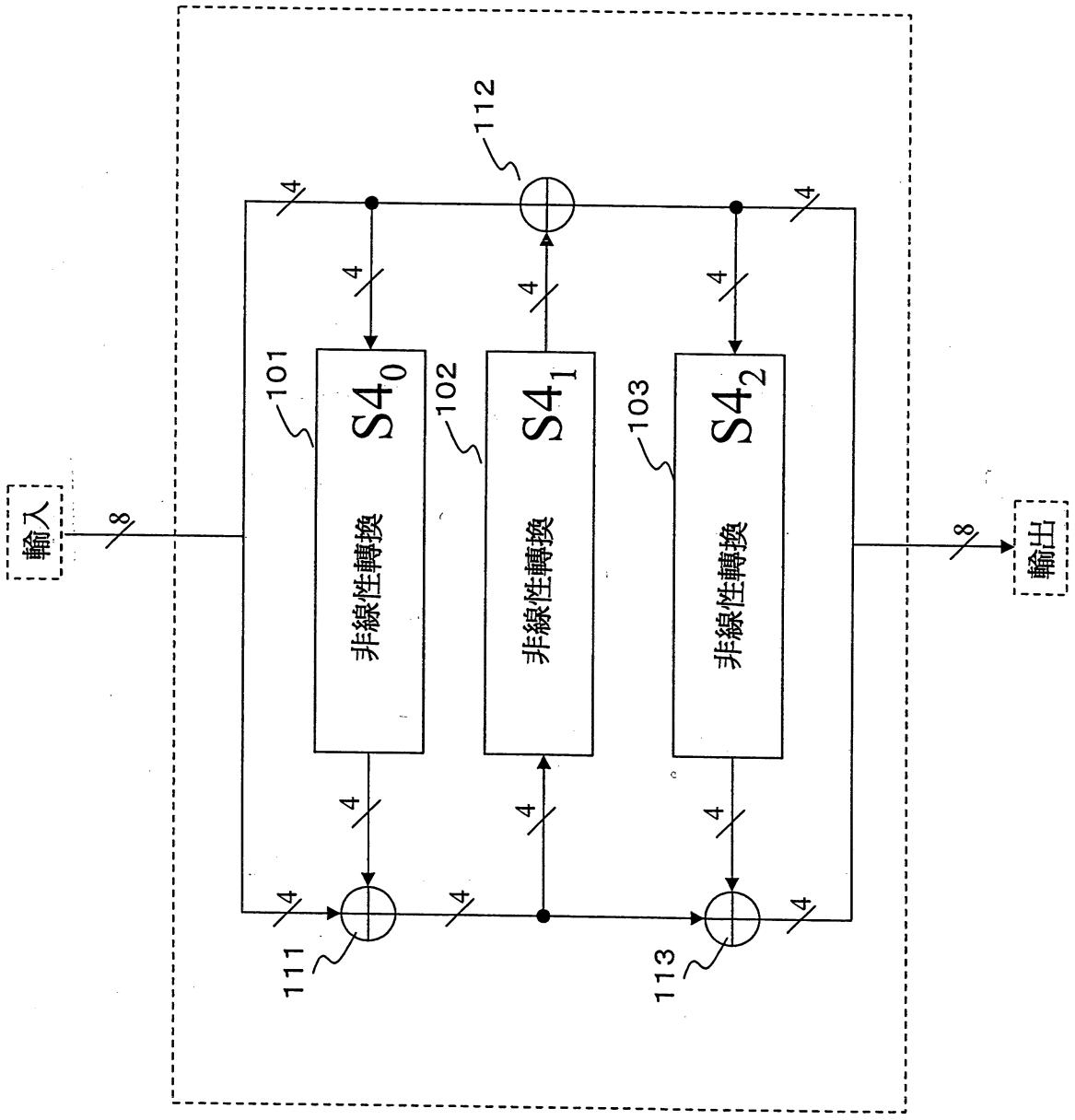


圖 9

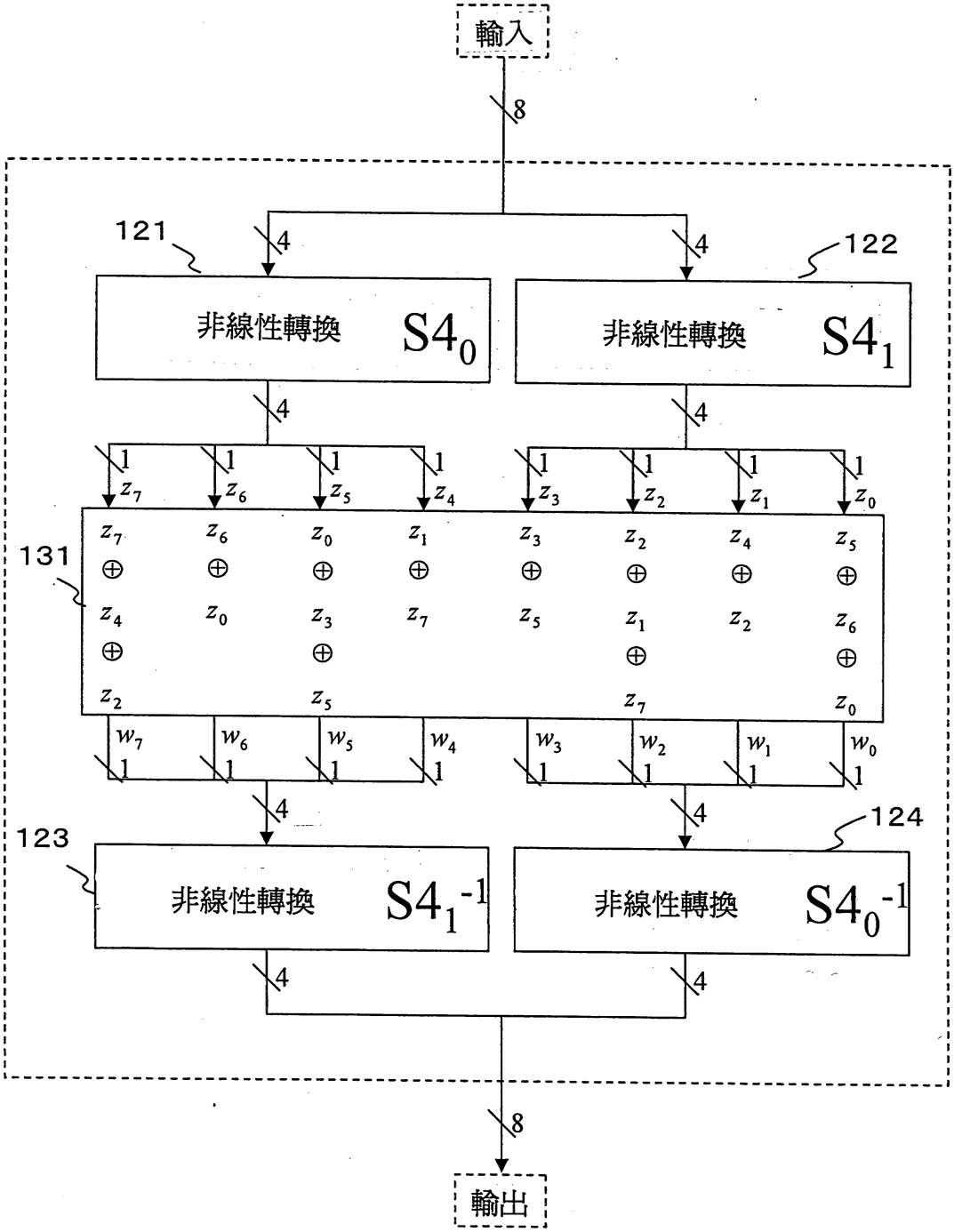

輸入
8
121
4
4
122
非線性轉換 $S4_0$
非線性轉換 $S4_1$
4
4
1 1 1 1
z_7 z_6 z_5 z_4
1 1 1 1
z_3 z_2 z_1 z_0
131
z_7 z_6 z_0 z_1 z_3 z_2 z_4 z_5
z_4 z_0 z_3 z_7 z_5 z_1 z_2 z_6
z_2 z_5 z_7 z_0
w_7 w_6 w_5 w_4
1 1 1 1
w_3 w_2 w_1 w_0
1 1 1 1
4
4
123
124
非線性轉換 $S4_1^{-1}$
非線性轉換 $S4_0^{-1}$
4
4
8
輸出

圖 10

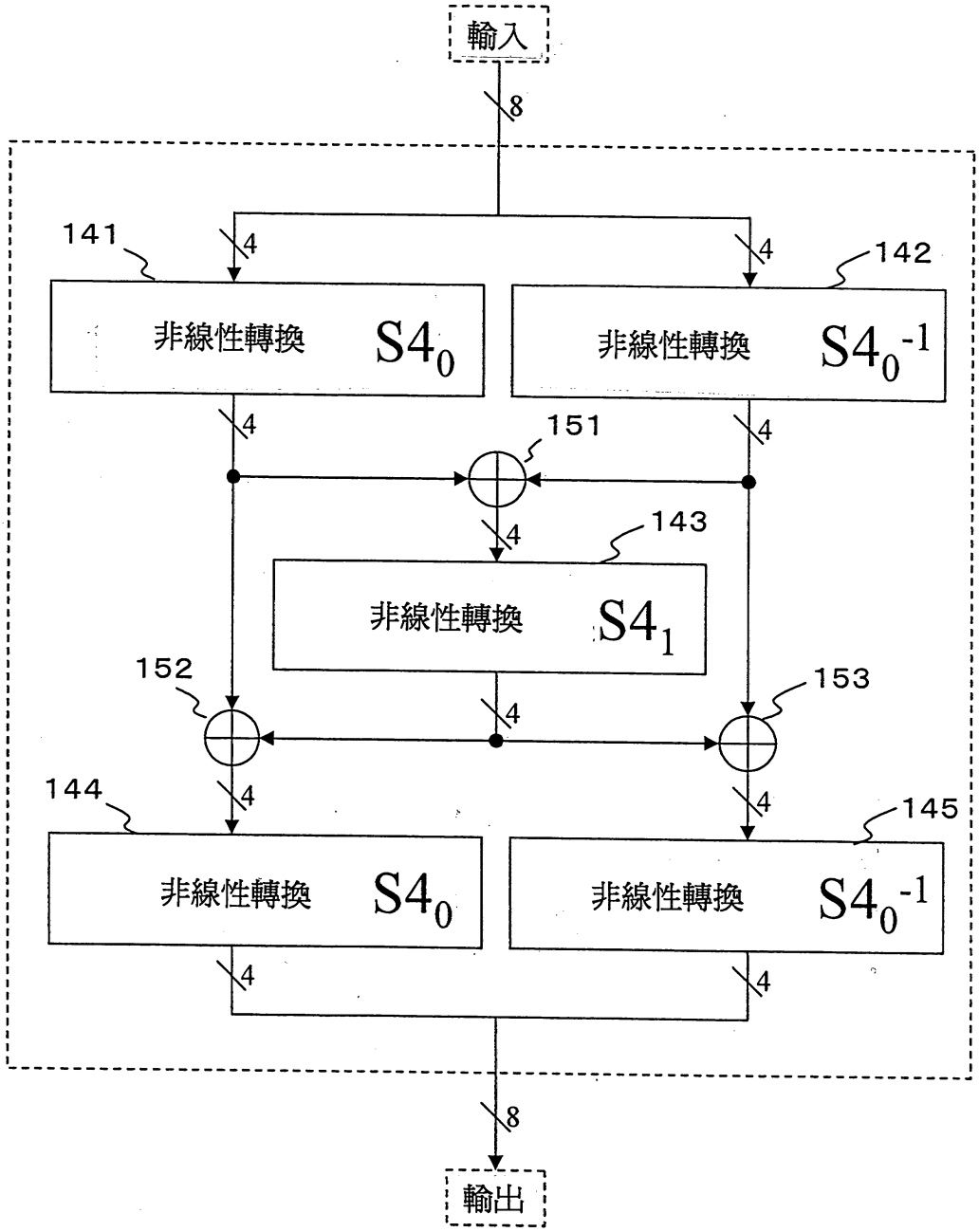

輸入
8
141
4
4
142
非線性轉換
$S4_0$
非線性轉換
$S4_0^{-1}$
4
151
4
4
143
非線性轉換
$S4_1$
152
153
4
144
4
4
145
非線性轉換
$S4_0$
非線性轉換
$S4_0^{-1}$
4
4
8
輸出

圖 11

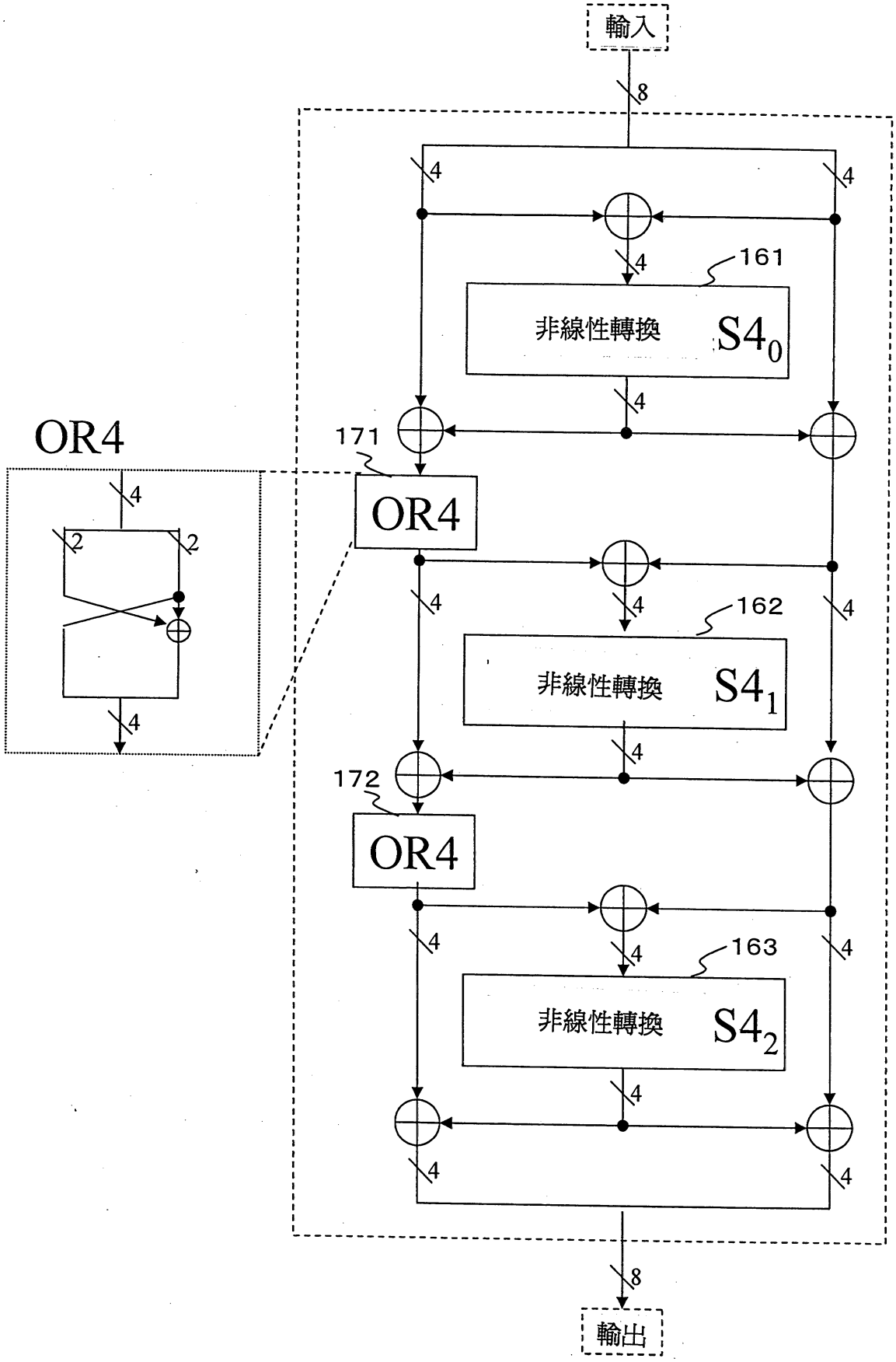

輸入
8
4
4
4
161
非線性轉換
S4₀
4
171
OR4
OR4
4
4
4
162
非線性轉換
S4₁
4
172
OR4
4
4
4
163
非線性轉換
S4₂
4
4
4
4
8
輸出
OR4
4
2
2
4

圖 12

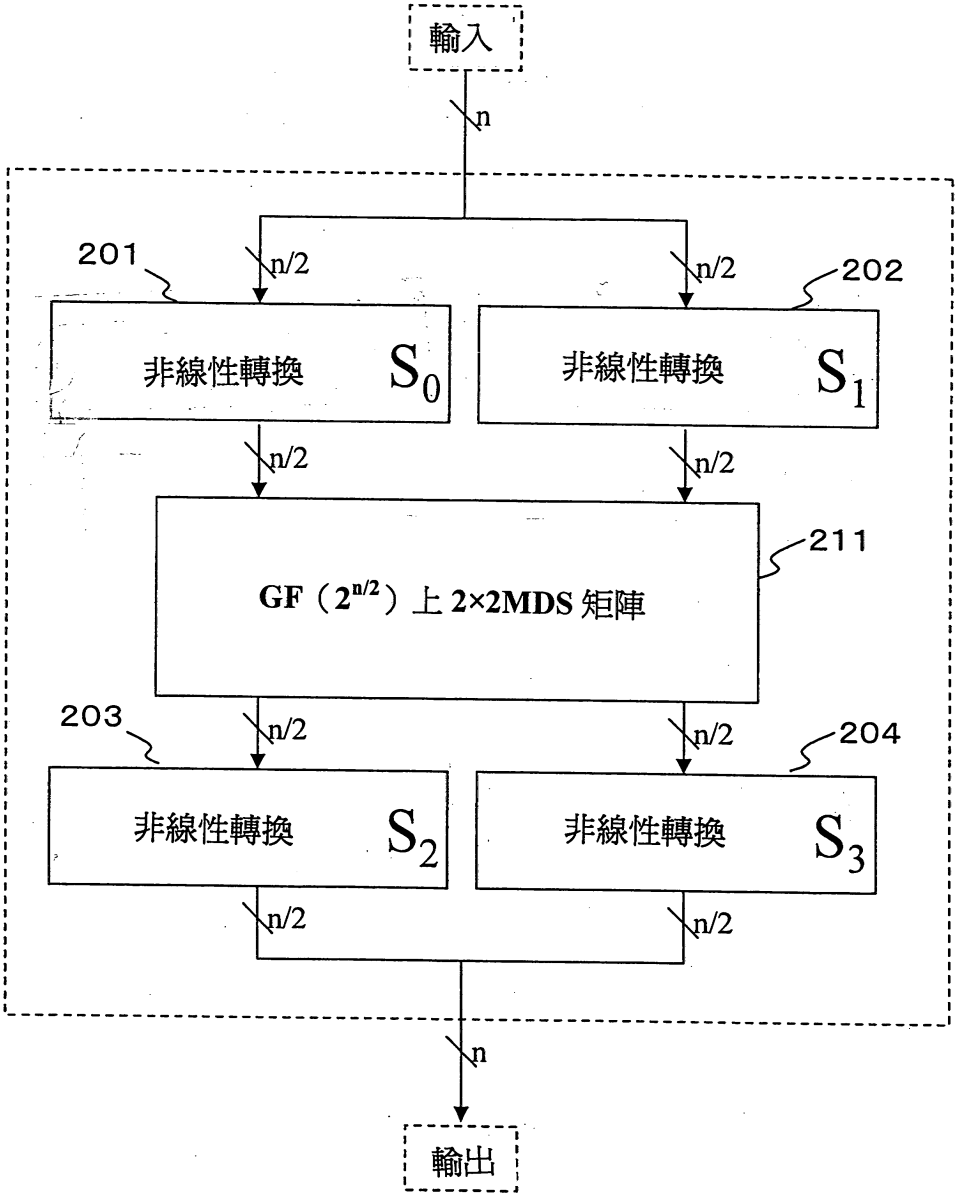
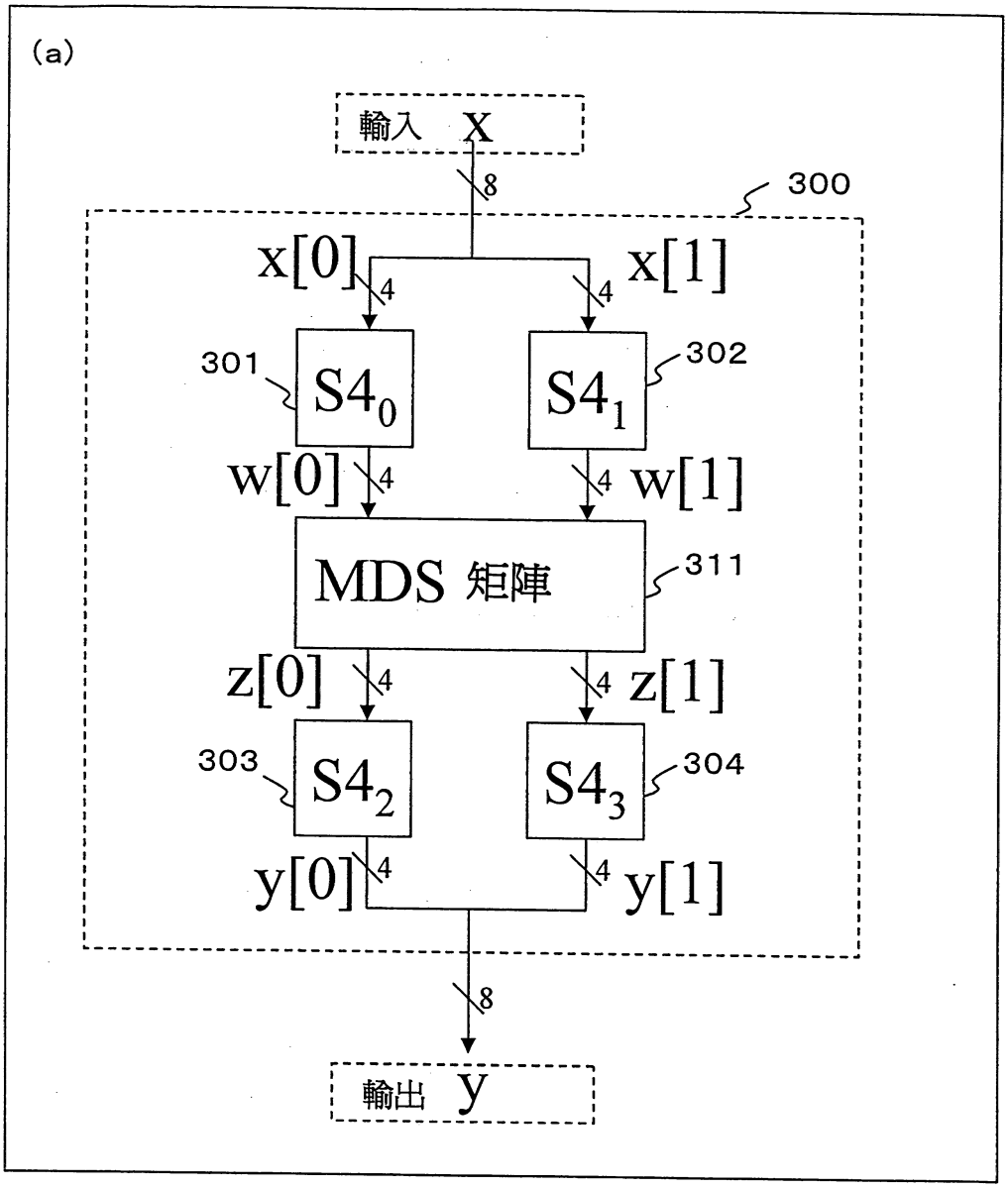

輸入
n
201
n/2
n/2
202
非線性轉換 S_0
非線性轉換 S_1
n/2
n/2
211
GF（$2^{n/2}$）上 2×2MDS 矩陣
203
n/2
n/2
204
非線性轉換 S_2
非線性轉換 S_3
n/2
n/2
n
輸出

圖 13

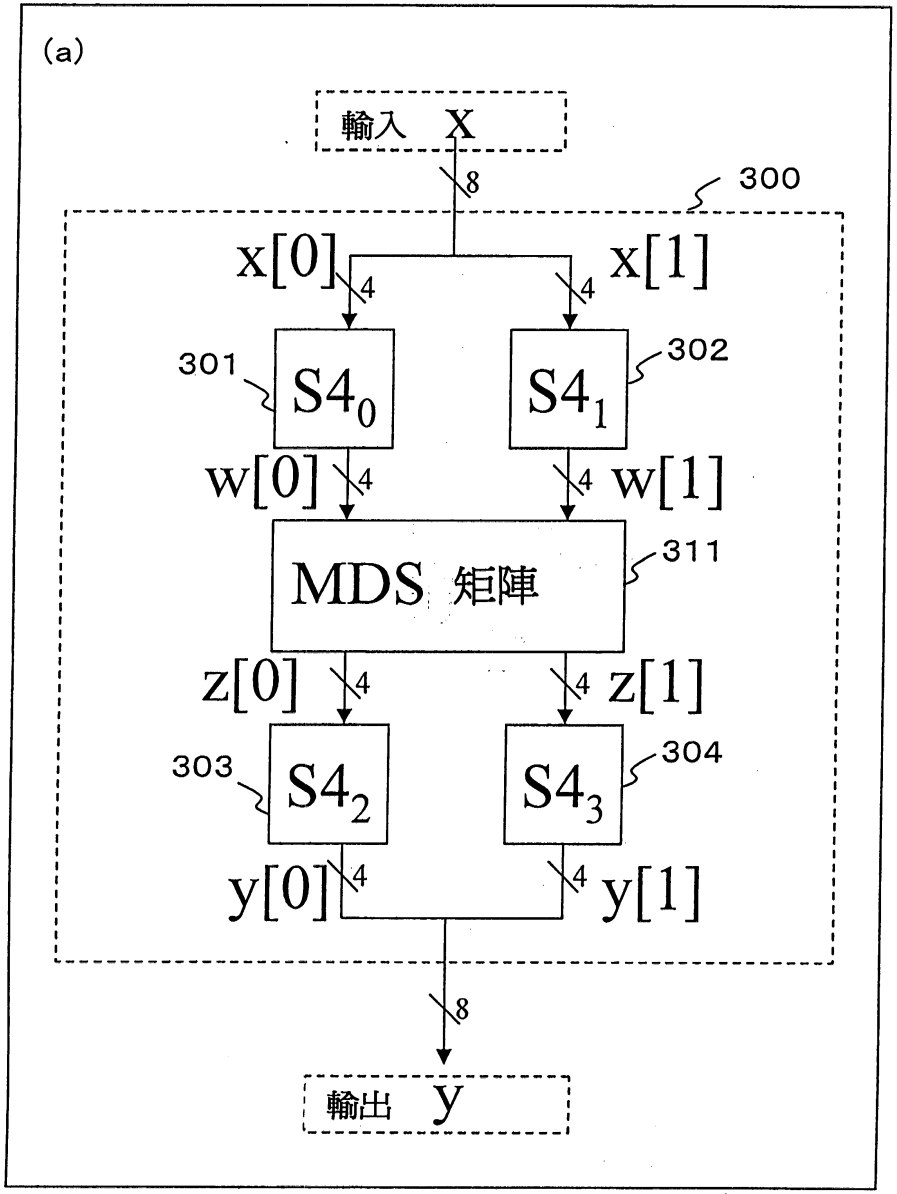
(a)



(b)

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S4_0(x)$	E	6	C	A	8	7	2	F	B	1	4	0	5	9	D	3
$S4_1(x)$	6	4	0	D	2	B	A	3	9	C	E	F	8	7	5	1
$S4_2(x)$	B	8	5	E	A	6	4	C	F	7	2	3	1	0	D	9
$S4_3(x)$	A	2	6	D	3	4	5	E	0	7	8	9	B	F	C	1

圖 14



(c)

MDS 矩陣：

$$\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} over\ GF(2^4), p(x) = x^4 + x + 1$$

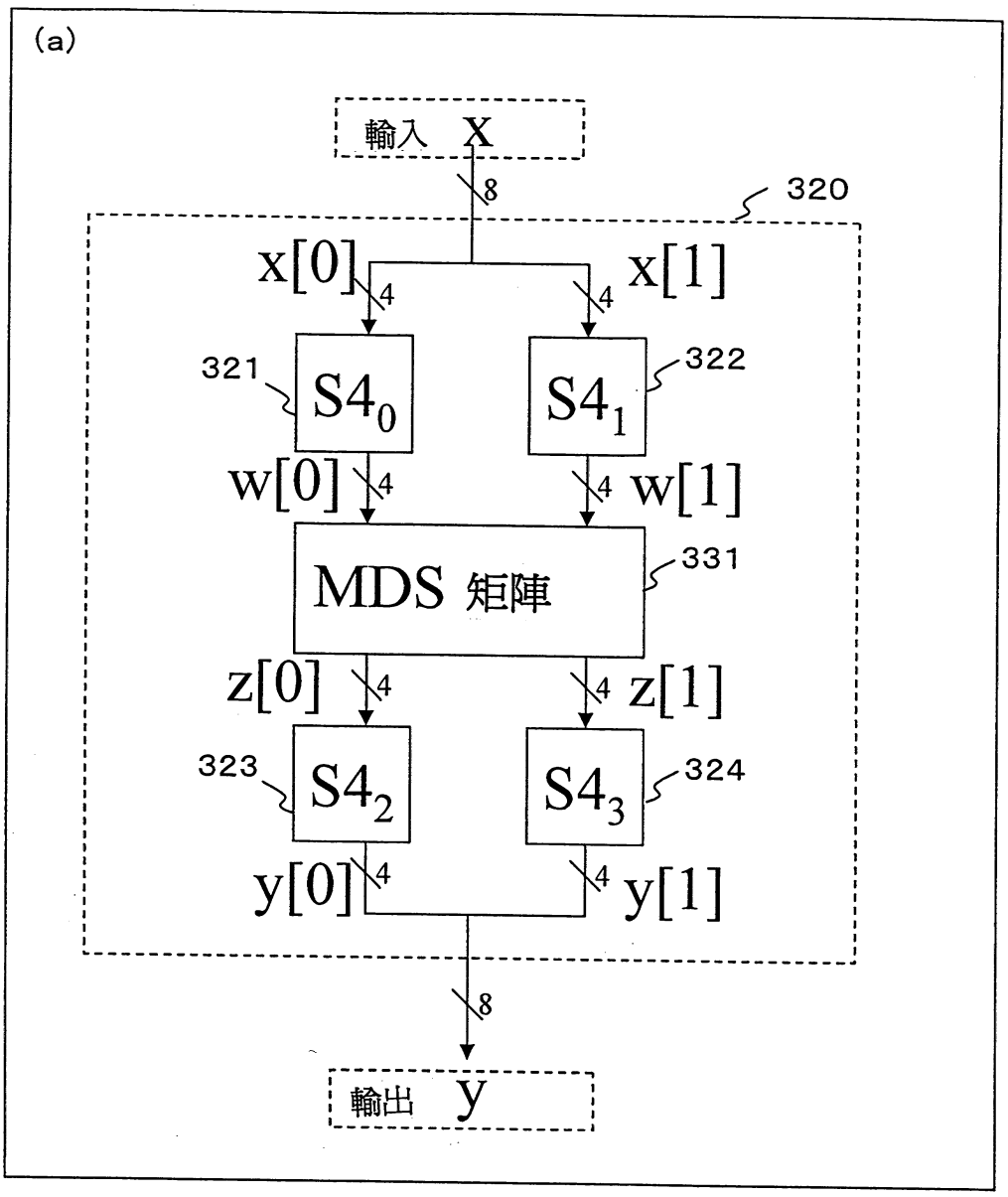
$$\begin{pmatrix} z[0] \\ z[1] \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} w[0] \\ w[1] \end{pmatrix}$$

$$z[0] = w[0] \oplus w[1] \times 2$$

$$z[1] = w[0] \times 2 \oplus w[1]$$

圖 15

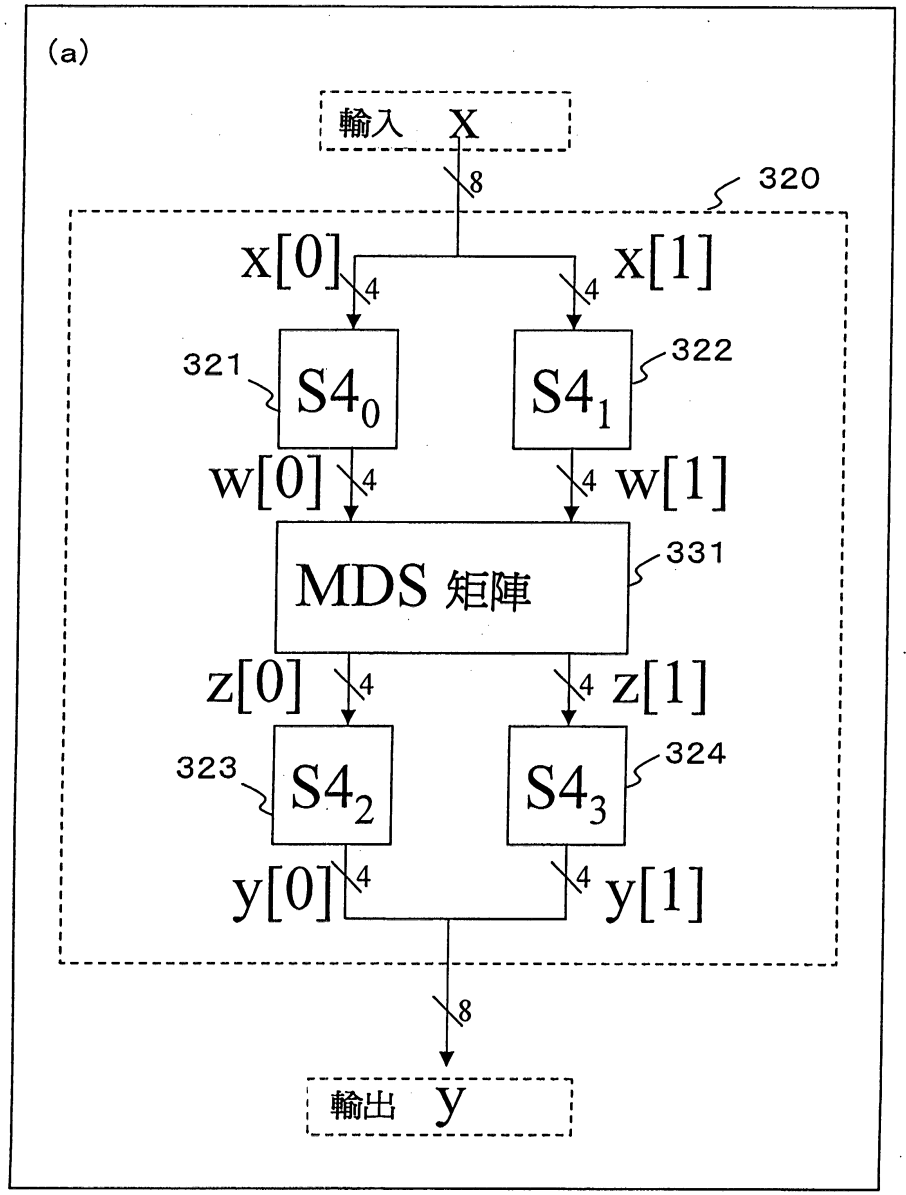
(a)



(b)

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S4_0(x)$	8	7	D	0	E	2	3	B	6	4	9	5	F	C	1	A
$S4_1(x)$	4	5	E	1	D	0	2	B	A	8	7	9	3	6	F	C
$S4_2(x)$	3	B	C	6	F	2	8	0	A	4	E	D	9	7	5	1
$S4_3(x)$	C	0	B	E	6	7	F	2	3	1	5	9	D	8	4	A

圖 16



(c)

MDS 矩陣：

$$\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} over\ GF(2^4), p(x) = x^4 + x + 1$$

$$\begin{pmatrix} z[0] \\ z[1] \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} w[0] \\ w[1] \end{pmatrix}$$

$$z[0] = w[0] \oplus w[1]$$

$$z[1] = w[0] \oplus w[1] \times 2$$

圖 17

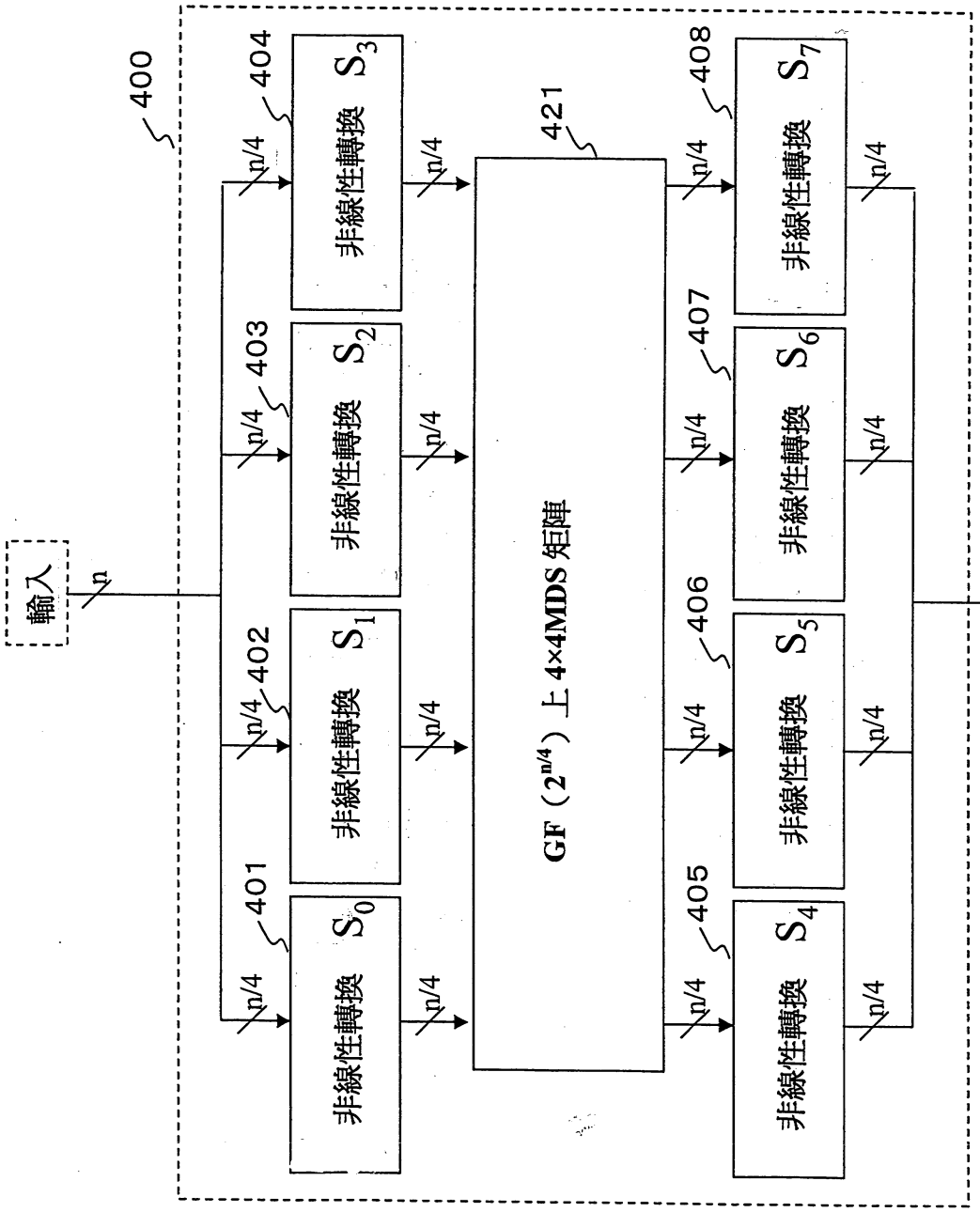

400
輸入
n
401
402
403
404
405
406
407
408
非線性轉換 S_0
非線性轉換 S_1
非線性轉換 S_2
非線性轉換 S_3
非線性轉換 S_4
非線性轉換 S_5
非線性轉換 S_6
非線性轉換 S_7
n/4
421
GF（$2^{n/4}$）上 4×4MDS 矩陣
輸出

圖 18

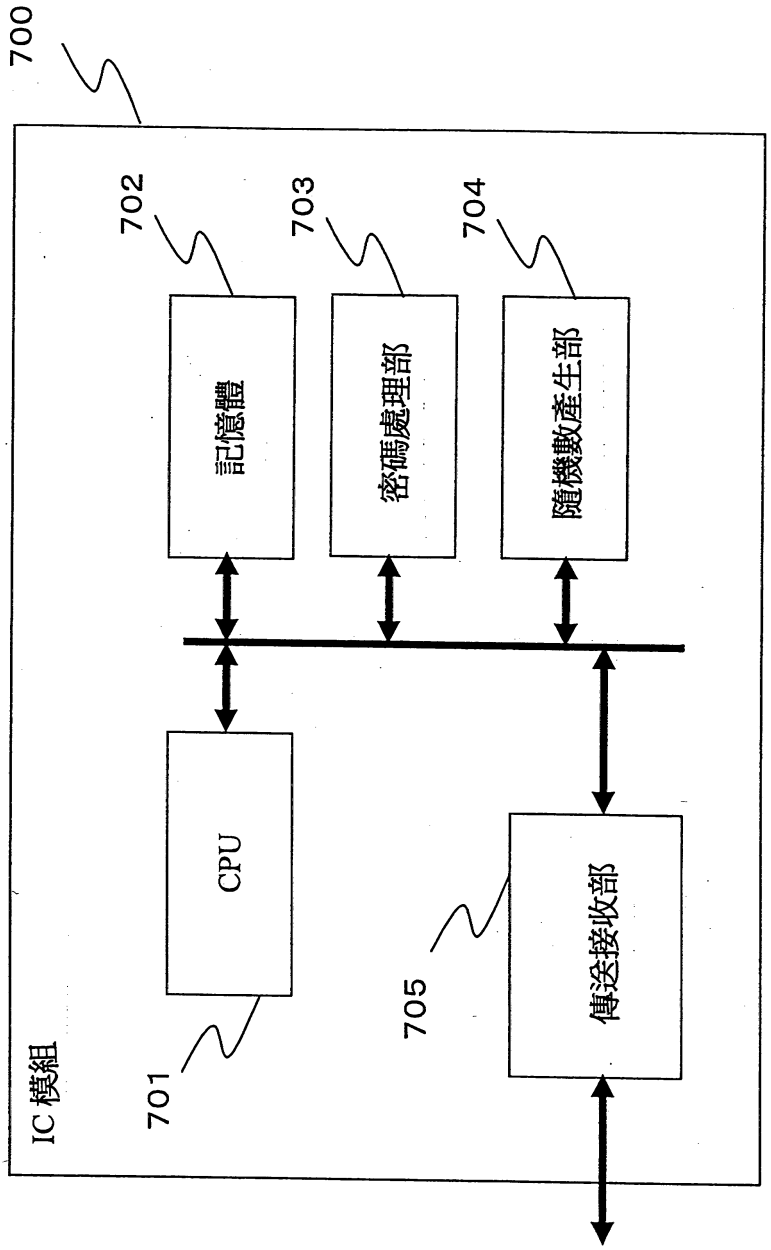


圖 19

七、指定代表圖：

(一)本案指定代表圖為：第(13)圖。

(二)本代表圖之元件符號簡單說明：

201~204	雙射S-box
211	線性轉換處理部

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）