I552121

(19)中華民國智慧財產局

(12)發明說明書公告本 **(11)證書號數：TW I552121 B**

(45)公告日： 中華民國 105 (2016) 年 10 月 01 日

(21)申請案號：101105911 (22)申請日： 中華民國 101 (2012) 年 02 月 22 日

(51)Int. Cl.： *G09C1/00 (2006.01)* *H04L9/06 (2006.01)*

(30)優先權：2011/03/28 日本 2011-069182

2011/09/22 日本 2011-207702

(71)申請人：新力股份有限公司 (日本) SONY CORPORATION (JP)

日本

(72)發明人：涉谷香士 SHIBUTANI, KYOJI (JP) ；秋下徹 AKISHITA, TORU (JP) ；五十部孝典 ISOBE, TAKANORI (JP) ；白井太三 SHIRAI, TAIZO (JP) ；樋渡玄良 HIWATARI, HARUNAGA (JP) ；三津田敦司 MITSUDA, ATSUSHI (JP)

(74)代理人：陳長文

(56)參考文獻：

TW	200830233A	US	2010/0014659A1
US	2010/0061548A1	WO	2010/024248A1

審查人員：洪丈力

申請專利範圍項數：13 項 圖式數：40 共 90 頁

(54)名稱

密碼處理裝置、密碼處理方法及程式

(57)摘要

本發明係實現一種擴散(diffusion)特性提升且安全性高之密碼處理。本發明之密碼處理裝置包含：密碼處理部，其將作為資料處理對象之資料之構成位元分割成複數列並輸入、且對各列之資料重複執行應用回合函數之資料轉換處理；在密碼處理部中，將以分割數 d 分割輸入資料即 n 位元資料之 n/d 位元資料輸入各列，且將包含應用回合函數之資料轉換處理之運算作為回合運算而重複執行。執行如下處理：將具有回合運算之輸出資料之列之 n/d 位元資料分割成 d/2 個，將該分割資料組合，再構成與前段之回合運算之輸出資料不同之 d 個 n/d 位元資料，作為次段之回合運算之輸入資料。藉由本構成而實現擴散(diffusion)特性提高且安全性高之密碼處理。

指定代表圖：

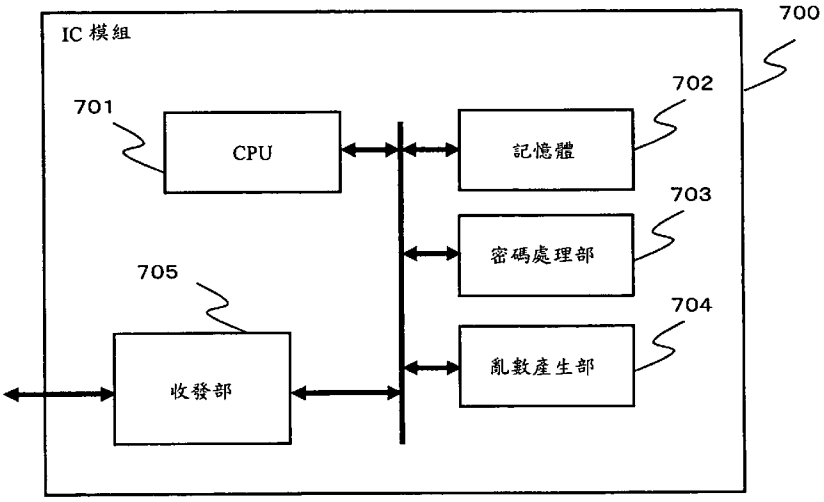

圖 40

符號簡單說明：

700・・・IC 模組

701・・・CPU (Central processing Unit)

702・・・記憶體

703・・・密碼處理部

704・・・亂數產生部

705・・・收發部

I552121

公告本

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：101105911

※申請日：101. 2. 22　　※IPC 分類：G09C1/00 (2006.01)

H04L 9/06 (2006.01)

一、發明名稱：(中文/英文)

密碼處理裝置、密碼處理方法及程式

二、中文發明摘要：

本發明係實現一種擴散(diffusion)特性提升且安全性高之密碼處理。本發明之密碼處理裝置包含：密碼處理部，其將作為資料處理對象之資料之構成位元分割成複數列並輸入、且對各列之資料重複執行應用回合函數之資料轉換處理；在密碼處理部中，將以分割數d分割輸入資料即n位元資料之n/d位元資料輸入各列，且將包含應用回合函數之資料轉換處理之運算作為回合運算而重複執行。執行如下處理：將具有回合運算之輸出資料之列之n/d位元資料分割成d/2個，將該分割資料組合，再構成與前段之回合運算之輸出資料不同之d個n/d位元資料，作為次段之回合運算之輸入資料。藉由本構成而實現擴散(diffusion)特性提高且安全性高之密碼處理。

三、英文發明摘要：

四、指定代表圖：

(一)本案指定代表圖為：第（ 40 ）圖。

(二)本代表圖之元件符號簡單說明：

700	IC模組
701	CPU(Central processing Unit)
702	記憶體
703	密碼處理部
704	亂數產生部
705	收發部

五、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

（無）

六、發明說明：

【發明所屬之技術領域】

本揭示係關於密碼處理裝置、密碼處理方法及程式。更詳言之，係關於執行共用金鑰系密碼之密碼處理裝置、密碼處理方法及程式。

【先前技術】

隨資訊化社會發展，用以保護處理資訊安全之資訊保全技術之重要性日益增加。作為資訊保全技術構成要素之一有密碼技術，目前於各種產品、系統已使用密碼技術。

密碼處理演算法有多種多樣，作為基本技術之一，有被稱為共用金鑰區塊密碼者。共用金鑰區塊密碼中，用以加密之金鑰與用以解密之金鑰為共通者。加密處理、解密處理皆由該共用金鑰產生複數個金鑰，以某區塊單位、例如64位元、128位元、256位元等之區塊資料單位重複執行資料轉換處理。

作為具代表性之共用金鑰區塊密碼之演算法，已知有先前之美國標準之DES(Data Encryption Standard，資料加密標準)、或目前之美國標準之AES(Advanced Encryption Standard，先進加密標準)。如今亦持續提案出各種其他之共用金鑰區塊密碼，2007年由索尼股份公司提案之CLEFIA亦為共用金鑰區塊密碼之一。

藉此，共用金鑰區塊密碼之演算法主要藉由具有重複執行輸入資料之轉換之回合函數執行部之密碼處理部、及產生於應用回合函數部之各回合之回合金鑰的金鑰排程部而

構成。金鑰排程部基於秘密金鑰之主金鑰(master key)，首先產生使位元數增加之擴張金鑰，並基於所產生之擴張金鑰，產生在密碼處理部之各回合函數部應用之回合金鑰(副金鑰)。

作為執行此種演算法之具體結構，已知有重複執行包含線性轉換部及非線性轉換部之回合函數之結構。例如代表性結構有Feistel結構、與一般性Feistel結構。Feistel結構與一般性Feistel結構具有藉由單純重複執行包含作為資料轉換函數之F函數的回合函數，而將明文轉換為密文之結構。在F函數中執行線性轉換處理及非線性轉換處理。另，作為記述關於應用Feistel結構之密碼處理之文獻，有例如非專利文獻1、非專利文獻2。

作為評價區塊密碼安全性之指標之一，有被稱為擴散(diffusion)特性者。該特性可被視為使輸入資料之變化波及(擴散)輸出資料之特性，且謀求安全性區塊密碼中如此之輸入資料之變化之影響儘可能快速地傳遞至輸出資料。

為提高擴散(diffusion)特性，預測例如增加回合函數之重複次數係有效。然而，先前技術中尚未揭示有關於如何以更少之回合函數之重複次數來提升擴散(diffusion)特性之技術。

[先前技術文獻]

[非專利文獻]

[非專利文獻1]K. Nyberg,「Generalized Feistel networks」, ASIACRYPT 96, Springer Verlag, 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]

本揭示係鑒於例如上述狀況而完成者，其目的在於提供一種提升擴散(diffusion)特性之安全性高的密碼處理裝置、密碼處理方法及程式。

[解決問題之技術手段]

本揭示之第1態樣係一種密碼處理裝置，其包含密碼處理部，該密碼處理部係將作為資料處理對象之資料之構成位元分割成複數列而輸入，且對各列之資料重複執行應用回合函數之資料轉換處理；

上述密碼處理部係將以分割數d分割輸入資料即n位元資料之n/d位元資料輸入上述各列，且將包含應用上述回合函數之資料轉換處理之運算作為回合運算而重複執行之構成，且

執行如下處理：將具有回合運算之輸出資料之列之n/d位元資料再分割成d/2個，將該再分割資料再度組合，再構成與前段之回合運算之輸出資料不同之d個n/d位元資料，而設定作為次段之回合運算之輸入資料。

再者，在本揭示之密碼處理裝置之一實施形態中，上述回合函數包含：應用回合金鑰之運算；非線性轉換處理；

包含線性轉換處理之F函數；及與對F函數之輸入或輸出之其他列資料之互斥或運算(Exclusive-OR operation)。

再者，在本揭示之密碼處理裝置之一實施形態中，上述密碼處理部係藉由滿足下述(1)~(3)之分配條件之處理，將前段之回合運算之運算結果設定作為次段之回合運算之輸入：

(1)F函數輸入側資料序列必然分配至下一回合函數之互斥或側資料序列；

(2)互斥或側資料序列必然分配至下一回合函數之F函數輸入側資料序列；

(3)各自分割為d/2個之資料序列不重複地分別分配至d/2處之下一回合函數之資料序列。

再者，在本揭示之密碼處理裝置之一實施形態中，上述密碼處理部具有輸入資料之分割數d為4以上之一般性Feistel結構。

再者，在本揭示之密碼處理裝置之一實施形態中，上述密碼處理部係執行如下處理：將具有回合運算之輸出資料之d個列之各n/d位元資料再分割成d/2個，生成d×(n/d)個再分割資料，並將從對應分割數d之d條之列之不同列中選出之d/2個再分割資料進行再組合，再構成與前段之回合運算之輸出資料不同之d個n/d位元資料，而設定為次段之回合運算之輸入資料。

再者，在本揭示之密碼處理裝置之一實施形態中，上述密碼處理部當其全輸出位元成滿足下述2個條件之擴散

(diffusion)狀態，即，在將輸出位元描述為輸入位元之關係式之情形下，係實現滿足下述2個條件之全擴散(full diffusion)狀態之構成：

(條件1)全輸入位元包含於關係式；

(條件2)全輸入位元至少通過一次上述回合函數。

再者，在本揭示之密碼處理裝置之一實施形態中，上述密碼處理部係藉由4回合之回合運算而實現上述全擴散(full diffusion)狀態。

再者，在本揭示之密碼處理裝置之一實施形態中，決定上述密碼處理部之前段之回合運算之輸出資料、與次段之回合運算之再分割資料之輸入輸出關係之連接構成，係自將藉由具有回合運算輸出資料之列之n/d位元資料之再分割處理所生成之d×(n/d)個再分割資料之組合資料、即(d/2)個2n/d位元資料集作為單位之連接構成中選擇之連接構成。

再者，在本揭示之密碼處理裝置之一實施形態中，上述密碼處理部具有可應用於加密處理與解密處理兩者之對合性(involutions)。

再者，在本揭示之密碼處理裝置之一實施形態中，上述密碼處理部之各回合運算之再分割資料之再構成處理係根據預先決定之規則，將前段之回合函數輸入側序列之再分割資料分配至次段之互斥或側序列，且根據預先決定之規則，將前段之互斥或側序列之再分割資料分配至次段之回合函數輸入側序列之構成。

再者，在本揭示之密碼處理裝置之一實施形態中，上述密碼處理部係執行將作為輸入資料之明文轉換為密文之加密處理，或將作為輸入資料之密文轉換為明文之解密處理。

再者，本發明之第2態樣係一種密碼處理方法，其係在密碼處理裝置中執行者，且包含：密碼處理步驟，其係由密碼處理部將作為資料處理對象之資料之構成位元分割成複數列並輸入，並重複執行對各列之資料應用回合函數之資料轉換處理；

上述密碼處理步驟係將以分割數d分割輸入資料的n位元資料之n/d位元資料輸入上述各列，將包含應用上述回合函數之資料轉換處理之運算作為回合運算而重複執行，且

執行如下處理：將具有回合運算之輸出資料之列之n/d位元資料再分割成d/2個，將該再分割資料再度組合，再構成與前段之回合運算之輸出資料不同之d個n/d位元資料，而設定為次段之回合運算之輸入資料。

再者，本發明之第3態樣係一種程式，其係在密碼處理裝置中執行密碼處理者，且使密碼處理部執行將成為資料處理對象之資料之結構位元分割成複數列並輸入、且重複執行對各列之資料應用回合函數之資料轉換處理之密碼處理步驟；

在上述密碼處理步驟中，將以分割數d分割輸入資料的n位元資料之n/d位元資料輸入上述各列，使包含應用上述回合函數之資料轉換處理之運算作為回合運算而重複執

行；且

執行如下處理：將具有回合運算之輸出資料之列之n/d位元資料再分割成d/2個，將該再分割資料再度組合，再構成與前段之回合運算之輸出資料不同之d個n/d位元資料，而設定作為次段之回合運算之輸入資料。

另，本發明之程式係可利用例如記憶媒體而對可執行各種程式、編碼之資訊處理裝置或電腦系統提供之程式。藉由在資訊處理裝置或電腦系統上之程式執行部執行此種程式，而實現對應於程式之處理。

再者，本發明其他之目的、特徵、及優點將基於下文記述之本發明實施例與附圖藉由更詳細之說明當可明瞭。此外，本說明書中，系統是指複數裝置之邏輯性集合構成，各構成之裝置不限於同一殼體內者。

[發明之效果]

根據本發明之一實施例，可實現擴散(diffusion)特性提高之安全性高之密碼處理。

具體而言，係包含：密碼處理部，其係將成為資料處理對象之資料之構成位元分割成複數列並輸入、重複執行對各列之資料應用回合函數之資料轉換處理；在密碼處理部中，將以分割數d分割輸入資料的n位元資料之n/d位元資料輸入各列，將包含應用回合函數之資料轉換處理之運算作為回合運算而重複執行。且執行如下處理：將具有回合運算之輸出資料之列之n/d位元資料分割成d/2個，使該分割資料組合，再構成與前段之回合運算之輸出資料不同之

d個n/d位元資料，並作為次段之回合運算之輸入資料。藉由如此構成，可實現擴散(diffusion)特性提高之安全性高之密碼處理。

【實施方式】

以下，一邊參照圖式一邊對本揭示之密碼處理裝置、密碼處理方法及程式加以詳細說明。說明按以下項目進行。

1．共用金鑰區塊密碼之概要

2．關於擴散(diffusion)特性之概要

(2-1)關於擴散(diffusion)特性之說明

(2-2)關於目前為止考慮擴散(diffusion)特性之構成例

3．關於根據本揭示提高擴散(diffusion)特性之構成例

4．關於具有更高效率之資料分配法之構成例

5．關於具備對合(involution)性之構成例

6．關於密碼處理裝置之構成例

7．本揭示之構成匯總

[1．共用金鑰區塊密碼之概要]

首先對共用金鑰區塊密碼之概要加以說明。

(1-1．共用金鑰區塊密碼)

此處作為共用金鑰區塊密碼(以下稱為區塊密碼)係指定義於下文中者。

區塊密碼係以輸入取得明文P與金鑰K，並輸出密文C。明文與密文之位元長稱為區塊尺寸，此處表示為n。n可取任意整數值，但通常針對每區塊密碼演算法已預先決定1個值。有時亦將區塊長為n之區塊密碼稱為n位元區塊密

碼。

金鑰之位元長以k表示。金鑰可取任意整數值。共用金鑰區塊密碼演算法係對應1個或複數個金鑰尺寸。例如，某區塊密碼演算法A之區塊尺寸n=128，亦可有對應k=128、或k=192、又或k=256之金鑰尺寸之構成。

明文P：n位元

密文C：n位元

金鑰K：k位元

圖1係顯示對應k位元之金鑰長之n位元共用金鑰區塊密碼演算法E之圖。

對應加密演算法E之解密演算法D係可定義為加密演算法E之倒函數E^{-1}，且以輸入取得密文C與金鑰K，並輸出明文P。圖2係顯示對應圖1所示之密碼演算法E之解密演算法D之圖。

(1-2．內部構成)

區塊密碼可分為2部分來考慮。其中一部分係「金鑰排程部」，其係將金鑰K作為輸入，藉由某個既定之步驟，輸出可擴張位元長之擴張金鑰K'(位元長k')；另一部分為「資料加密部」，其接收明文P與自金鑰排程部擴張之金鑰K'，且進行資料轉換而輸出密文C。

2部分之關係係如圖3所示。

(1-3．資料加密部)

以下實施例中所用之資料加密部係可分割為被稱為回合函數之處理單位者。回合函數係以輸入取得2個資料，在

內部實施處理後輸出1個資料。輸入資料之一者係加密期間之n位元資料，成為某回合中將回合函數之輸出供給作為下一回合之輸入而構成。另一項輸入資料係使用由金鑰排程輸出之擴張金鑰之一部分之資料，該金鑰資料被稱為回合金鑰。另，回合函數之總數被稱為總回合數，係預先設定於每個密碼演算法之值。此處以R表示總回合數。

將自資料加密部之輸入側來看為第1回合之輸入資料作為X_1，且將輸入至第i下一回合函數之資料作為X_i，若回合金鑰設為RK_i，則資料加密部整體係如圖4所示。

(1-4．回合函數)

利用區塊密碼演算法可採取各種形態之回合函數。回合函數係可藉由該密碼演算法所採用之結構(structure)來分類。作為代表性之結構，此處例示有SPN結構、Feistel結構、及擴張Feistel結構。

(A)SPN結構回合函數

對所有n位元之輸入資料，應用與回合金鑰之互斥或運算、非線性轉換、及線性轉換處理等而構成。各運算之順序未特別決定。圖5係顯示SPN結構之回合函數之例。

(B)Feistel結構

將n位元之輸入資料分割為n/2位元之2個資料。應用具有將其中一者之資料與回合金鑰作為輸入之函數(F函數)，且將輸出與其中另一者之資料進行互斥或運算。其後將資料左右替換者作為輸出資料。F函數之內部構成雖亦有各種類型，但基本與SPN結構相同，以與回合金鑰資

料之互斥或運算、非線性運算、及線性轉換之組合來實現。圖6係顯示Feistel結構之回合函數之一例。

(C)擴張Feistel結構

擴張Feistel結構係將Feistel結構中資料分割數為2者擴張為分割成3以上之形式者。若將分割數設為d，則藉由d可定義各種擴張Feistel結構。F函數之輸入輸出之尺寸由於相對變小，故被認為適於小型安裝。圖7係顯示d=4且一回合內並列應用2個F函數之情形之擴張Feistel結構之一例。又，圖8係顯示d=8且一回合內應用1個F函數之情形之擴張Feistel結構之一例。

(1-5．非線性轉換處理部)

非線性轉換處理部有若輸入之資料尺寸變大則安裝成本變高之傾向。為避免該問題，多採用將對象資料分割成複數個單位，並分別對各者實施非線性轉換之構成。例如，將輸入尺寸作為ms位元，且將該等分割為每s位元之m個資料，並對各者進行具有s位元輸入輸出之非線性轉換之構成。該等之s位元單位之非線性轉換被稱為S-box。圖9顯示其例。

(1-6．線性轉換處理部)

線性轉換處理部在其性質上可定義為矩陣。矩陣之要素係$GF(2^8)$之個體要素或GF(2)之要素等，一般可有多種表現。圖10係顯示具有ms位元之輸入輸出，且藉由根據$GF(2^s)$定義之m×m之矩陣所定義之線性轉換處理部之例。

[2．關於擴散(diffusion)特性之概要]

在說明本發明之密碼處理之前針對擴散(diffusion)特性之概要加以說明。

(2-1)針對擴散(diffusion)特性之說明

如先前簡單之說明，作為評價區塊密碼安全性之指標之一，有被稱為diffusion(擴散)特性者。該特性可認為係輸入資料之變化波及(擴散)輸出資料之特性，且要求安全性區塊密碼中如此輸入資料之變化之影響儘快傳遞至輸出資料。

在下文中定義「擴散狀態」、「全擴散狀態」、及「全擴散回合數」。

某輸出位元以輸入位元關係式描述，且滿足以下條件時，該輸出位元係定義為「擴散狀態」。

(條件1)全輸入位元包含於關係式

(條件2)全輸入位元至少通過一次上述回合函數(F函數)

再者，將全輸出位元成擴散(diffusion)狀態定義為全擴散(full diffusion)狀態。

將為滿足該全擴散(full diffusion)狀態之最低限度需要之回合數(重複數)定義為「全擴散(full diffusion)回合數」。

關於該等定義，作為具體例使用具有如圖11、圖12所記載之Feistel結構之區塊密碼來詳細說明。圖11係表示具有Feistel結構之區塊密碼之回合函數之構成例，圖12係表示將該回合函數重複執行3回合之結構。

將自圖12中第i、i+1、i+2回合輸出之左側(第i+1、i+2、

i+3輸入之左側)之n/2位元資料X_{i+1}^1、X_{i+2}^1、X_{i+3}^1及第i、i+1、i+2回合輸出之右側(第i+1、i+2、i+3輸入之右側)之n/2位元資料X_{i+1}^2、X_{i+2}^2、X_{i+3}^2可分別使用第i回合輸入之X_i^1、X_i^2、與回合金鑰RK_i^1、RK_i^2、RK_i^3，以下述方式表現。

$X_{i+1}^1=F(RK_i^1, X_i^1)(+)X_i^2$

$X_{i+2}^1=F(RK_{i+1}^1, X_{i+1}^1)(+)X_{i+1}^2=F(RK_{i+1}^1, F(RK_i^1, X_i^1)(+)X_i^2)(+)X_i^1$

$X_{i+3}^1=F(RK_{i+2}^1, X_{i+2}^1)(+)X_{i+2}^2=F(RK_{i+2}^1, F(RK_{i+1}^1, X_{i+1}^1)(+)X_{i+1}^2)(+)X_{i+2}^2$

$=F(RK_{i+2}^1, F(RK_{i+1}^1, F(RK_i^1, X_i^1)(+)X_i^2)(+)X_i^1)(+)F(RK_i^1, X_i^1)(+)X_i^2$

$X_{i+1}^2=X_i^1$

$X_{i+2}^2=X_{i+1}^1=F(RK_i^1, X_i^1)(+)X_i^2$

$X_{i+3}^2=X_{i+2}^1=F(RK_{i+1}^1, X_{i+1}^1)(+)X_{i+1}^2=F(RK_{i+1}^1, F(RK_i^1, X_i^1)(+)X_i^2)(+)X_i^1$

另，上述式中，F(K，X)係表示將資料X使用參數K以F函數予以轉換之資料，(+)表示每位元之互斥或(exclusive OR)。

X_{i+1}^1係使用輸入資料X_i^1、X_i^2來表現，但由於Xi^2未通過F函數，故不成擴散(diffusion)狀態。X_{i+2}^1係使用輸入資料X_i^1、X_i^2來表現，且該等輸入資料係作為F函數之輸入被給與，故可謂係處於擴散(diffusion)狀態。同理，X_{i+3}^1亦可謂處於擴散(diffusion)狀態。

因X_{i+1}^2係僅以X_i^1表現，又由於X_i^2未通過F函數，故X_{i+2}^2不成擴散(diffusion)狀態。X_{i+3}^2係滿足條件，因此成擴散(diffusion)狀態。

自上述結果得知由於第i+3回合輸出之X_{i+3}^1，X_{i+3}^2係同時成擴散(diffusion)狀態，故稱為全擴散(full diffusion)狀態。如此可知具有如圖11、圖12所示之Feistel結構之區塊密碼之全擴散(full diffusion)回合數為3下一回合。

在未成全擴散(full diffusion)狀態之情形下，由於特定之輸出位元變得不受特定之輸入位元與非線性函數(F函數)之影響，故預計在面對各種攻擊時將變得脆弱。尤其擴散(diffusion)特性亦作為直接評價面對不能差分攻擊、飽和攻擊等攻擊時之安全性之指標來使用。因此，可以說全擴散(full diffusion)回合數較少者，其擴散(diffusion)特性較高。

圖13、圖14中例舉有其他例。該等之圖係顯示4-列中於1段中使用2個F函數之一般性Feistel結構。

圖15中顯示將第i下一回合之n-位元輸入X_i分割成每個各占n/4-位元之4個，且在僅使該第4個之n/4-位元資料(表示為X_i^4)的一部分變化之情形下，其影響之波及。

其中，圖中粗虛線係表示輸入之變化以未通過F函數之狀態來傳播之資料，粗線係表示輸入之變化以至少通過1次F函數之狀態來傳播之資料。又，F函數之各輸出位元係假設受F函數之全輸入位元之影響。如此，假定所有輸入位元之變化，即可求得全輸出位元受影響之前之回合數，

亦可求得全擴散(full diffusion)回合數。實際上已知d=4，於1段中使用2次F函數之一般性Feistel結構之全擴散(full diffusion)回合數為5回合。

(2-2)關於目前為止考慮擴散(diffusion)特性之構成例

其次，對考慮目前為止提案之擴散(diffusion)特性之處理構成之概要加以說明。

一般而言，已知在1段中使用d/2個F函數之d-列一般性Feistel結構之擴散(diffusion)特性並非很好，且全擴散(full diffusion)回合數變為d+1回合。其係如非專利文獻3(T. Suzaki, k. Minematsu,「Improving the Generalized Feistel」, FSE 2010, LNCS6147, pp.19-39, 2010.)所描述。

圖16係顯示d=6之情形下之通常一般性Feistel結構，圖17係顯示作為同構成之全擴散(full diffusion)狀態之路徑之一例。

非專利文獻3中，為解決該課題提案有藉由分別變更分割成每個各占n/d位元之d個資料之回合間配線，而使分割數d為6以上之情形，可以全擴散(full diffusion)回合數比先前構成要少之構成法。

圖18係顯示d=6之情形之該構成法，又，圖19係顯示作為該情形之全擴散(full diffusion)狀態之路徑之一例。

已知以該構成達成之全擴散(full diffusion)回合數係在d=6、8、10、12、14、16之情形下，分別為5、6、7、8、8、8回合，且取得比通常構成之d+1回合更良好之擴散(diffusion)特性。然而，該構成於d=4之情形下無效，且無

法削減以上全擴散(full diffusion)回合數。

又，非專利文獻4(洲崎，角尾，久保，川幡，「於一般性Feistel結構中組合擴散層之構造提案」，SCIS2008，2008)中，提案有藉由分別對分割成每個各n/d位元之d個資料實施線性運算，而使擴散(diffusion)特性變得比先前要高之構成。然而，在該構成之情形下，由於有必要安裝用以線性運算之機構，故致使安裝成本增大。

[3．關於根據本揭示提高擴散(diffusion)特性之構成例]

鑒於上述問題，本揭示係提案有不增大一般性Feistel結構之安裝成本，而取得高擴散(diffusion)特性之構成法。

本構成中，首先與通常之構成相同，在d-列之一般性Feistel構造中，將n位元輸入資料分割成每個n/d位元之d個資料，並分別進行F函數處理、及互斥或處理(圖20：步驟1)。

此時，將輸入F函數之資料序列稱為F函數輸入側資料序列，將互斥或運算資料序列稱為互斥或側資料序列。

其後，將各序列(各列)中傳送之各個n/d位元資料再分割成d/2個資料(此時之分割亦可不為等分割)。

將各序列(各列)中分別再分割成d/2個之資料，依下述規則分配(圖20：步驟2)。

(1)F函數輸入側資料序列係必須分配至下一回合函數之互斥或側資料序列。

(2)互斥或側資料序列係必須分配至下一回合函數之F函數輸入側資料序列

(3)分割成d/2個之資料序列係無重複分別分配至d/2處之下一回合函數之資料序列

如此分配後，將分割成各d/2個之資料分別與1個資料結合(圖20：步驟3)。

此必須重複執行必要回數。

圖20係顯示分割數d=4之情形之構成例。

如此構成之情形下，無關資料之分割數d，亦可實現全擴散(full diffusion)回合數4。

本方式無關分割數d，亦滿足實現全擴散(full diffusion)之回合數=4之理由係如下所示。

(1)第i回合之所有輸入資料之變化係至少影響第i+1回合之一個F函數。

(2)第i+1回合之互斥或側資料序列中至少1個成擴散(diffusion)狀態。

(3)第i+1回合之互斥或側資料序列中，成擴散(diffusion)狀態之資料係進而分割成d/2個，並影響第i+2回合之d/2個之全F函數。因此，第i+2回合之全互斥或側資料序列係成擴散(diffusion)狀態。

(4)由於第i+2回合之互斥或側資料序列係作為第i+3回合之F函數輸入側資料序列，故第i+3回合之F函數輸入側資料序列成全擴散(full diffusion)狀態。又，因該等擴散(diffusion)狀態之資料被輸入第i+3回合之所有F函數，故與其輸出進行互斥或運算之互斥或側資料序列亦全體成擴散(diffusion)狀態。

由上述理由可知，必須在第i+3回合後，即在第4回合成全擴散(full diffusion)狀態。使用圖21、22顯示具體例。

圖21係顯示d=4之情形下本方式之一例。由於d=4，故將分割成4個之各n/4位元資料進而再分割為二(=d/2)。

將對應第i回合輸入X_i^1之第i回合輸出之2分割資料分別作為Y_i^{1L}、Y_i^{1R}，同樣將對應X_i^2、X_i^3、X_i^4之各分割資料作為Y_i^{2L}、Y_i^{2R}、Y_i^{3L}、Y_i^{3R}、Y_i^{4L}、Y_i^{4R}。該等分割資料之尺寸於等分割時為n/8位元。

然而，各列資料之再分割處理未必需要等分割。例如輸入位元數=256位元，且分割數d=4之情形，

各列之位元數係d/4=256/4=64位元，該再分割資料若等分割，則為32位元，從而產生2個32位元資料。

然而未必須等分割，亦可將由64位元之資料產生之再分割資料分割成20位元與44位元等之任意組合。

其中，在輸入至下一回合運算部時，藉由不同列中所分割之20位元與44位元之組合，再構成分割數d=4個之64位元單位之資料，並輸入至各分割列。

亦即在分割數d之構成中，d列之各列之再分割處理雖未必須等分割，但d列之各列之再分割形式(分割比例)係必須一致。

此時，對第i回合輸入資料之某處施加變化之情形，其影響係必須輸入第i+1回合之2個F函數中之至少1個。例如，僅對X_i^4之LSB1位元施加變化之情形，其影響係僅傳播至Y_i^{4R}，繼而其影響傳播至X_{i+1}^1，且該X_{i+1}^1係輸入第i+1

回合之左側F函數(圖22)。對輸入位元之其他位置施加變化之情形亦可同樣考慮，並保證傳播對至少1個F函數之影響。

由於第i+1回合之F函數中至少1個F函數被輸入變化所影響，故其輸出與互斥或運算資料係成擴散(diffusion)狀態。即，保證(Y_{i+1}^{2L}，Y_{i+1}^{2R})，(Y_{i+1}^{4L}，Y_{i+1}^{4R})之任意組係成擴散(diffusion)狀態。圖22顯示(Y_{i+1}^{2L}，Y_{i+1}^{2R})成擴散(diffusion)狀態之例。

根據本方式之規則2、3，第i+1回合之輸出Y_{i+1}^{2L}、Y_{i+1}^{2R}係輸入至第i+2回合之2(=d/2)個全F函數。同樣，Y_{i+1}^{4L}、Y_{i+1}^{4R}亦輸入至第i+2回合之全F函數。亦即，即使第i+1回合中(Y_{i+1}^{2L}，Y_{i+1}^{2R})，(Y_{i+1}^{4L}，Y_{i+1}^{4R})之任意組係成擴散(diffusion)狀態，第i+2回合之全F函數中亦輸入有擴散(diffusion)狀態之資料。藉此，該等F函數之輸出與互斥或資料Y_{i+2}^{2L}，Y_{i+2}^{2R}，Y_{i+2}^{4L}，Y_{i+2}^{4R}係成全體擴散(diffusion)狀態，該等係因根據規則2、3供給至X_{i+3}^{1}、X_{i+3}^{3}，故可知X_{i+3}^{1}、X_{i+3}^{3}亦成擴散(diffusion)狀態。

由於處於該等擴散(diffusion)狀態之X_{i+3}^{1}、X_{i+3}^{3}係輸入至第i+3回合之各個F函數，故其輸出與互斥或運算結果的Y_{i+2}^{2L}、Y_{i+2}^{2R}、Y_{i+2}^{4L}、Y_{i+2}^{4R}即X_{i+4}^{1}、X_{i+4}^{3}亦成擴散(diffusion)狀態。

由上述結果可知，本方式可滿足全擴散(full diffusion)回合數4。圖22係顯示在d=4之情形之本方式中成全擴散(full diffusion)狀態之路徑之一例。已知該構成例可實現

比先前構成之全擴散(full diffusion)回合數5更少之4回合。圖22係顯示滿足該構成中d=4之情形之全擴散(full diffusion)之路徑之一例。

又，圖23顯示d=6之情形之構成例、圖24顯示該情形下成全擴散(full diffusion)狀態之路徑之一例(描述於圖中回合間替換前後之數字係表示用以顯示替換後資料配置於哪個位置之索引)。

如上說明之本揭示之構成中，已知與先前之構成相比，可取得極高之擴散(diffusion)特性。又，本揭示之構成中，由於未包含線性運算，故不會使安裝成本增加。

如此，本實施例具有：密碼處理部，其係將作為資料處理對象之資料之構成位元分割成複數列並輸入、且對各列之資料重複執行應用回合函數之資料轉換處理，在該密碼處理部中，重複執行伴隨如下之資料之再分割與再構成之回合運算。

即，密碼處理部係以分割數d分割輸入資料即n位元資料之n/d位元資料輸入上述各列，且將包含應用上述回合函數之資料轉換處理之運算作為回合運算而重複執行。

在重複該回合運算處理時，執行如下處理：將具有回合運算之輸出資料之列之n/d位元資料再分割成d/2個，且使該再分割資料再度組合，再構成與前段之回合運算之輸出資料不同之d個n/d位元資料，而設定作為次段之回合運算之輸入資料。

具體而言，執行滿足如下條件之再分割與再構成處理：

(1)F函數輸入側資料序列必然分配至下一回合函數之互斥或側資料序列；

(2)互斥或側資料序列必然分配至下一回合函數之F函數輸入側資料序列；

(3)分割為各d/2個之資料序列不重複地分別分配至d/2處之下一回合函數之資料序列。

進行滿足如上條件之處理。

例如，密碼處理部係執行如下處理：將具有回合運算之輸出資料之d列各n/d位元之資料再分割成d/2個，生成d×(n/d)個再分割資料，並從對應分割數d之d條之列之不同列中選出d/2個再分割資料進行組合，再構成與前段之回合運算之輸出資料不同之d個n/d位元資料，而設定作為次段之回合運算之輸入資料。

藉由執行該等處理，可將用以滿足上述全擴散(full diffusion)狀態所必須之最低限度之回合數(重複數)，即「全擴散(full diffusion)回合數」設定為4。

另，如上所述，在將某輸出位元作為輸入位元之關係式來描述，且滿足下述條件之情形下，該輸出位元係定義成「全擴散(full diffusion)狀態」。

(條件1)全輸入位元包含於關係式。

(條件2)全輸入位元至少通過一次上述回合函數(F函數)。

再者，全輸出位元成擴散(diffusion)狀態之情形係「全擴散(full diffusion)狀態」。

在作為本揭示之實施例加以說明之構成例中，對傳送將輸入n位元資料d分割後之資料之各列，即，將各自以(d/2)列F函數輸入側資料序列之列、與(d/2)列互斥或側序列之列而傳送之各n/d位元資料分別分割成d/2個之例加以說明。

此係用以實現滿足全擴散(full diffusion)之最小回合數=4之設定。

圖25係顯示分割數d：d=6之情形下，將以各列傳送之n/d位元資料(n/6位元資料)進行2分割，即分割成d/12位元並進行回合間傳送之構成例。

然而，若未將回合數限定為4，則用以實現全擴散(full diffusion)之分割數係不限定各列各為(d/2)個。

輸入n位元之分割數：d、與

各列各自之分割數：p、及

用以實現全擴散(full diffusion)之回合數，

該等之對應關係如圖26所示。

若將資料序列適當分配，則全擴散(full diffusion)回合數可以如下公式算出。

回合數$=3+[\log_p(d/2)]$

其中，[x]係為x以上之最小之整數。

再者，作為擴張例，圖27係顯示F函數輸入側資料序列與互斥或側資料序列分別進行不同分割之構成。

圖27所示之構成係分割數d：d=6之情形，

對(d/2)=3列之F函數輸入側資料序列之列進行2分割，

對(d/2)=3列之互斥或側序列之列進行3分割之例。

以如此之構成，若適當分配資料序列，則全擴散(full diffusion)回合數可為4。

又，本方式係無關擴張金鑰(回合金鑰)之插入位置亦可取得效果。圖28係顯示變更圖21中描述之構成例之擴張金鑰(回合金鑰)之插入位置之構成例。

圖21中，將擴張金鑰(回合金鑰)插入各F函數並應用。

對此，如圖28所示之構成中，將擴張金鑰(回合金鑰)插入F函數輸出與互斥或側資料序列之互斥或運算部。

即使在如此構成中，亦藉由利用上述各回合間資料之再分割處理之傳送構成，實現全擴散(full diffusion)回合數之削減。

[4．關於具有更高效率之資料分配法之構成例]

上述項目[3．關於根據本揭示提高擴散(diffusion)特性之構成例]之一般性Feistel結構中，對藉由不增加安裝成本亦取得高擴散(diffusion)特性之構成法加以說明。

即，以分割數d將輸入資料之n位元資料分割成n/d位元資料並輸入各列，在將包含應用回合函數之資料轉換處理之運算作為回合運算而重複執行之構成中，進而將具有回合運算之輸出資料之各列之n/d位元資料再分割成d/2個，且使該再分割資料組合，再構成與前段之回合運算之輸出資料不同之d個n/d位元資料，並作為次段之回合運算之輸入資料而執行處理之構成。

以下，對與上述實施例中說明之資料分配法相比更有效

率之技術加以說明。

首先，參照圖29對本實施例之基板構成例加以說明。

本構成首先與上述項目[3]所說明之實施例相同，在d-列之一般性Feistel結構中，以分割數d將n位元輸入資料分割成各n/d位元之d個資料，並各自將包含應用回合函數之資料轉換處理之運算作為回合運算而重複執行。

在i段回合運算後，再分別將d個之各列(序列)之n/d位元序列分割成d/2個。

在第i段之回合運算後分割成各列(序列)各自為d/2個之輸出資料之資料中，將第j項資料表示為$Y_i[j]$(其中，j係1以上$d^2/2$以下之整數)。

同樣，在將第i+1段之回合運算部中分割數：d之各列單位之n/d位元分別再分割成d/2個之資料中，將第j項資料表示為$X_{i+1}[j]$(其中，j係1以上$d^2/2$以下之整數)。

又，$YY_i[t]$在$Y_i[j]$中，作為將滿足$j=(d/2)s+t$者按序連結之資料。

其中s係0以上(d-1)以下，t係1以上d/2以下之整數。

具體而言，例如

$YY_i[1]=Y_i[1]||Y_i[1\times d/2+1]||Y_i[2\times d/2+1]||...||Y_i[(d-1)\times d/2+1]$、

$YY_i[2]=Y_i[2]||Y_i[1\times d/2+2]||Y_i[2\times d/2+2]||...||Y_i[(d-1)\times d/2+2]$、

...

$YY_i[d/2]=Y_i[d/2]||Y_i[1\times d/2+d/2]||Y_i[2\times d/2+d/2]||...||Y_i[(d$

-1)×d/2+d/2]。

同樣，$XX_i[t]$在$X_i[j]$中作為將滿足$j=(d/2)s+t$者按序連結之資料。

其中，$X_i[j]$係將第i段之輸入資料分割成d個各n/d位元之資料分別分割成d/2個資料中第j項資料，

s係0以上(d-1)以下，t係1以上d/2以下之整數。

上述項目[3]中說明之技術中，因分配之模式變多而使評價需要時間。即，上述項目[3]所說明之技術中，只要為滿足如下(1)~(3)之條件之分配模式即可。

(1)F函數輸入側資料序列係必然分配至下一回合函數之互斥或側資料序列

(2)互斥或側資料序列係必然分配至下一回合函數之F函數輸入側資料序列

(3)分割為各d/2個之資料序列係不重複分別分配至d/2處之下一回合函數之資料序列。

滿足該等條件(1)~(3)之分配模式有很多。尤其如輸入資料之分割數d較大之情形，由於分配模式變得極多而無法簡單決定。此外，利用分配法亦存在安裝時成本變大之問題。

以下，提案有預先限定可容許選擇之分配模式，進而亦可降低安裝成本之分配法。本提案方式係作為改良上述項目[3]所說明之分配方式者。

首先，在將第i+1段輸入資料分割成各n/d位元之d個資料分別再分割成d/2個資料之第j項資料$X_{i+1}[j]$中，將僅使滿

足j=(d/2)s+t者按序連結之資料$XX_{i+1}[t]$之資料序列之2t-1資料部分循環移位至左側之資料序列作為$ZZ_{i+1}[t]$。

具體而言，例如：

由於$ZZ_{i+1}[1]=XX_{i+1}[1]<<<1$、故

$ZZ_{i+1}[1]=XX_{i+1}[1]<<<1$

$=(X_{i+1}[1]||X_{i+1}[1\times d/2+1]||X_{i+1}[2\times d/2+1]||...||X_{i+1}[(d-1)\times d/2+1])<<<1$

$=X_{i+1}[1\times d/2+1]||X_{i+1}[2\times d/2+1]||...||X_{i+1}[(d-1)\times d/2+1]||X_{i+1}[1]$。

藉由使用如上定義之$YY_i[j]$、及$ZZ_{i+1}[j]$，自各$YY_i[j]$中無重複逐個選擇$ZZ_{i+1}[j]$並連接，可決定將第i回合之資料轉換為第i+1回合之資料。

圖30係例示輸入資料之分割數d：d=6之情形。

圖30中各中間變量係如下定義。

另，中間變量係以下三種資料。

$YY_i[t]$：在第i段之分割成d/2個輸出資料之第j項資料$Y_i[j]$(其中，j係1以上$d^2/2$以下之整數)中，將滿足j=(d/2)s+t(其中s係0以上(d-1)以下，t係1以上d/2以下之整數)者按序連結之資料。

$XX_{i+1}[t]$：在第i+1段之輸入資料分割成各n/d位元之d個者分別分割成d/2個資料之第j項資料$X_{i+1}[j]$中，將滿足j=(d/2)s+t(其中s係0以上(d-1)以下，t係1以上d/2以下之整數)者按序連結之資料。

$ZZ_{i+1}[t]$：僅使$XX_{i+1}[t]$之資料序列之2t-1資料部分循環

移位至左側之資料序列。

為該等之中間變量。

如圖30所示，輸入資料之分割數d：d=6之情形，

t係1以上d/2以下之整數，設定t=1、2、3之各值，且

作為中間變量，

第i段輸出資料對應之中間變量$YY_i[t]$：$YY_i[1]$、$YY_i[2]$、$YY_i[3]$

第i+1段移位前輸入資料對應之中間變量$XX_{i+1}[t]$:$XX_{i+1}[1]$、$XX_{i+1}[2]$、$XX_{i+1}[3]$

第i+1段移位後輸入資料對應之中間變量$ZZ_{i+1}[t]$:$ZZ_{i+1}[1]$、$ZZ_{i+1}[2]$、$ZZ_{i+1}[3]$

該等係以下述方式算出。

第i段輸出資料對應之中間變量$YY_i[t]$：$YY_i[1]$、$YY_i[2]$、$YY_i[3]$係如下設定。

$YY_i[1]=Y_i[1]||Y_i[4]||Y_i[7]||Y_i[10]||Y_i[13]||Y_i[16]$、

$YY_i[2]=Y_i[2]||Y_i[5]||Y_i[8]||Y_i[11]||Y_i[14]||Y_i[17]$、

$YY_i[3]=Y_i[3]||Y_i[6]||Y_i[9]||Y_i[12]||Y_i[15]||Y_i[18]$、

第i+1段移位前輸入資料對應之中間變量$XX_{i+1}[t]$:$XX_{i+1}[1]$、$XX_{i+1}[2]$、$XX_{i+1}[3]$係如下設定。

$XX_{i+1}[1]=X_{i+1}[1]||X_{i+1}[4]||X_{i+1}[7]||X_{i+1}[10]||X_{i+1}[13]||X_{i+1}[16]$、

$XX_{i+1}[2]=X_{i+1}[2]||X_{i+1}[5]||X_{i+1}[8]||X_{i+1}[11]||X_{i+1}[14]||X_{i+1}[17]$、

$XX_{i+1}[3]=X_{i+1}[3]||X_{i+1}[6]||X_{i+1}[9]||X_{i+1}[12]||X_{i+1}[15]||X_{i+1}$

[18]、

第i+1段移位後輸入資料對應之中間變量$ZZ_{i+1}[t]$：$ZZ_{i+1}[1]$、$ZZ_{i+1}[2]$、$ZZ_{i+1}[3]$係如下設定。

$ZZ_{i+1}[1]=$

$X_{i+1}[4]||X_{i+1}[7]||X_{i+1}[10]||X_{i+1}[13]||X_{i+1}[16]||X_{i+1}[1]$、

$ZZ_{i+1}[2]=$

$X_{i+1}[11]||X_{i+1}[14]||X_{i+1}[17]||X_{i+1}[2]||X_{i+1}[5]||X_{i+1}[8]$、

$ZZ_{i+1}[3]=$

$X_{i+1}[18]||X_{i+1}[3]||X_{i+1}[6]||X_{i+1}[9]||X_{i+1}[12]||X_{i+1}[15]$。

此處，如圖30所示，例如將$YY_i[1]$與$ZZ_{i+1}[1]$連接，$YY_i[2]$與$ZZ_{i+1}[2]$連接，$YY_i[3]$與$ZZ_{i+1}[3]$連接。該情形，作為如圖31上部之(a)所示之資料分配法。

此外，例如將$YY_i[1]$與$ZZ_{i+1}[2]$連接，$YY_i[2]$與$ZZ_{i+1}[3]$連接，$YY_i[3]$與$ZZ_{i+1}[1]$連接之情形係作為圖31下部之(b)所示之資料分配法。

如此，本實施例之密碼處理裝置之密碼處理部之設定，即，決定前段之回合運算之輸出資料、與次段之回合運算之再分割資料之輸入輸出關係之連接構成，係從藉由具有回合運算之輸出資料之列之n/d位元資料之再分割處理產生之d×(n/d)個再分割資料之組合資料之(d/2)個之2n/d位元之資料集作為單位之連接構成中選擇。

以上述方式決定之資料分配法係滿足上述項目[3]中說明之條件，即滿足該條件(1)~(3)：

(1)F函數輸入側資料序列係必然分配至下一回合函數之

互斥或側資料序列

(2)互斥或側資料序列係必然分配至下一回合函數之F函數輸入側資料序列

(3)分割為各d/2個之資料序列係不重複分別分配至d/2處之下一回合函數之資料序列。

因此，可改善擴散(diffusion)特性。

又，上述項目[3]之方法中，有必要將d/2×d/2種資料序列自d/2×d/2種資料序列中逐個選擇並分配(實際上，有進而再重複1次該處理之必要)，本方式中，由於將d/2種資料序列從d/2種資料序列中逐個選擇並分配即可，故可大量削減必須選擇之模式。再者，以上述方法選擇之分配法係因對資料之分配具有規則性，故可削減安裝成本。

[5．關於具備對合(involution)性之構成例]

通常之Feistel結構之加密函數係可如圖32所表示。又，通常之Feistel結構之解密函數係可如圖33所表示。

從該等圖32、圖33之構成可理解，只要適當替換插入F函數之擴張金鑰(回合金鑰)之順序，加密函數與解密函數幾乎可使用相同函數。如此，除去擴張金鑰(回合金鑰)之插入，將加密函數與解密函數可以相同構成實現之性質稱為對合性。

具有對合性之密碼處理構成中，若適當替換擴張金鑰(回合金鑰)之順序，則加密函數、與解密函數可共用，無須再另準備解密函數。因此，具有一般對合性之密碼與不具備對合性之密碼相比，可以較少安裝成本進行安裝。

又，加密函數與解密函數使用相同函數係可使驗證成本減半(驗證係只驗證加密函數、或解密函數之任一者即可)，亦具有可使代碼量減半等之優點。

如此，圖32、圖33之分割數d=2之通常之Feistel結構中，僅將插入F函數之擴張金鑰(回合金鑰)之順序適當替換，即可使加密函數與解密函數使用幾乎相同之函數，從而可簡單構成具有對合性之結構。

然而，包含分割數：d為2以外之構成之一般性Feistel結構(Generalized Feistel Networks)之對合性不能說是簡單構成。

從1段中使用d/2個F函數之d-列一般性Feistel結構之對合性來看(其中，d>2)。

如先前說明之圖14所示之4-列一般性Feistel結構中，若處理回合數為奇數，則可知具有對合性。例如以3回合構成之4-列一般性Feistel結構係具有對合性(5回合之構成亦相同)。然而處理回合數為偶數之情形下，係不具有對合性。

一般而言，在d-列一般性Feistel結構中，將構成回合數以分割數：d分割時之剩餘部分係僅在1、或(d/2)+1之情形下具有對合性。

例如，在如圖14所示之4-列一般性Feistel結構中，將構成回合數以分割數d=4分割時之剩餘部分係僅在1、或(d/2)+1=(4/2)+1=3之情形下具有對合性。

具體而言，構成回合數=1、3、5、7、9・・・

即僅在構成回合數為奇數之情形下具有對合性。

又，例如分割數d=6之6-列一般性Feistel結構中，將構成回合數以分割數d=6分割時之剩餘部分係僅在1、或(d/2)+1=(6/2)+1=4之情形下具有對合性。

具體而言，構成回合數=1、4、7、10、13・・・

構成回合數係僅在該等數之情形下具有對合性。

如此，在一般d-列一般性Feistel結構中，無關構成回合數而具有對合性之說法係不存在。

圖34係顯示藉由在上述項目[3・關於根據本揭示提高擴散(diffusion)特性之構成例]中說明之回合運算間之資料再分割、再合成處理而取得高擴散(diffusion)特性之4-列結構之一方式之圖。

該方式中，構成回合數係僅在1+3n(其中n為0以上整數)之情形下滿足對合性。

構成回合數係與安全性、安裝性能有較大關聯。若存在無關構成回合數而具有對合性之結構，則在可更靈活地設定回合數，且可更靈活地變更安全性、安裝性能外，藉由對合性之特性，亦可實現小型安裝。

對藉由不增加安裝成本而取得高擴散(diffusion)特性，進而無關構成回合數而滿足對合性之回合間替換之構成法加以說明。

以下說明之方式係在取得上述項目[3・關於根據本揭示提高擴散(diffusion)特性之構成例]中說明之高擴散(diffusion)特性之構成上，進而具有對合性之方式。

關於本方式之一例，參照圖35加以說明。本方式係如圖35所示，重複執行如下步驟1~3之處理。

(步驟1)

首先與通常構成相同，在分割數d之d-列一般性Feistel結構中，將n位元輸入資料對應分割數d，分割成各n/d位元之d個，且將各n/d位元輸入至各分割列，並分別進行F函數處理、互斥或處理。

此時，將輸入至F函數之資料序列稱為F函數輸入側資料序列，將互斥或運輸資料序列稱為互斥或側資料序列。

將F函數輸入側資料序列中最左側之F函數輸入側資料序列作為L(0)，例如自左側起按序表示為L(1)、...、L((d/2)-1)。

同樣，互斥或側資料序列例如自左側起按序表示為R(0)、...、R((d/2)-1)。

(步驟2)

其後，將各序列(列)之傳送資料的n/d位元資料進而再分割成d/2個。該再分割亦可不為等分割。

將該再分割之資料對各個F函數輸入側資料序列、互斥或側資料序列分別表現為$L(i)_j$、$R(i)_j$。

i係各序列(列)之識別碼(編號)、

j係1個序列(列)之再分割資料之各個識別碼(編號)。

例如，將由最左側之F函數輸入資料序列再分割成d/2個資料中最左側之資料作為$L(0)_0$，按序表示為$L(0)_1$、...、$L(0)_{d/2-1}$。

接著在各序列(列)中，將再分割成d/2個之資料根據下述規則來分配。

規則(2-1)

分配最左側之F函數輸入資料序列，即i=0之L(0)之資料。

將$L(0)_0$分配至下一回合函數之$R(0)_0$，

將$L(0)_1$分配至下一回合函數之$R(1)_1$，

同樣，將$L(0)_i$分配至$R(i)_i$，直至i=(d/2)-1。

即，

$L(0)_0= R(0)_0$，

$L(0)_1= R(1)_1$，

$L(0)_2= R(2)_2$，

．．．。

規則(2-2)

繼而分配L(1)之資料。

將$L(1)_0$分配至下一回合函數之$R(1)_0$，

將$L(1)_1$分配至下一回合函數之$R(2)_1$，

同樣，將$L(1)_i$分配至$R((i+1)\text{mod } d/2)_i$，直至i=(d/2)-1。

規則(2-3)

以下，重複與上述2相同之處理，直至L((d/2)-1)之資料。即，將$L(i)_j$分配至下一回合之$R((i+j)\text{mod } d/2)_j$(其中，i、j分別為0以上(d/2)-1以下)。

規則(2-4)

對互斥或側資料序列亦重複相同處理。即，將$R(i)_j$分配

至下一回合函數之$L(((d/2)+i-j)\bmod d/2)_j$。其中，i、j分別為0以上(d/2)-1以下。

(步驟3)

如此分配後，將分割成各d/2個之資料分別結合成1個資料。

將上述處理根據回合運算之執行回數重複必要之回數。

圖36係顯示在4-列(d=4)之情形下執行上述處理之構成之一構成例，

圖37係顯示在6-列(d=6)之情形下執行上述處理之構成之一構成例。

在該等如圖36、圖37所示之構成中，具有將各序列(列)中再分割成d/2個之資料根據如上述步驟2所示之規則(2-1)~(2-4)對月的回合進行再分配之構成。藉由該資料之再分割與再分配構成，該等之方式係無關回合數而具有對合性。

又，圖38、圖39雖係與上述構成例不同之構成法，亦無關構成回合數而具有對合性之方式。另，如先前項目[3]中說明之圖21所示之方式係若構成回合數為奇數，則具有對合性之構成之一例。

如此，密碼處理部之各回合運算之再分割資料之再構成處理係作為將前段之回合函數輸入側序列之再分割資料根據上述預先決定之規則，分配至次段之互斥或側序列，且將前段之互斥或側序列之再分割資料根據上述預先決定之規則，分配至次段之回合函數輸入側序列之構成。藉由該

構成，可實現具有可以相同構成應用加密處理與解密處理兩者之對合性之構成。

[6．關於密碼處理裝置之構成例]

最後，對執行根據上述實施例之密碼處理之密碼處理裝置之實施例加以說明。

執行根據上述實施例之密碼處理之密碼處理裝置係可搭載於執行密碼處理之各種資訊處理裝置中。具體而言，如PC、TV、錄音機、播放器、通訊機器、進而如RFID、智慧卡、傳感器網路機器、電池/蓄電池認證模組、健康醫療機器、及自載型網路機器等，可用於應對執行例如資料處理或通訊處理之密碼處理時之各種危機。

圖40中顯示作為執行本揭示之密碼處理之裝置之一例之IC模組700之構成例。上述處理係可於例如PC、IC卡、讀卡機、及其他各種資訊處理裝置中執行，圖40所示之IC模組700可於該等各種機器中構成。

圖40所示之CPU(Central processing Unit，中央處理單元)701係執行密碼處理之開始、結束、資料之收發控制、各構成部間之資料轉送控制、及其他各種程式之處理器。記憶體702包含CPU701所執行之程式、或儲存運算參數等固定資料之ROM(Read-Only-Memory，唯讀記憶體)、在CPU701之處理中執行之程式、在程式處理中適當變化之參數之儲存區域、及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係可作為密碼處理所必需之金鑰資料、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。另，資料儲存區域較好係作為具有防篡改構造之記憶體而構成。

密碼處理部703係執行上述說明之密碼處理構成，即，按照應用例如一般性Feistel結構或Feistel結構之共用金鑰區塊密碼處理演算法執行加密處理、解密處理。

另，此處，雖顯示將密碼處理機構作為個別模組之例，但亦可不設置如此之獨立之密碼處理模組，而是以例如將密碼處理程式儲存於ROM、由CPU701讀出並執行ROM儲存之程式之方式構成。

亂數產生部704係在產生密碼處理所必要之金鑰等時執行產生必要亂數之處理。

收發部705係執行與外部之資料通訊之資料通訊處理部，例如執行與讀卡機等之IC模組之資料通訊，且輸出在IC模組內產生之密文，或執行自外部之讀卡機等機器輸入之資料等。

另，上述實施例所說明之密碼處理裝置係不僅可用於將作為輸入資料之明文加密之加密處理，亦可用於將作為輸入資料之密文解密成明文之解密處理。

在加密處理、解密處理之兩者之處理中，可應用上述實施例所說明之構成。

[7．本揭示之構成匯總]

以上，一邊參照特定實施例並針對本發明加以詳細說明。然而，在未脫離本發明主旨之範圍內，熟知本技藝者

當可對該實施例進行修正或取代。亦即，以上以例示之形態揭示本發明，但不應限定性地解釋。為了判斷本發明之要旨，應參酌照專利申請範圍項。

另，本說明書所揭示之技術可取得如下構成。

(1)一種密碼處理裝置，其包含密碼處理部，其係將作為資料處理對象之資料之構成位元分割成複數列而輸入、且重複執行對各列之資料應用回合函數之資料轉換處理，

上述密碼處理部係將分割數d分割輸入資料之n位元資料的n/d位元資料輸入至上述各列，且將包含應用上述回合函數之資料轉換處理之運算作為回合運算而重複執行之構成，且

執行如下處理：將具有回合運算之輸出資料之列之n/d位元資料再分割成d/2個，使該再分割資料再度組合，再構成與前段之回合運算之輸出資料不同之d個n/d位元資料，而設定作為次段之回合運算之輸入資料。

(2)如上述(1)描述之密碼處理裝置，其中上述回合函數包含：應用回合金鑰之運算；非線性轉換處理；包含線性轉換處理之F函數；及與對F函數之輸入或輸出之其他列資料之互斥或運算。

(3)如上述(1)或(2)描述之密碼處理裝置，其中上述密碼處理部係藉由滿足下述(1)~(3)之分配條件之處理，將前段之回合運算之運算結果設定作為次段之回合運算之輸入。

(1)F函數輸入側資料序列係必然分配至下一回合函數之互斥或側資料序列，

(2)互斥或側資料序列係必然分配至下一回合函數之F函數輸入側資料序列，

(3)分割為各d/2個之資料序列係不重複分別分配至d/2處之下一回合函數之資料序列。

(4)如上述(1)~(3)之任一項所描述之密碼處理裝置，其中上述密碼處理部係具有輸入資料之分割數d為4以上之一般性Feistel結構。

(5)如上述(1)~(4)之任一項所描述之密碼處理裝置，其中上述密碼處理部係執行如下處理：將具有回合運算之輸出資料之d個各n/d位元之資料再分割成d/2個，生成d×(n/d)個再分割資料，並從分割數d所對應之d條之列之不同列中選出d/2個再分割資料進行再組合，再構成與前段之回合運算之輸出資料不同之d個n/d位元資料，設定作為次段之回合運算之輸入資料。

(6)如上述(1)~(5)之任一項所描述之密碼處理裝置，其中上述密碼處理部之全輸出位元成滿足下述2個條件之擴散(diffusion)狀態，即，在輸出位元作為輸入位元之關係式描述之情形下，實現滿足下述2個條件之全擴散(full diffusion)狀態之構成。

(條件1)全輸入位元包含於關係式

(條件2)全輸入位元至少通過一次上述回合函數。

(7)如上述(1)~(6)之任一項所描述之密碼處理裝置，其中上述密碼處理部係藉由4回合之回合運算來實現上述全擴散(full diffusion)狀態。

(8)如上述(1)~(7)之任一項所描述之密碼處理裝置，其中決定上述密碼處理部前段之回合運算之輸出資料、與次段之回合運算之再分割資料之輸入輸出關係之連接構成，係自將藉由具有回合運算輸出資料之列之n/d位元資料之再分割處理所產生之d×(n/d)個再分割資料組合而成之資料，即(d/2)個2n/d位元資料集作為單位之連接構成中選擇之連接構成。

(9)如上述(1)~(8)之任一項所描述之密碼處理裝置，其中上述密碼處理部係具有可應用於加密處理與解密處理兩者之對合性。

(10)如上述(1)~(9)之任一項所描述之密碼處理裝置，其中上述密碼處理部之各回合運算之再分割資料之再構成處理，係根據預先決定之規則，將前段之回合函數輸入側序列之再分割資料分配至次段之互斥或側序列，且根據預先決定之規則，將前段之互斥或側序列之再分割資料分配至次段之回合函數輸入側序列之構成。

(11)如上述(1)~(10)之任一項所描述之密碼處理裝置，其中上述密碼處理部係執行將作為輸入資料之明文轉換為密文之加密處理，或將作為輸入資料之密文轉換為明文之解密處理。

再者，在上述裝置及系統中執行處理之方法、或執行處理之程式亦包含於本揭示之構成。

此外，說明書中所說明之一連串處理可藉由硬體、軟體或兩者之複合構成來執行。藉由軟體來執行處理之情形，

可將記錄處理順列之程式安裝於被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通用電腦來執行。例如，程式可預先記錄於記錄媒體。除了可自記錄媒體安裝於電腦以外，亦可經由稱為LAN(Local Area Network，區域網路)、網際網路等之網絡傳送至電腦，並安裝於內建之硬碟等記錄媒體。

此外，說明書所記載之各種處理係不僅可按記述內容依時間序列來執行，亦可根據應執行處理之裝置之處理能力或需要，同時或個別地執行。又，本說明書中之系統係指複數裝置之邏輯性集合構成，各構成之裝置不限於在同一殼體內。

[產業上之可利用性]

如上所述，根據本揭示之一實施例之結構，可實現擴散(diffusion)特性提高且安全性高之密碼處理。

具體而言，其係具有密碼處理部，將作為資料處理對象之資料之構成位元分割成複數列而輸入、且對各列之資料重複執行應用回合函數之資料轉換處理，在密碼處理部中，將以分割數d分割輸入資料之n位元資料之n/d位元資料輸入各列，且將包含應用回合函數之資料轉換處理之運算作為回合運算而重複執行。並執行如下處理：將具有回合運算之輸出資料之列之n/d位元資料分割成d/2個，使該分割資料組合，再構成與前段之回合運算之輸出資料不同之d個n/d位元資料，設定作為次段之回合運算之輸入資料。藉由該構成而實現擴散(diffusion)特性提高且安全性

高之密碼處理。

【圖式簡單說明】

圖1係說明對應k位元之金鑰長之n位元共用金鑰區塊密碼演算法之圖。

圖2係說明與對應圖1所示之k位元之金鑰長之n位元共用金鑰區塊密碼演算法對應之解密演算法之圖。

圖3係說明金鑰排程部與資料加密部之關係之圖。

圖4係說明資料加密部之構成例之圖。

圖5係說明SPN結構之回合函數之例之圖。

圖6係說明Feistel結構之回合函數之一例之圖。

圖7係說明擴張Feistel結構之一例之圖。

圖8係說明擴張Feistel結構之一例之圖。

圖9係說明非線性轉換部之構成例之圖。

圖10係說明線性轉換處理部之構成例之圖。

圖11係說明具有Feistel結構之區塊密碼之擴散(diffusion)狀態之圖。

圖12係說明具有Feistel結構之區塊密碼之擴散(diffusion)狀態之圖。

圖13係說明具有在4-列中於1段使用2個F函數之一般性Feistel結構之區塊密碼之擴散(diffusion)狀態之圖。

圖14係說明具有在4-列中於1段使用2個F函數之一般性Feistel結構之區塊密碼之擴散(diffusion)狀態之圖。

圖15係說明具有在4-列中於1段使用2個F函數之一般性Feistel結構之區塊密碼之擴散(diffusion)狀態之圖。

圖16係說明d=6之情形下通常之一般性Feistel結構之圖。

圖17係顯示成為d=6之情形下通常之一般性Feistel結構之全擴散(full diffusion)狀態之路徑的一例之圖。

圖18係說明藉由變更回合間配線，在分割數d為6以上之情形，比先前之構成減少全擴散(full diffusion)回合數之構成例之圖。

圖19係顯示藉由變更回合間配線，在分割數d為6以上之情形，在比先前之構成減少全擴散(full diffusion)回合數之構成中成為全擴散(full diffusion)狀態之路徑的一例之圖。

圖20係說明作為本揭示之一實施例之密碼處理構成之圖。

圖21係說明本揭示之一實施例之d=4情形之例之圖。

圖22係顯示在d=4之情形之本方式中，成為全擴散(full diffusion)狀態之路徑之一例圖。

圖23係說明本揭示之一實施例之d=6之情形之例之圖。

圖24係顯示以d=6之情形之本方式成為全擴散(full diffusion)狀態之路徑之一例圖。

圖25係顯示d=6之情形下將各n/d位元資料2分割之構成例之圖。

圖26係顯示n位元輸入資料之分割數d、及各n/d位元資料之分割數p中各全擴散(full diffusion)回合數之關係之一部分之圖。

圖27係顯示F函數輸入側資料序列與互斥或側資料序列分別進行不同分割之構成例之圖。

圖28係顯示變更圖21記述之構成例之擴張金鑰插入位置之構成例之圖。

圖29係說明資料分配法更有效率之技術之圖。

圖30係說明資料分配法更有效率之技術之圖。

圖31係說明資料分配法更有效率之技術之圖。

圖32係說明Feistel機構之對合性之圖。

圖33係說明Feistel機構之對合性之圖。

圖34係顯示取得高擴散(diffusion)特性之4-列結構之一方式之圖。

圖35係說明實現對合性之處理之圖。

圖36係說明4-列(d=4)之構成中具有對合性之構成之一例之圖。

圖37係說明6-列(d=6)之構成中具有對合性之構成之一例之圖。

圖38係說明具有對合性之構成之一例之圖。

圖39係說明具有對合性之構成之一例之圖。

圖40係顯示作為密碼處理裝置之IC模組700之構成例之圖。

【主要元件符號說明】

700	IC模組
701	CPU(Central processing Unit)
702	記憶體

703 密碼處理部

704 亂數產生部

705 收發部

七、申請專利範圍：

1. 一種密碼處理裝置，其包含密碼處理部，該密碼處理部係將作為資料處理對象之資料之構成位元分割成複數列並輸入，且對各列之資料重複執行應用回合函數之資料轉換處理；

上述密碼處理部係將以分割數d分割輸入資料即n位元資料之n/d位元資料輸入上述各列，且將包含應用上述回合函數之資料轉換處理之運算作為回合運算而重複執行之構成，且

執行如下處理：將具有回合運算之輸出資料之列之n/d位元資料再分割成d/2個，將該再分割資料再度組合，再構成與前段之回合運算之輸出資料不同之d個n/d位元資料，而設定作為次段之回合運算之輸入資料。

2. 如請求項1之密碼處理裝置，其中上述回合函數包含：應用回合金鑰之運算；非線性轉換處理；包含線性轉換處理之F函數；及與對F函數之輸入或輸出之其他列資料之互斥或運算。

3. 如請求項2之密碼處理裝置，其中上述密碼處理部係藉由滿足下述(1)~(3)之分配條件之處理，將前段之回合運算之運算結果設定作為次段之回合運算之輸入：

(1)F函數輸入側資料序列必然分配至下一回合函數之互斥或側資料序列；

(2)互斥或側資料序列必然分配至下一回合函數之F函數輸入側資料序列；

(3)分割為各d/2個之資料序列不重複地分別分配至d/2處之下一回合函數之資料序列。

4. 如請求項1之密碼處理裝置，其中上述密碼處理部具有輸入資料之分割數d為4以上之一般性Feistel結構。

5. 如請求項1之密碼處理裝置，其中上述密碼處理部係執行如下處理：將具有回合運算之輸出資料之d個列之各n/d位元資料再分割成d/2個，生成d×(n/d)個再分割資料，並從對應分割數d之d條之列之不同列中選出之d/2個再分割資料進行再組合，再構成與前段之回合運算之輸出資料不同之d個n/d位元資料，而設定作為次段之回合運算之輸入資料。

6. 如請求項1之密碼處理裝置，其中上述密碼處理部當其全輸出位元成滿足下述2個條件之擴散(diffusion)狀態，即，在將輸出位元描述為輸入位元之關係式之情形下，係實現滿足下述2個條件之全擴散(full diffusion)狀態之構成：

(條件1)全輸入位元包含於關係式；

(條件2)全輸入位元至少通過一次上述回合函數。

7. 如請求項6之密碼處理裝置，其中上述密碼處理部係藉由4回合之回合運算而實現上述全擴散(full diffusion)狀態。

8. 如請求項1之密碼處理裝置，其中決定上述密碼處理部之前段之回合運算之輸出資料、與次段之回合運算之再分割資料之輸入輸出關係之連接構成，係自將藉由具有

回合運算輸出資料之列之n/d位元資料之再分割處理所產生之d×(n/d)個再分割資料組合而成之資料、即(d/2)個2n/d位元資料集作為單位之連接構成中選擇之連接構成。

9. 如請求項1之密碼處理裝置，其中上述密碼處理部具有可應用於加密處理與解密處理兩者之對合性。

10. 如請求項9之密碼處理裝置，其中上述密碼處理部之各回合運算之再分割資料之再構成處理係根據預先決定之規則，將前段之回合函數輸入側序列之再分割資料分配至次段之互斥或側序列，且

根據預先決定之規則，將前段之互斥或側序列之再分割資料分配至次段之回合函數輸入側序列之構成。

11. 如請求項1之密碼處理裝置，其中上述密碼處理部係執行將作為輸入資料之明文轉換為密文之加密處理，或將作為輸入資料之密文轉換為明文之解密處理。

12. 一種密碼處理方法，其係在密碼處理裝置中執行密碼處理者，且

由密碼處理部執行將作為資料處理對象之資料之構成位元分割成複數列並輸入、且對各列之資料重複執行應用回合函數之資料轉換處理之密碼處理步驟；

上述密碼處理步驟係將以分割數d分割輸入資料之n位元資料之n/d位元資料輸入上述各列，且將包含應用上述回合函數之資料轉換處理之運算作為回合運算而重複執行；且

執行如下處理：將具有回合運算之輸出資料之列之n/d位元資料再分割成d/2個，將該再分割資料再度組合，再構成與前段之回合運算之輸出資料不同之d個n/d位元資料，而設定作為次段之回合運算之輸入資料。

13. 一種程式，其係在密碼處理裝置中執行密碼處理者，且

使密碼處理部執行將作為資料處理對象之資料之構成位元分割成複數列並輸入、且對各列之資料重複執行應用回合函數之資料轉換處理之密碼處理步驟；

在上述密碼處理步驟中，將以分割數d分割輸入資料之n位元資料之n/d位元資料輸入上述各列，使包含應用上述回合函數之資料轉換處理之運算作為回合運算而重複執行；且

執行如下處理：將具有回合運算之輸出資料之列之n/d位元資料再分割成d/2個，將該再分割資料再度組合，再構成與前段之回合運算之輸出資料不同之d個n/d位元資料，而設定作為次段之回合運算之輸入資料。

八、圖式：

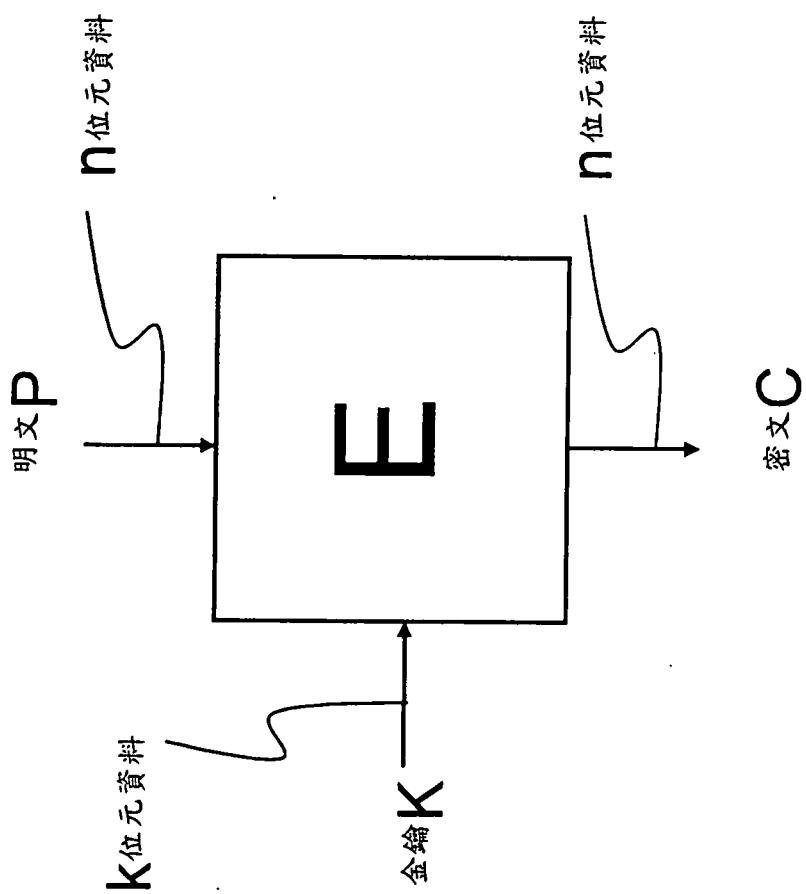

圖 1

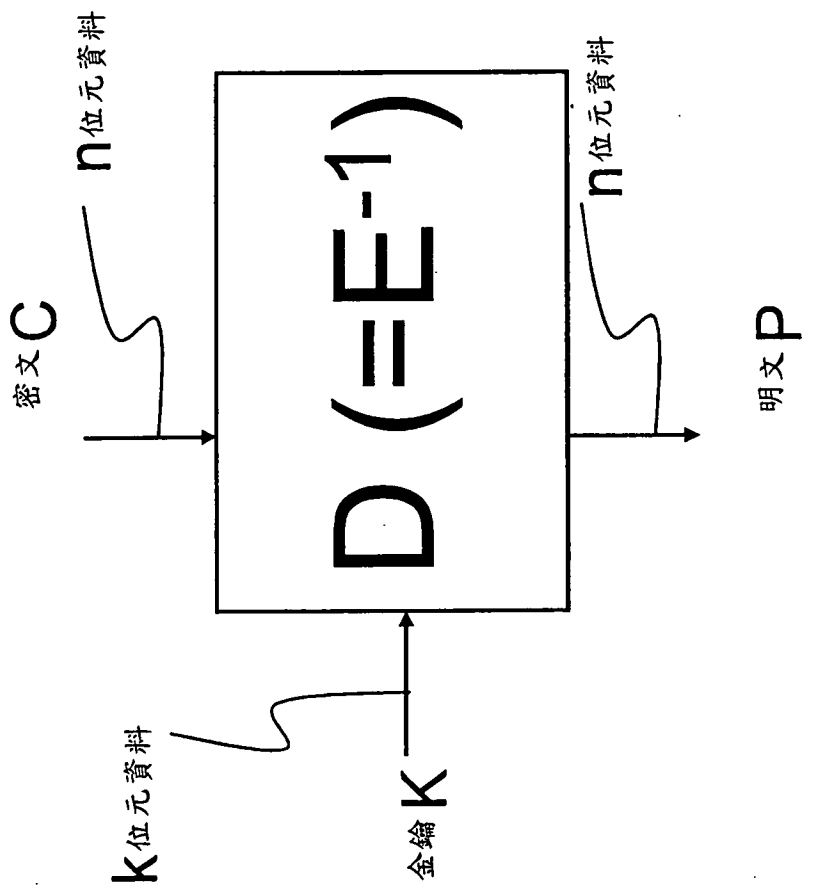

圖 2

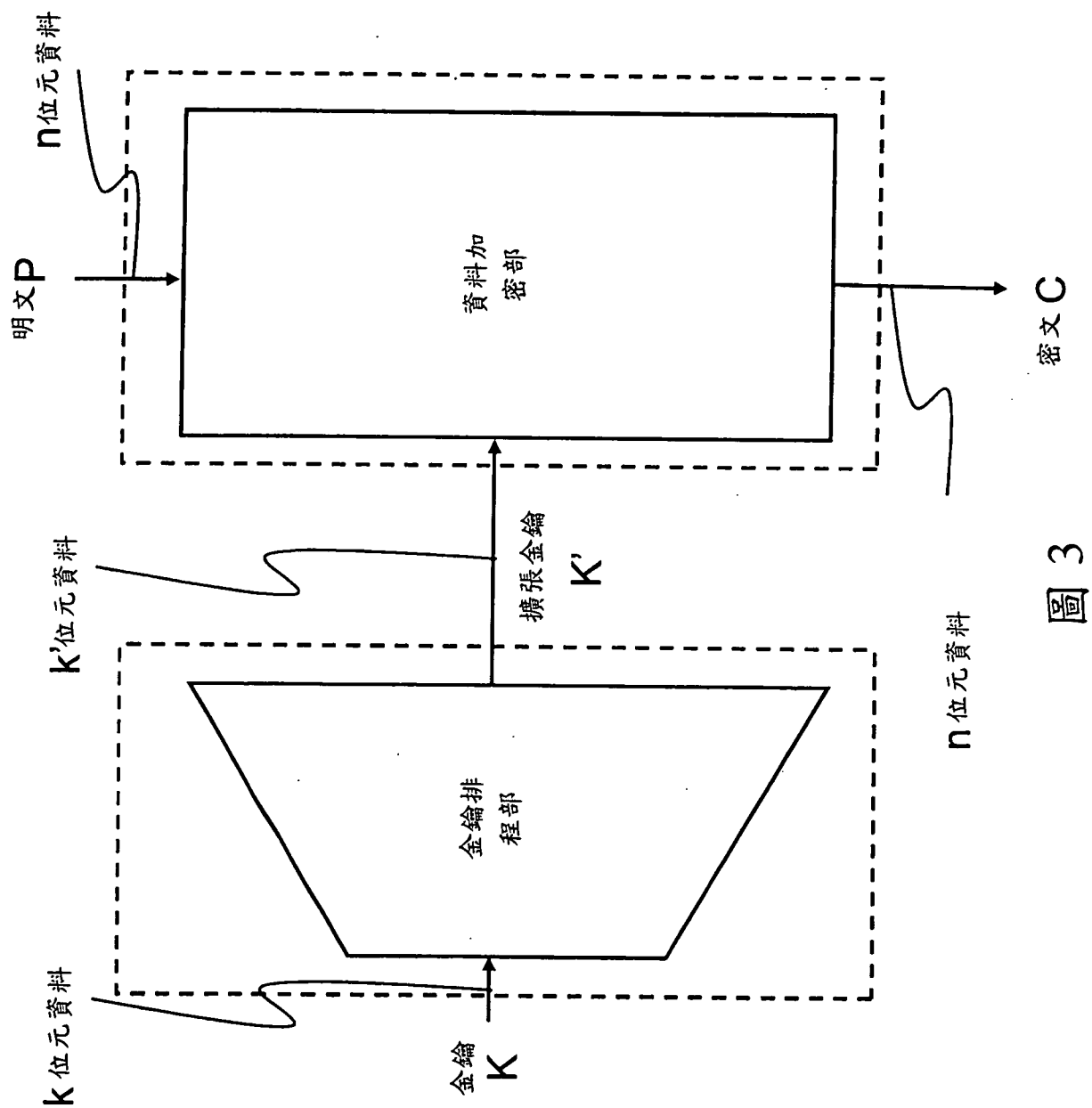

圖 3

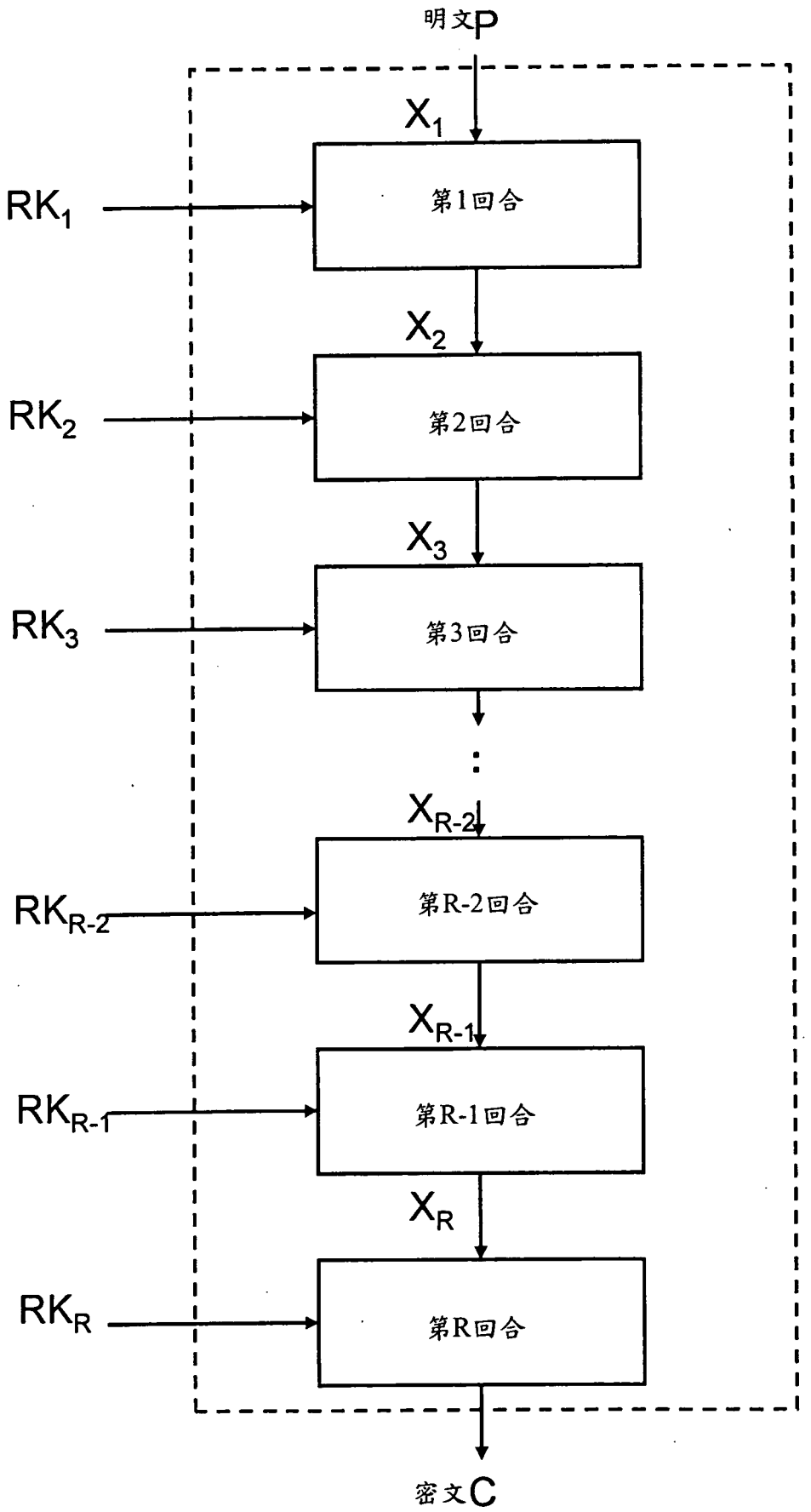
明文P
X1
第1回合
RK1
X2
第2回合
RK2
X3
第3回合
RK3
XR-2
第R-2回合
RKR-2
XR-1
第R-1回合
RKR-1
XR
第R回合
RKR
密文C

圖 4

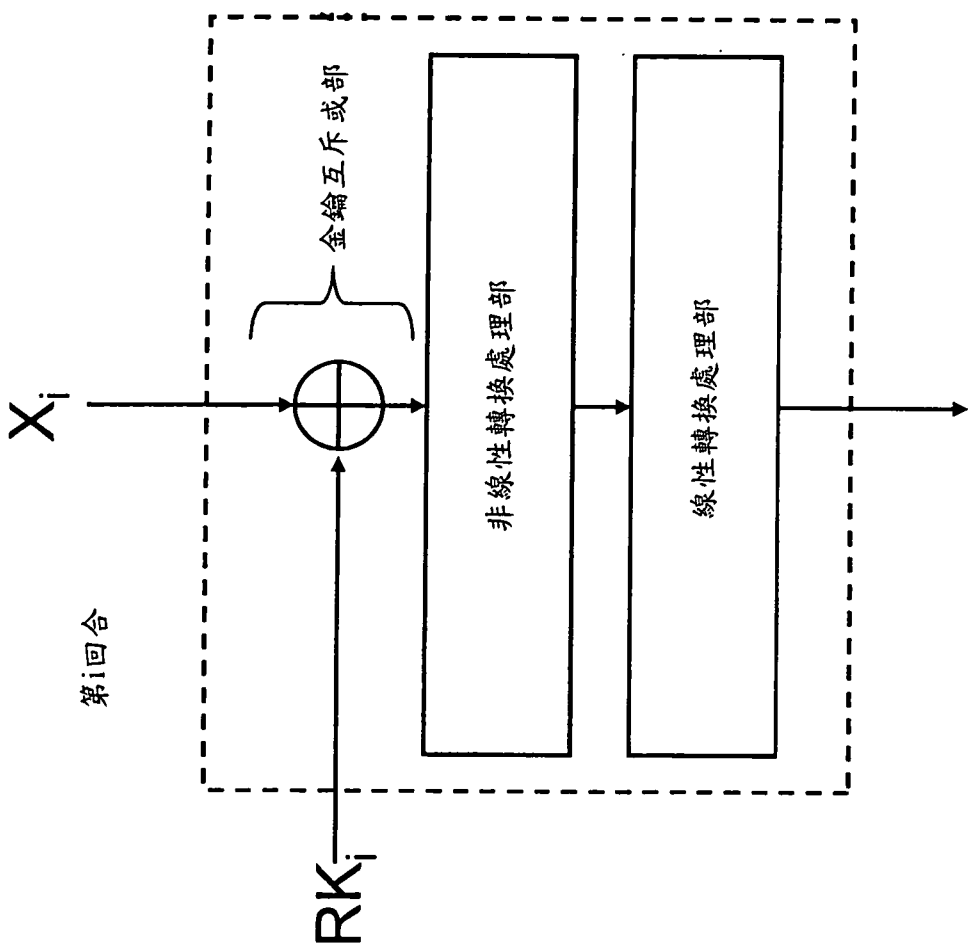

圖 5

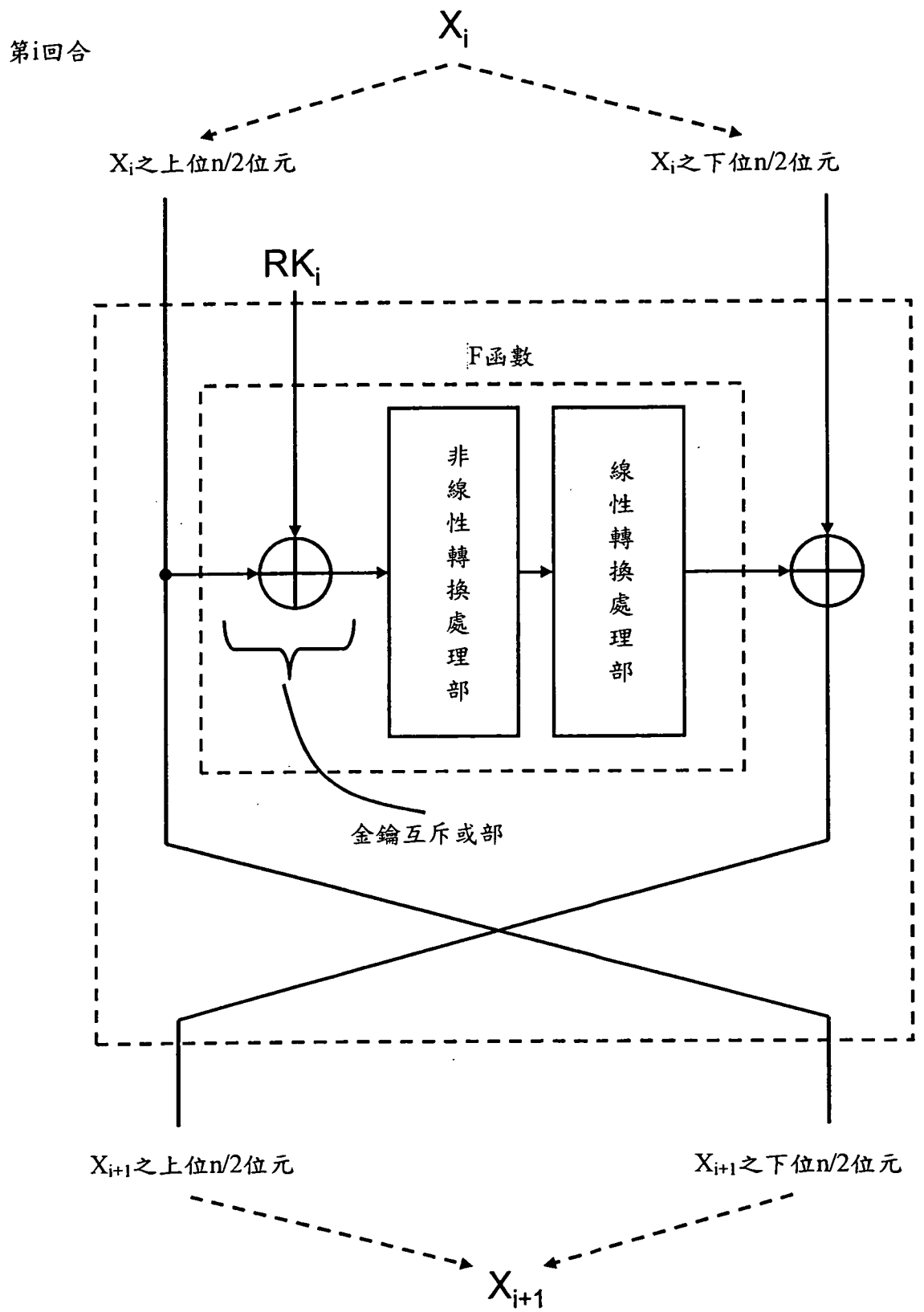
第i回合
X_i
X_i之上位n/2位元
X_i之下位n/2位元
RK_i
F函數
非線性轉換處理部
線性轉換處理部
金鑰互斥或部
X_{i+1}之上位n/2位元
X_{i+1}之下位n/2位元
X_{i+1}

圖 6

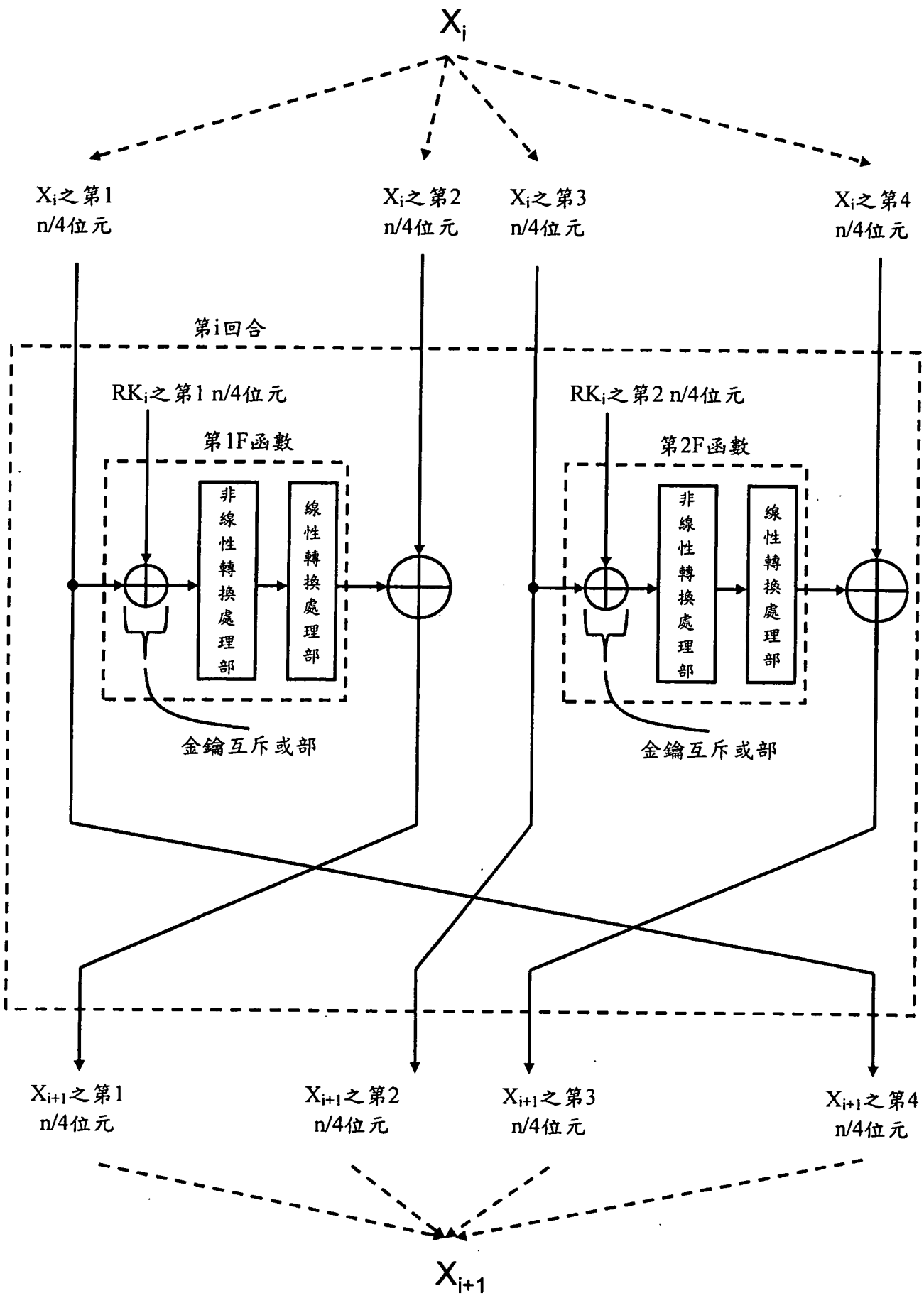
Xi
Xi之第1 n/4位元
Xi之第2 n/4位元
Xi之第3 n/4位元
Xi之第4 n/4位元
第i回合
RKi之第1 n/4位元
第1F函數
非線性轉換處理部
線性轉換處理部
金鑰互斥或部
RKi之第2 n/4位元
第2F函數
非線性轉換處理部
線性轉換處理部
金鑰互斥或部
Xi+1之第1 n/4位元
Xi+1之第2 n/4位元
Xi+1之第3 n/4位元
Xi+1之第4 n/4位元
Xi+1

圖 7

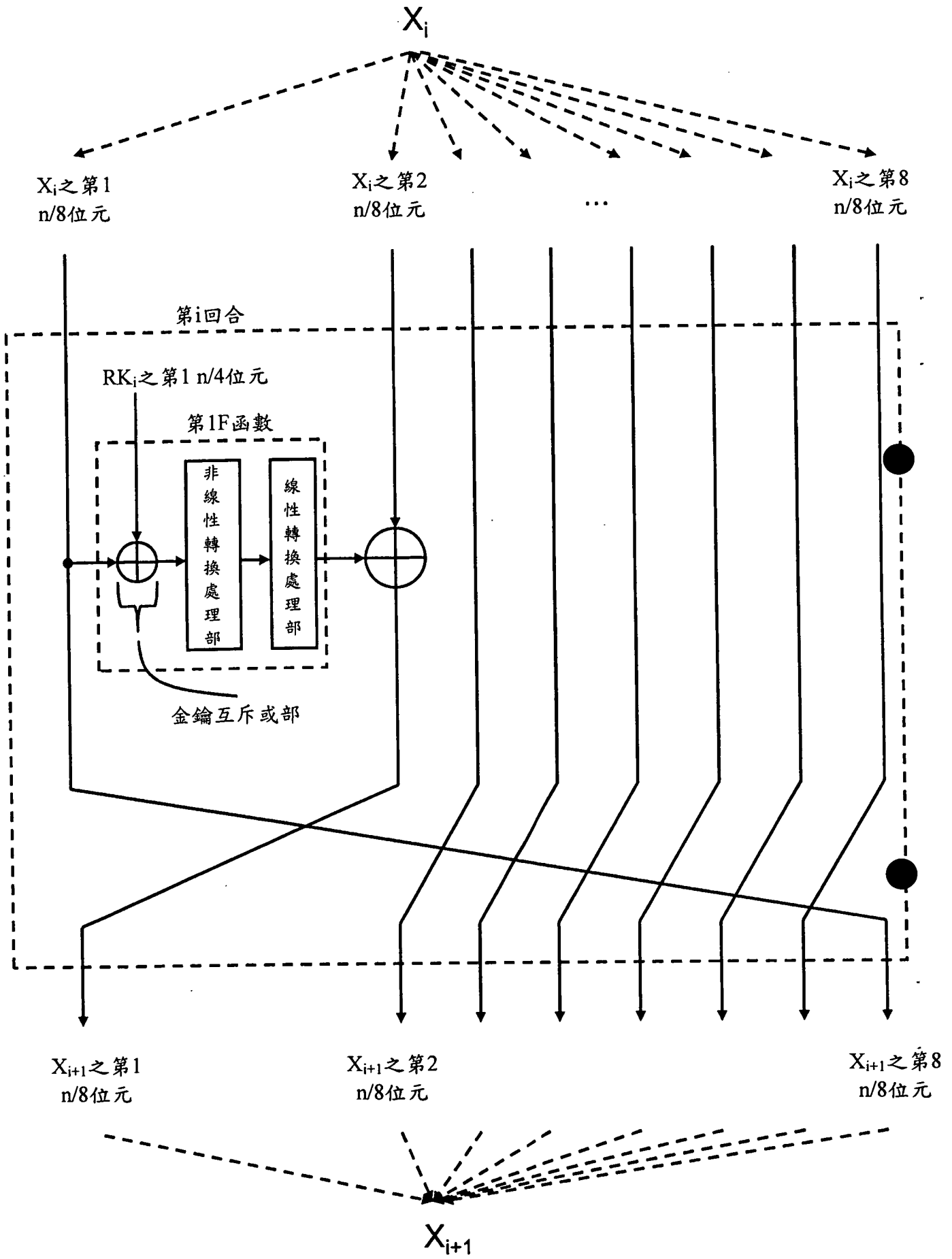
X_i
X_i之第1 n/8位元
X_i之第2 n/8位元
...
X_i之第8 n/8位元
第i回合
RK_i之第1 n/4位元
第1F函數
非線性轉換處理部
線性轉換處理部
金鑰互斥或部
X_{i+1}之第1 n/8位元
X_{i+1}之第2 n/8位元
X_{i+1}之第8 n/8位元
X_{i+1}

圖 8

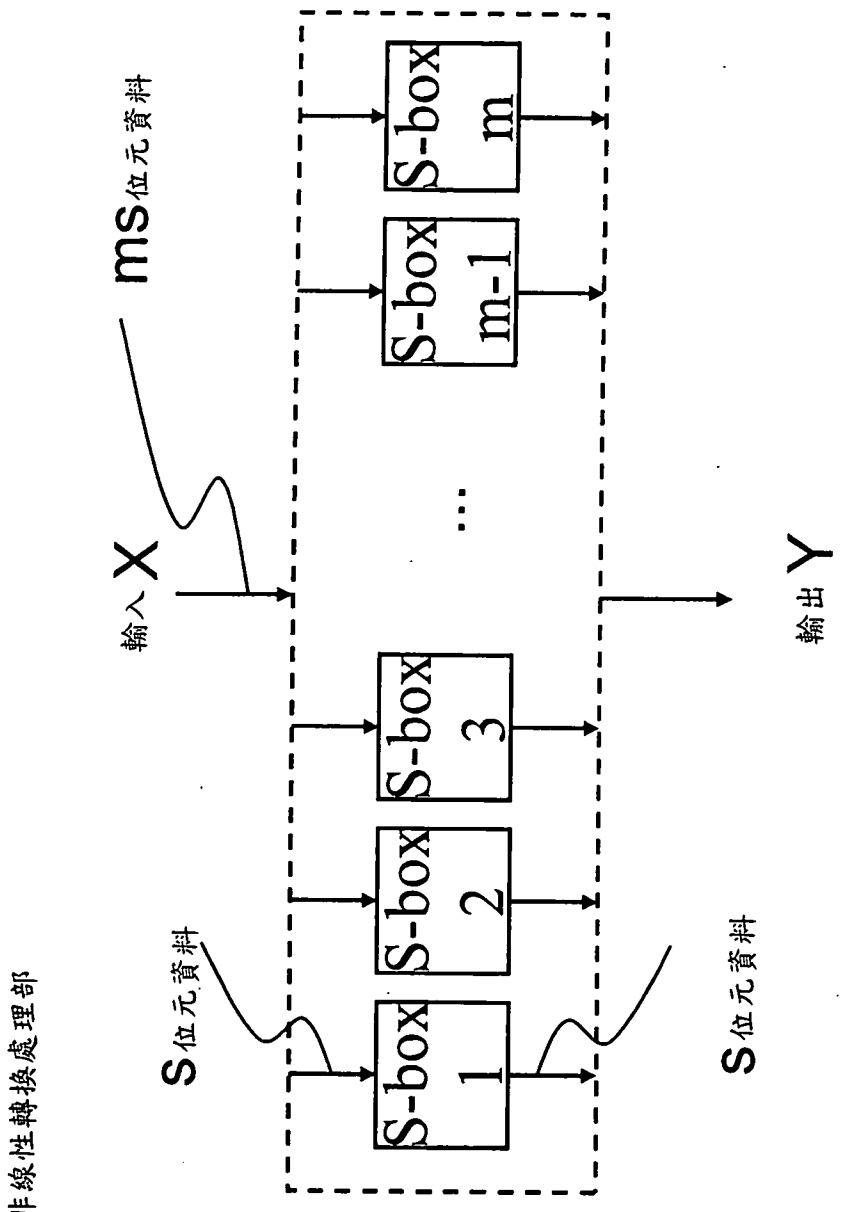
非線性轉換處理部
S位元資料
S-box 1
S-box 2
S-box 3
...
S-box m-1
S-box m
S位元資料
輸入 X
ms位元資料
輸出 Y

圖 9

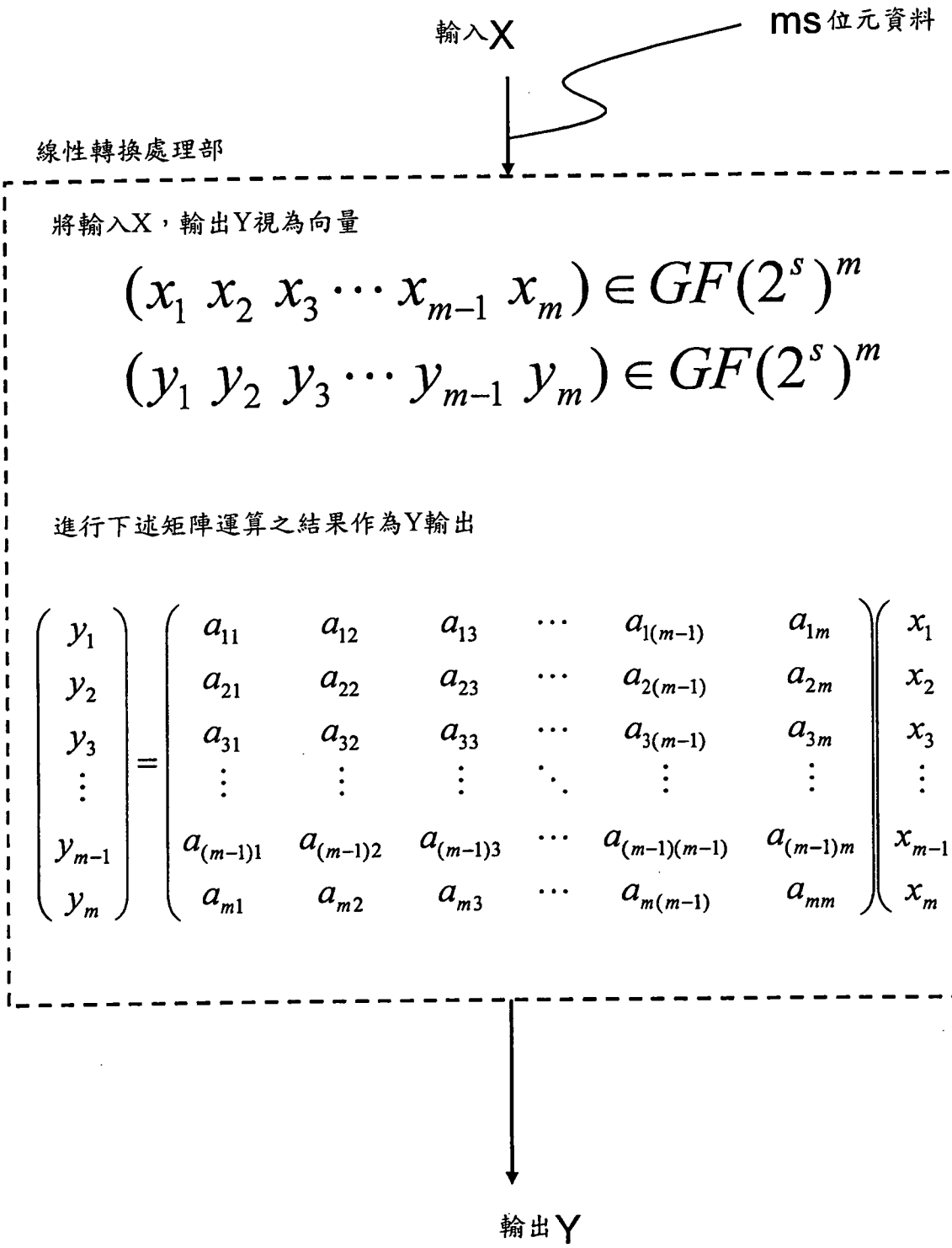
輸入X
ms位元資料
線性轉換處理部
將輸入X，輸出Y視為向量
$(x_1\ x_2\ x_3 \cdots x_{m-1}\ x_m) \in GF(2^s)^m$
$(y_1\ y_2\ y_3 \cdots y_{m-1}\ y_m) \in GF(2^s)^m$
進行下述矩陣運算之結果作為Y輸出
$\begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ \vdots \\ y_{m-1} \\ y_m \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1(m-1)} & a_{1m} \\ a_{21} & a_{22} & a_{23} & \cdots & a_{2(m-1)} & a_{2m} \\ a_{31} & a_{32} & a_{33} & \cdots & a_{3(m-1)} & a_{3m} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{(m-1)1} & a_{(m-1)2} & a_{(m-1)3} & \cdots & a_{(m-1)(m-1)} & a_{(m-1)m} \\ a_{m1} & a_{m2} & a_{m3} & \cdots & a_{m(m-1)} & a_{mm} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_{m-1} \\ x_m \end{pmatrix}$
輸出Y

圖 10

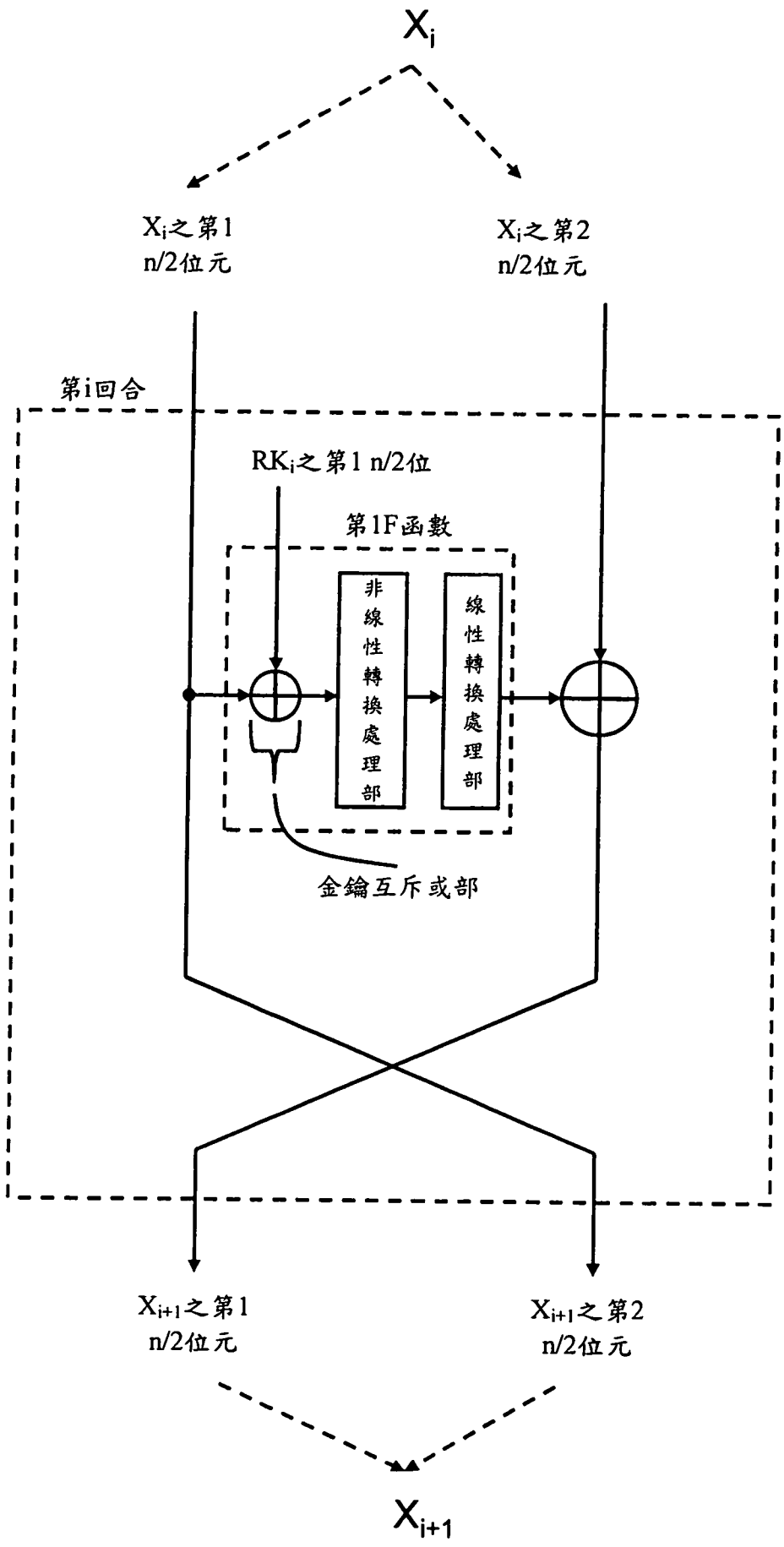
X_i
X_i之第1
n/2位元
X_i之第2
n/2位元
第i回合
RK_i之第1 n/2位
第1F函數
非線性轉換處理部
線性轉換處理部
金鑰互斥或部
X_{i+1}之第1
n/2位元
X_{i+1}之第2
n/2位元
X_{i+1}

圖 11

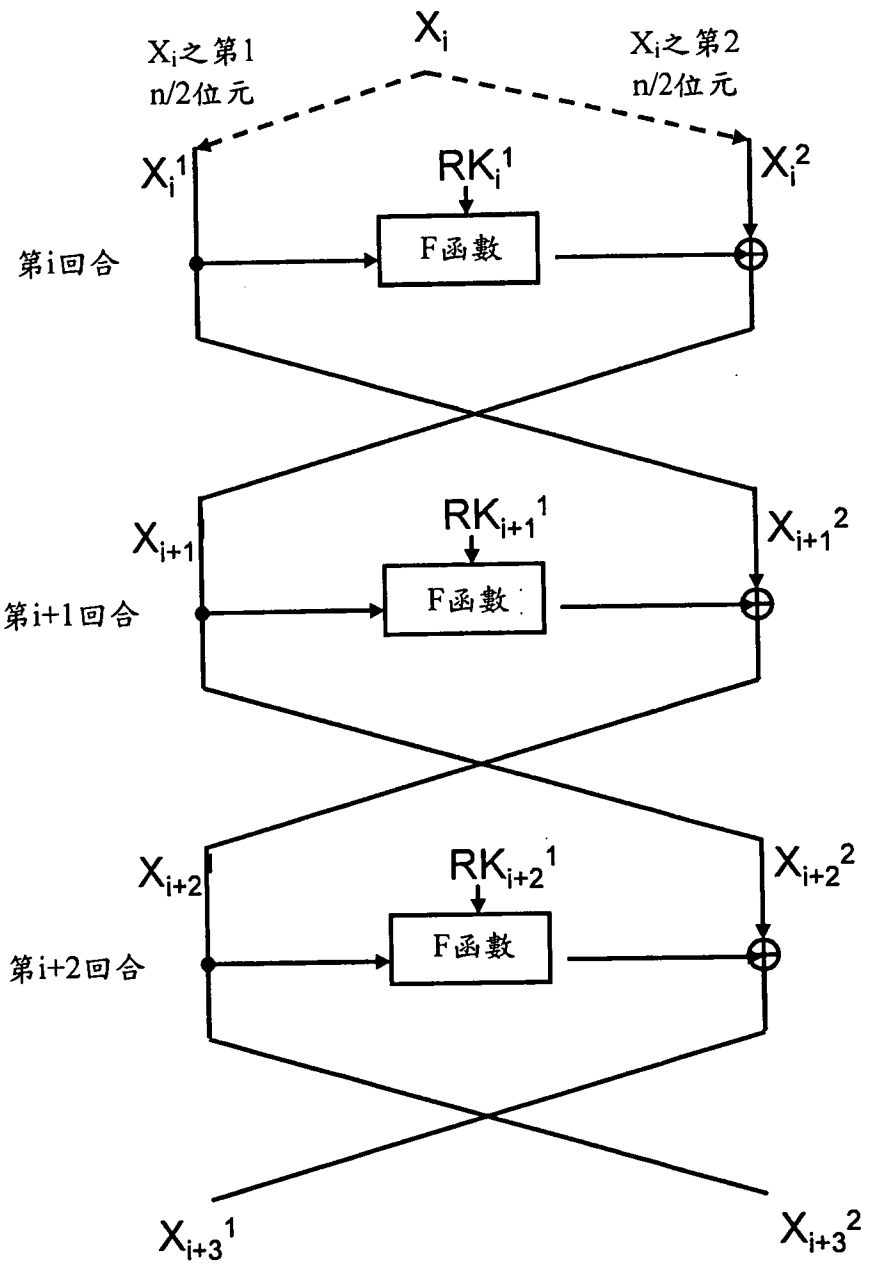
X_i
X_i之第1 n/2位元
X_i之第2 n/2位元
X_i^1
RK_i^1
X_i^2
F函數
第i回合
X_{i+1}
RK_{i+1}^1
X_{i+1}^2
F函數
第i+1回合
X_{i+2}
RK_{i+2}^1
X_{i+2}^2
F函數
第i+2回合
X_{i+3}^1
X_{i+3}^2

圖 12

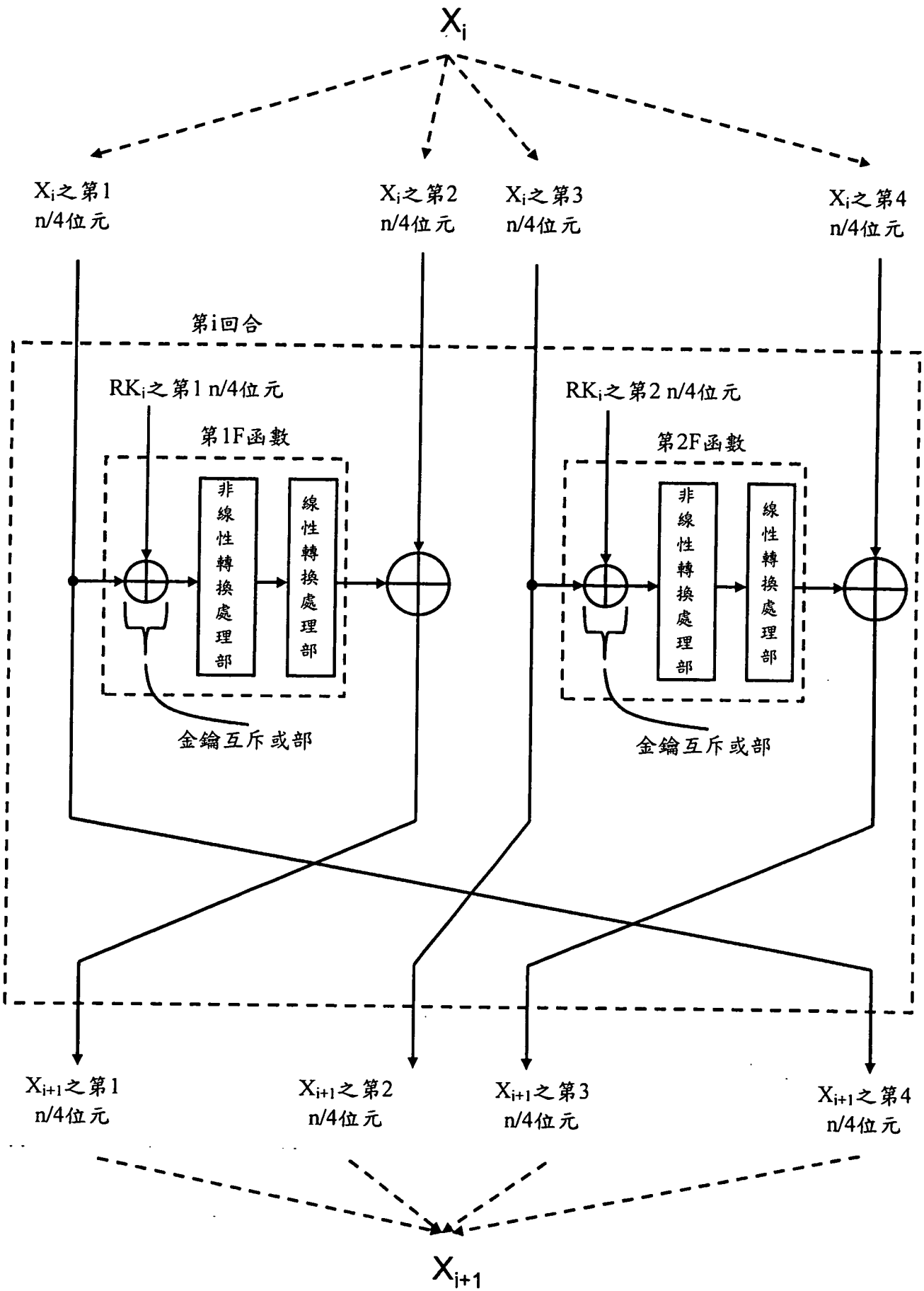
X_i
X_i之第1 n/4位元
X_i之第2 n/4位元
X_i之第3 n/4位元
X_i之第4 n/4位元
第i回合
RK_i之第1 n/4位元
第1F函數
非線性轉換處理部
線性轉換處理部
金鑰互斥或部
RK_i之第2 n/4位元
第2F函數
非線性轉換處理部
線性轉換處理部
金鑰互斥或部
X_{i+1}之第1 n/4位元
X_{i+1}之第2 n/4位元
X_{i+1}之第3 n/4位元
X_{i+1}之第4 n/4位元
X_{i+1}

圖 13

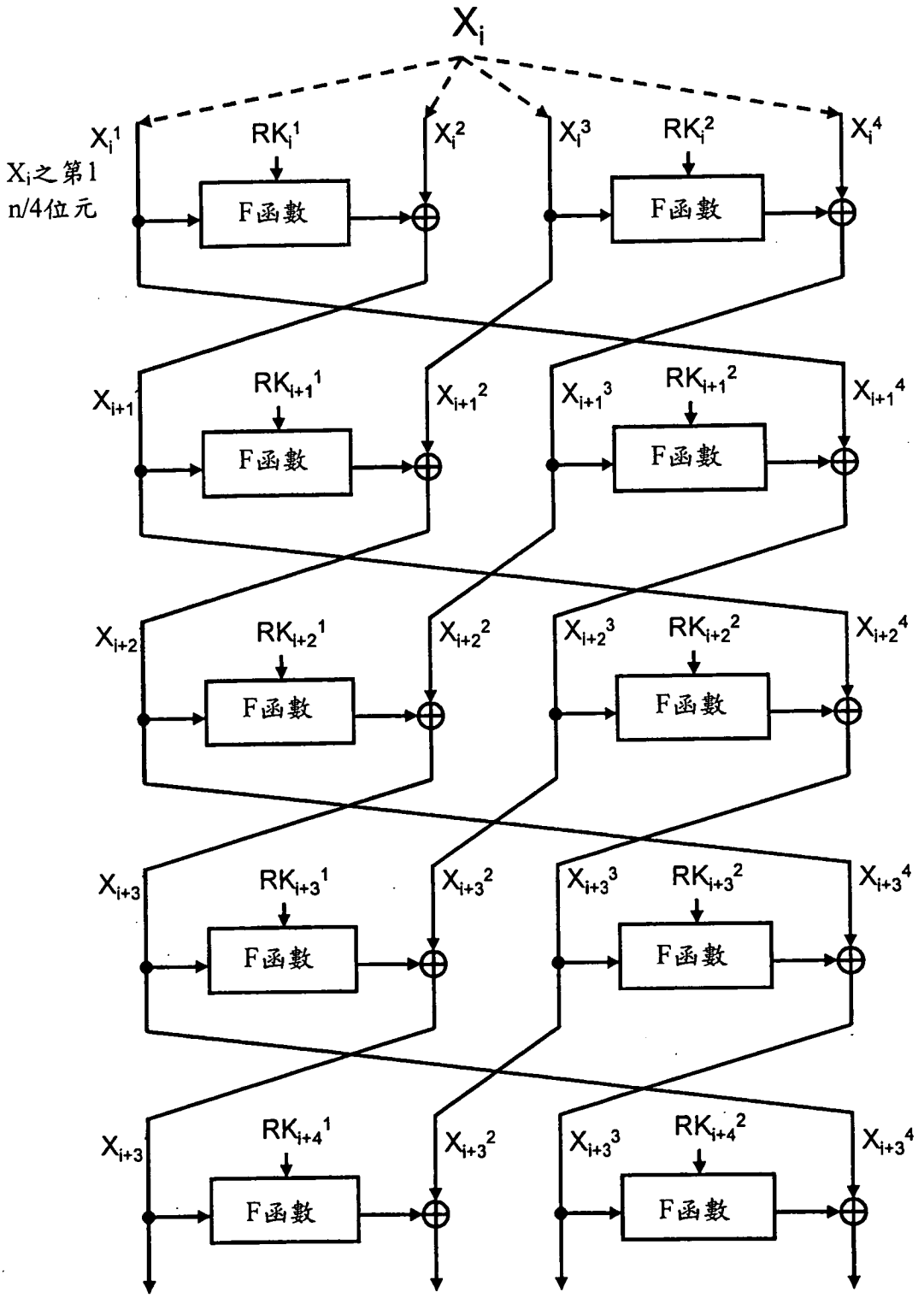
X_i
X_i^1
X_i之第1
n/4位元
RK_i^1
X_i^2
X_i^3
RK_i^2
X_i^4
F函數
X_{i+1}
RK_{i+1}^1
X_{i+1}^2
X_{i+1}^3
RK_{i+1}^2
X_{i+1}^4
X_{i+2}
RK_{i+2}^1
X_{i+2}^2
X_{i+2}^3
RK_{i+2}^2
X_{i+2}^4
X_{i+3}
RK_{i+3}^1
X_{i+3}^2
X_{i+3}^3
RK_{i+3}^2
X_{i+3}^4
X_{i+3}
RK_{i+4}^1
X_{i+3}^2
X_{i+3}^3
RK_{i+4}^2
X_{i+3}^4

圖 14

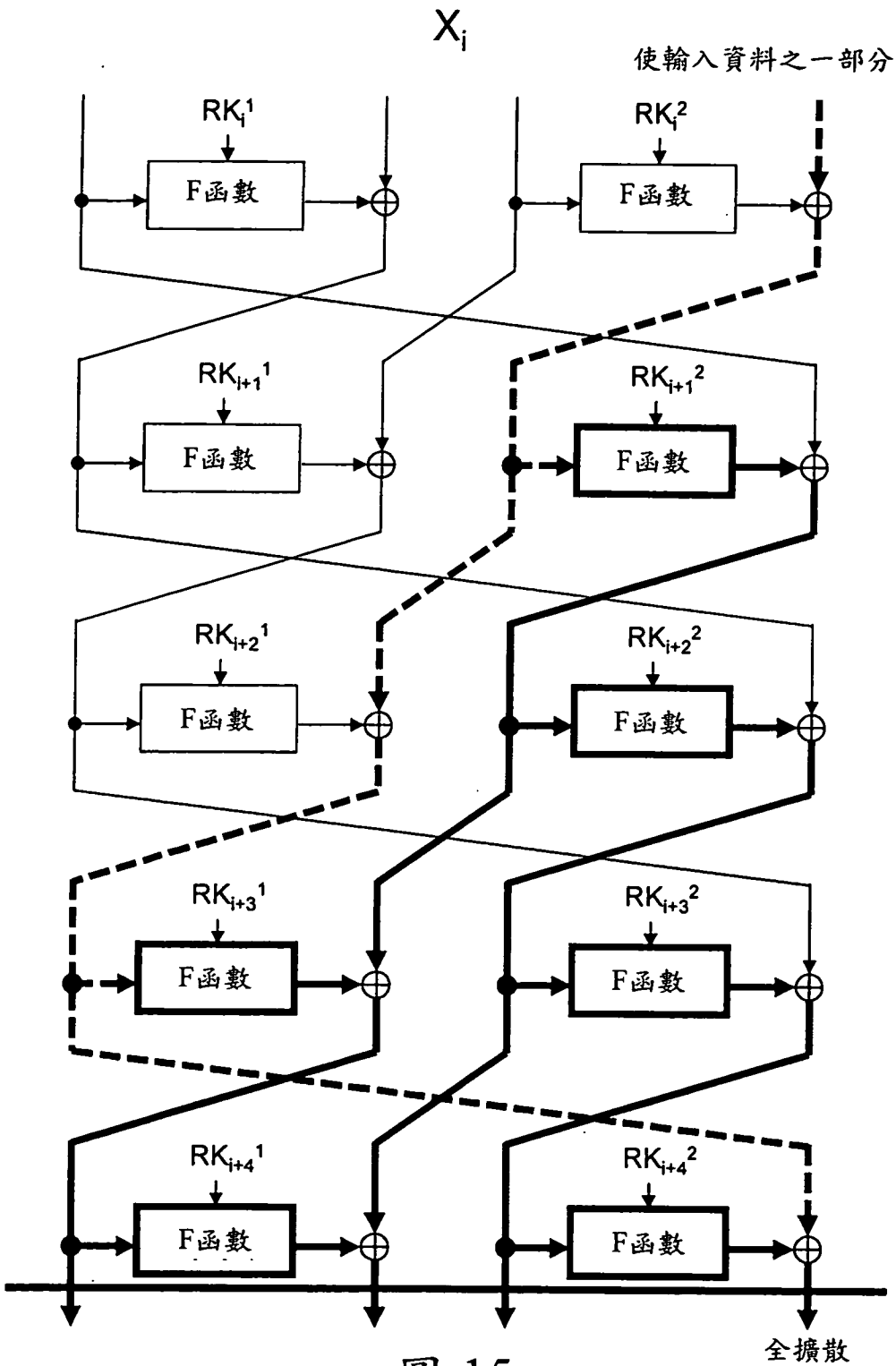
X_i
使輸入資料之一部分變化
RK_i^1
F函數
RK_i^2
F函數
RK_{i+1}^1
F函數
RK_{i+1}^2
F函數
RK_{i+2}^1
F函數
RK_{i+2}^2
F函數
RK_{i+3}^1
F函數
RK_{i+3}^2
F函數
RK_{i+4}^1
F函數
RK_{i+4}^2
F函數
全擴散

圖 15

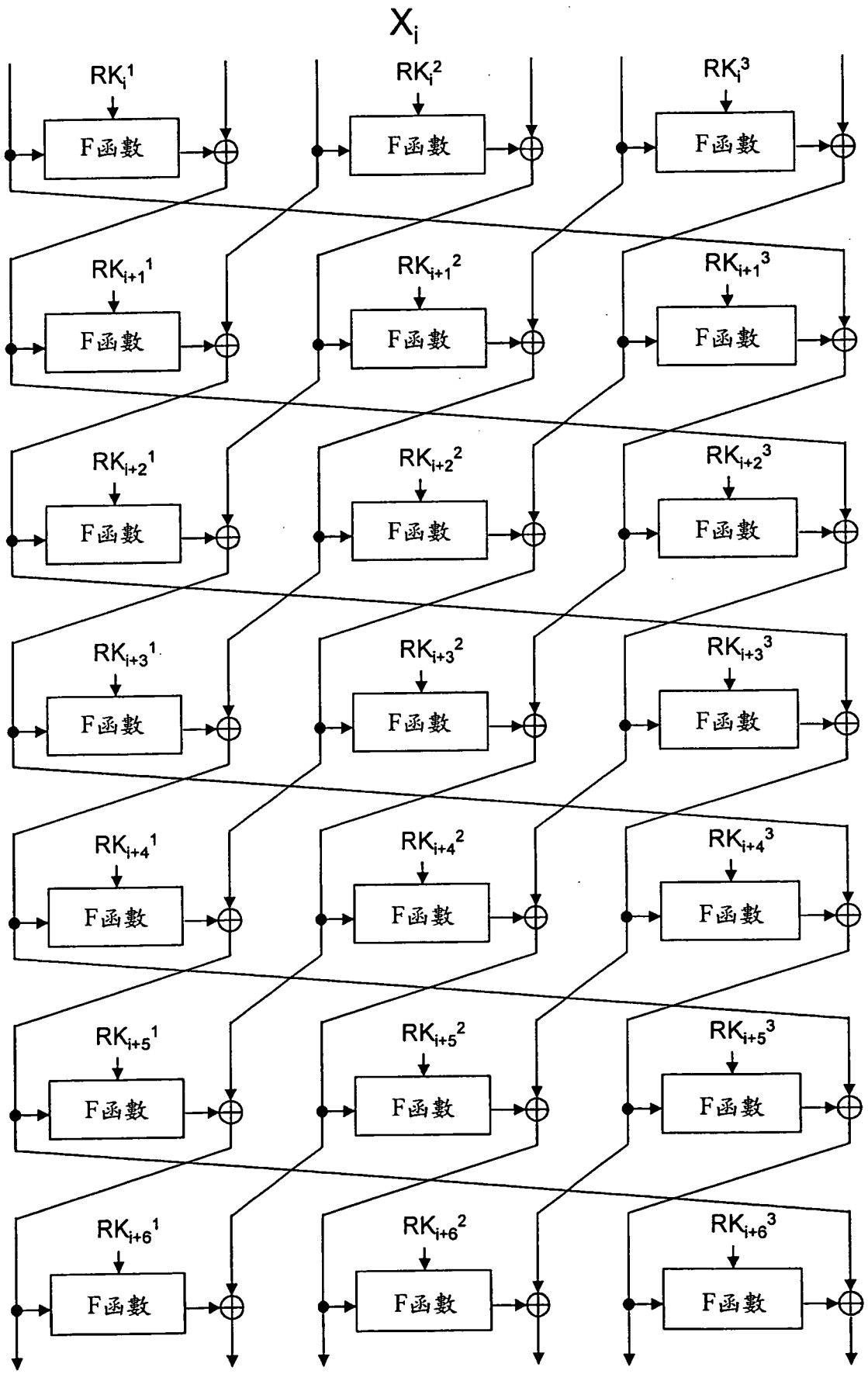
X_i
RK_i^1
RK_i^2
RK_i^3
RK_{i+1}^1
RK_{i+1}^2
RK_{i+1}^3
RK_{i+2}^1
RK_{i+2}^2
RK_{i+2}^3
RK_{i+3}^1
RK_{i+3}^2
RK_{i+3}^3
RK_{i+4}^1
RK_{i+4}^2
RK_{i+4}^3
RK_{i+5}^1
RK_{i+5}^2
RK_{i+5}^3
RK_{i+6}^1
RK_{i+6}^2
RK_{i+6}^3
F函數

圖 16

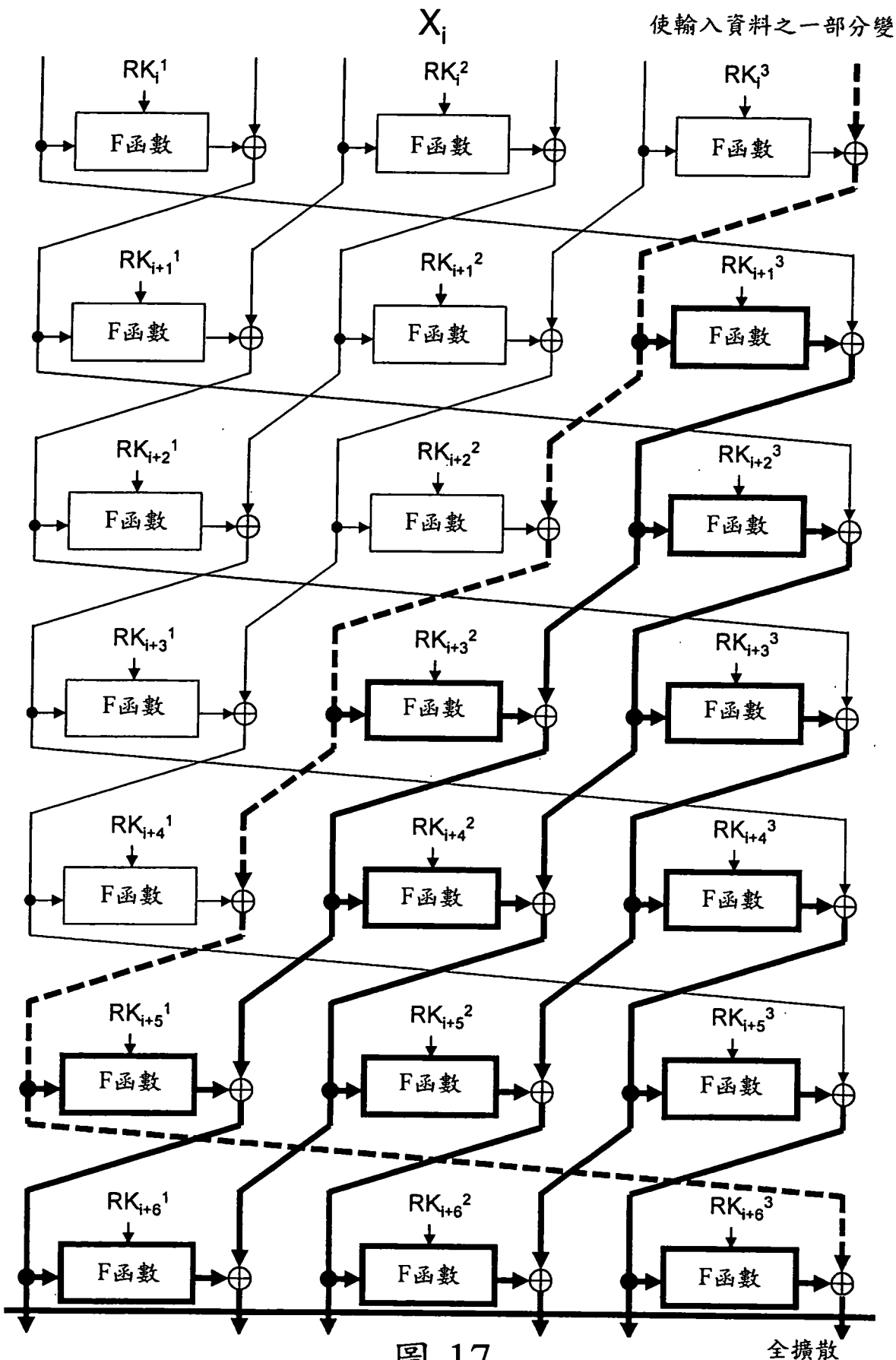
X_i
使輸入資料之一部分變化
RK_i^1
RK_i^2
RK_i^3
RK_{i+1}^1
RK_{i+1}^2
RK_{i+1}^3
RK_{i+2}^1
RK_{i+2}^2
RK_{i+2}^3
RK_{i+3}^1
RK_{i+3}^2
RK_{i+3}^3
RK_{i+4}^1
RK_{i+4}^2
RK_{i+4}^3
RK_{i+5}^1
RK_{i+5}^2
RK_{i+5}^3
RK_{i+6}^1
RK_{i+6}^2
RK_{i+6}^3
F函數
全擴散

圖 17

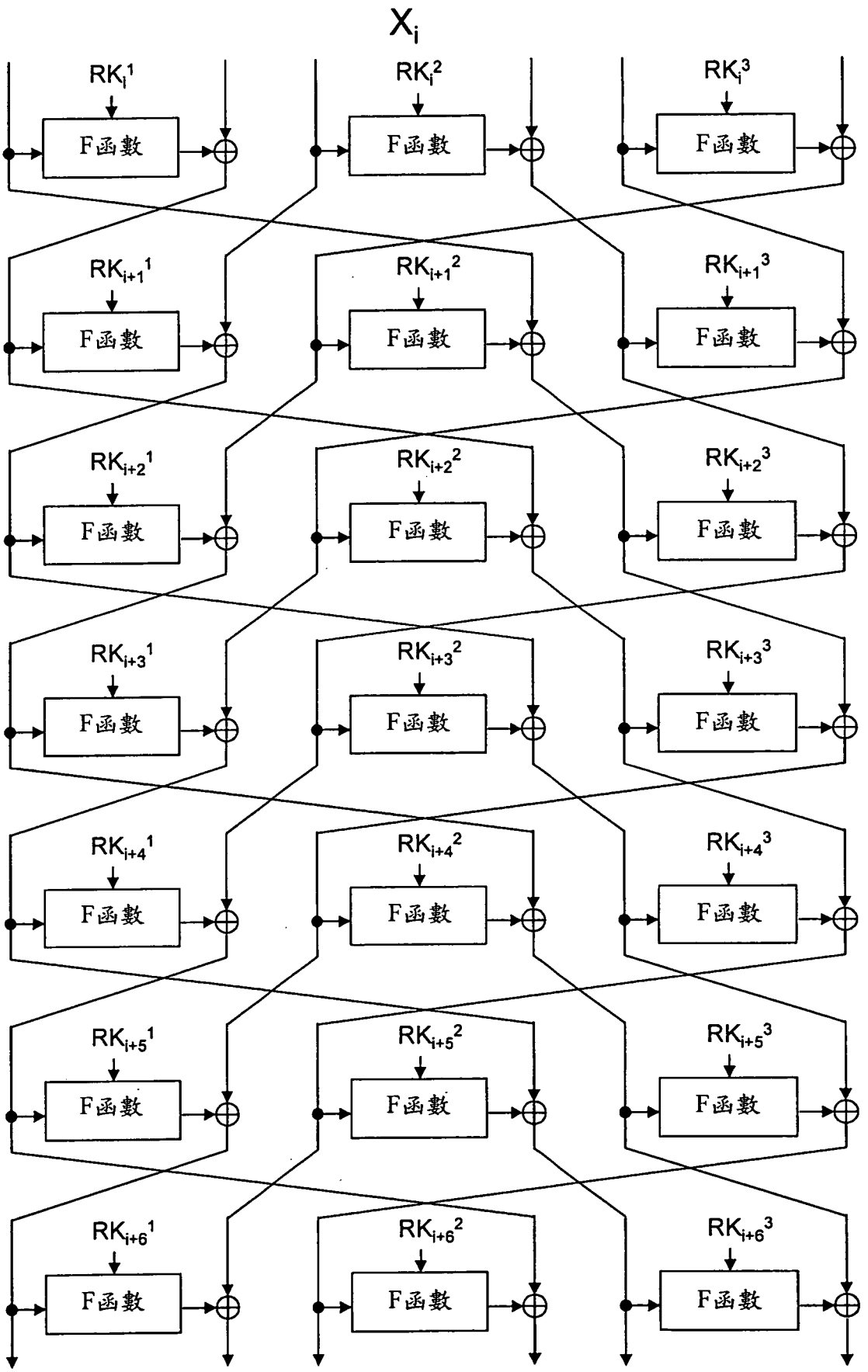
X_i
RK_i^1
RK_i^2
RK_i^3
RK_{i+1}^1
RK_{i+1}^2
RK_{i+1}^3
RK_{i+2}^1
RK_{i+2}^2
RK_{i+2}^3
RK_{i+3}^1
RK_{i+3}^2
RK_{i+3}^3
RK_{i+4}^1
RK_{i+4}^2
RK_{i+4}^3
RK_{i+5}^1
RK_{i+5}^2
RK_{i+5}^3
RK_{i+6}^1
RK_{i+6}^2
RK_{i+6}^3
F函數

圖 18

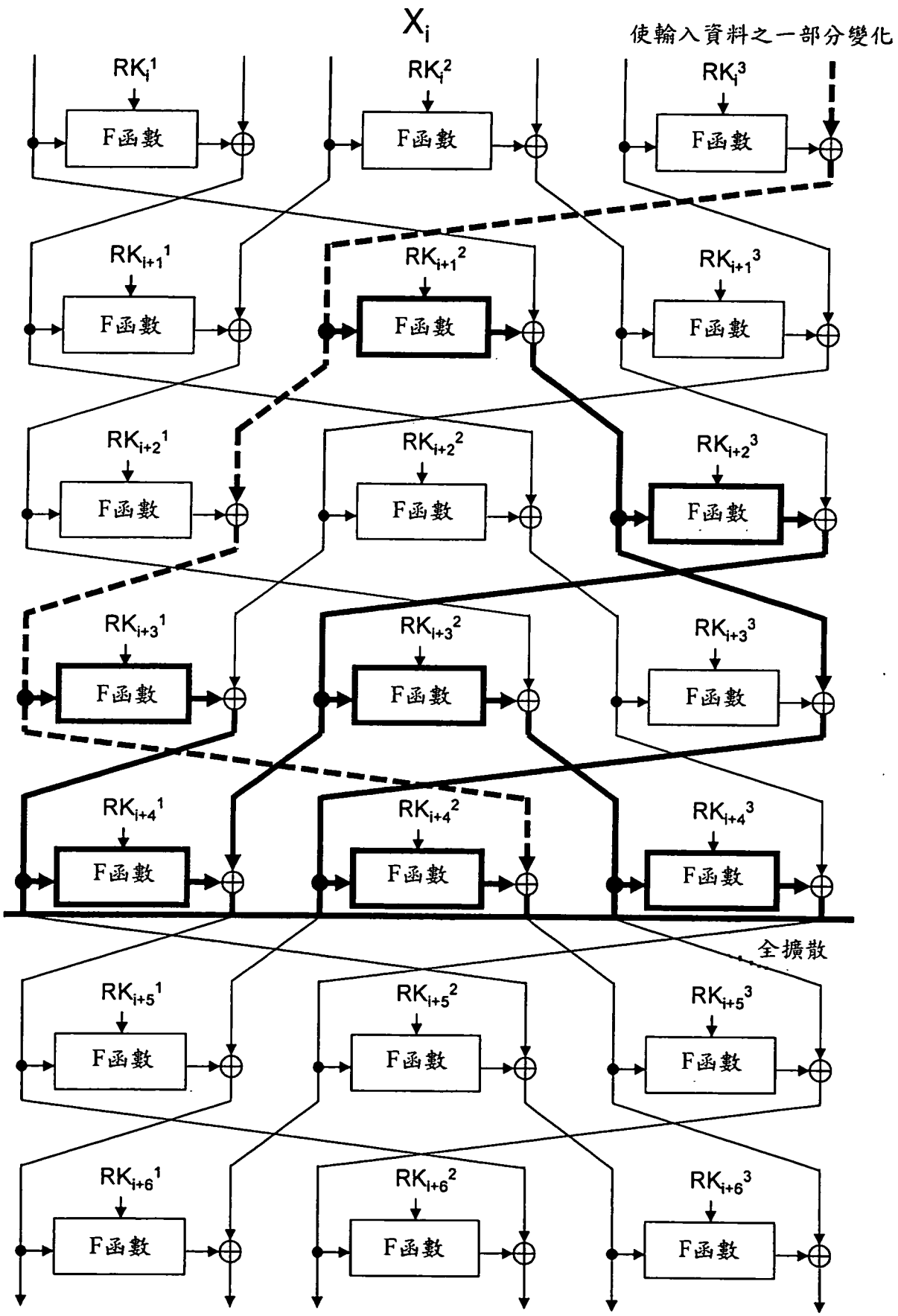
X_i
使輸入資料之一部分變化
RK_i^1
RK_i^2
RK_i^3
RK_{i+1}^1
RK_{i+1}^2
RK_{i+1}^3
RK_{i+2}^1
RK_{i+2}^2
RK_{i+2}^3
RK_{i+3}^1
RK_{i+3}^2
RK_{i+3}^3
RK_{i+4}^1
RK_{i+4}^2
RK_{i+4}^3
全擴散
RK_{i+5}^1
RK_{i+5}^2
RK_{i+5}^3
RK_{i+6}^1
RK_{i+6}^2
RK_{i+6}^3
F函數

圖 19

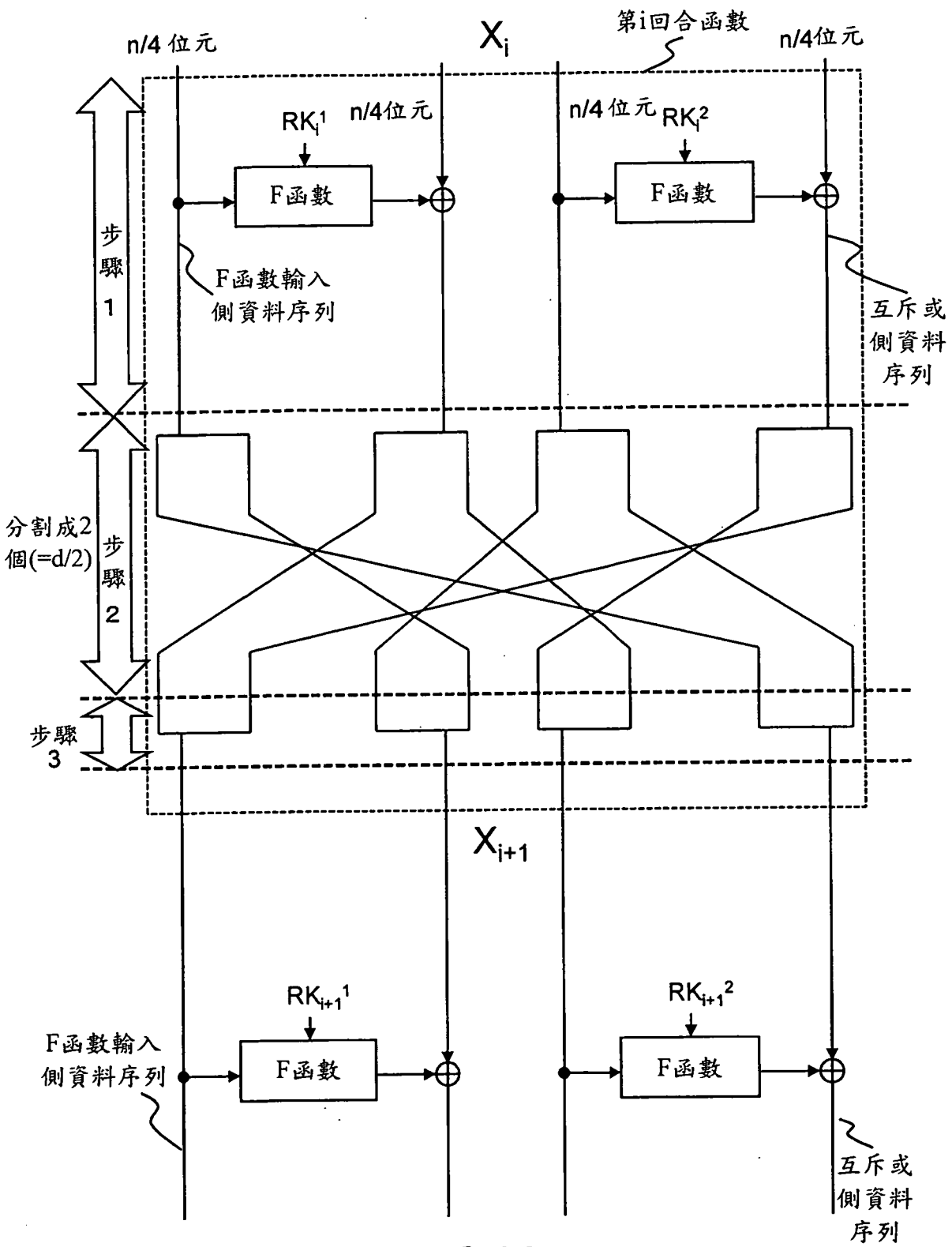
n/4 位元
X_i
第i回合函數
n/4位元
RK_i^1
n/4位元
n/4 位元
RK_i^2
F函數
F函數
步驟1
F函數輸入側資料序列
互斥或側資料序列
分割成2個(=d/2)
步驟2
步驟3
X_{i+1}
RK_{i+1}^1
RK_{i+1}^2
F函數輸入側資料序列
F函數
F函數
互斥或側資料序列

圖 20

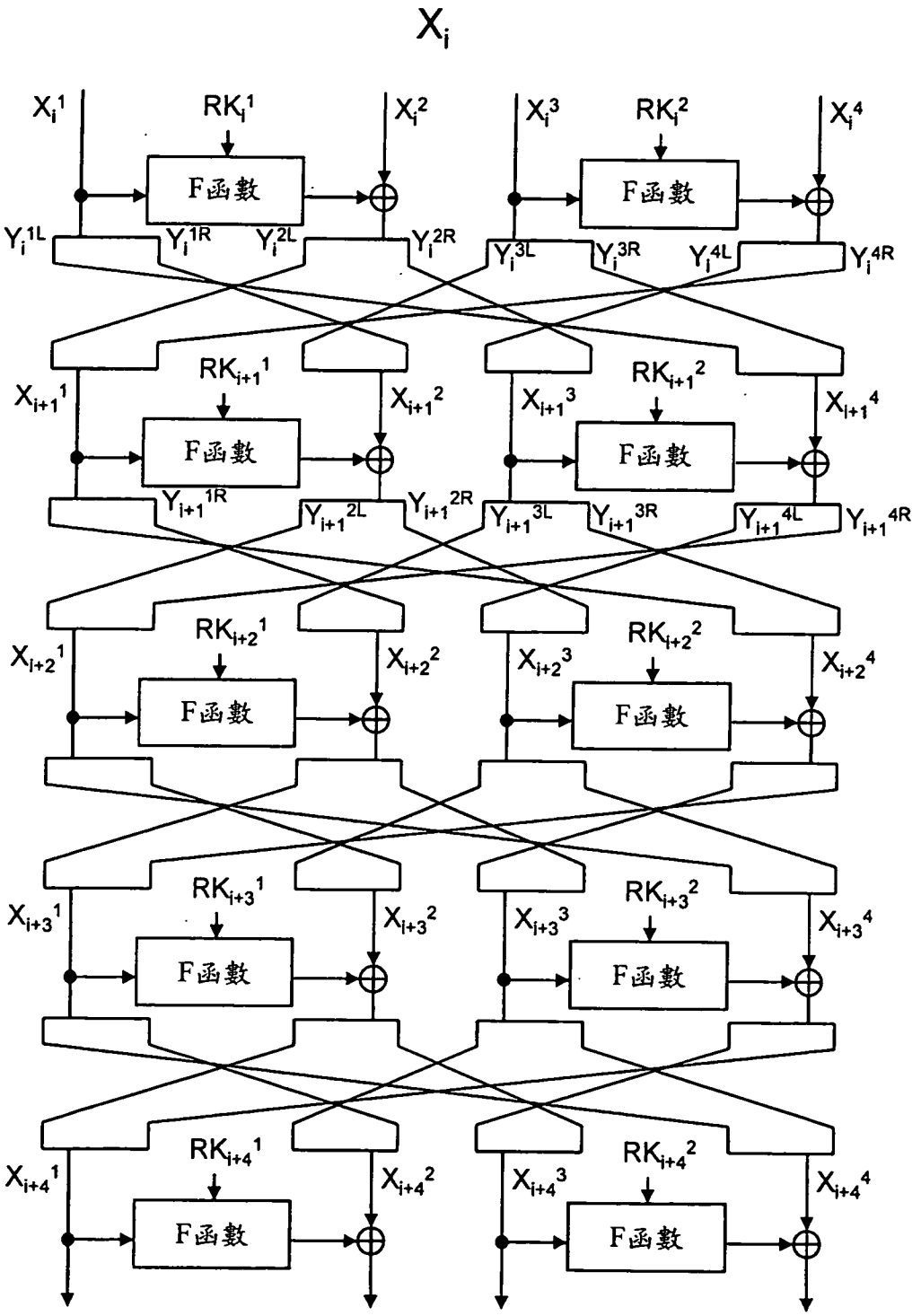
X_i
X_i^1
RK_i^1
X_i^2
X_i^3
RK_i^2
X_i^4
F函數
Y_i^{1L}
Y_i^{1R}
Y_i^{2L}
Y_i^{2R}
Y_i^{3L}
Y_i^{3R}
Y_i^{4L}
Y_i^{4R}
X_{i+1}^1
RK_{i+1}^1
X_{i+1}^2
X_{i+1}^3
RK_{i+1}^2
X_{i+1}^4
Y_{i+1}^{1R}
Y_{i+1}^{2L}
Y_{i+1}^{2R}
Y_{i+1}^{3L}
Y_{i+1}^{3R}
Y_{i+1}^{4L}
Y_{i+1}^{4R}
X_{i+2}^1
RK_{i+2}^1
X_{i+2}^2
X_{i+2}^3
RK_{i+2}^2
X_{i+2}^4
X_{i+3}^1
RK_{i+3}^1
X_{i+3}^2
X_{i+3}^3
RK_{i+3}^2
X_{i+3}^4
X_{i+4}^1
RK_{i+4}^1
X_{i+4}^2
X_{i+4}^3
RK_{i+4}^2
X_{i+4}^4

圖 21

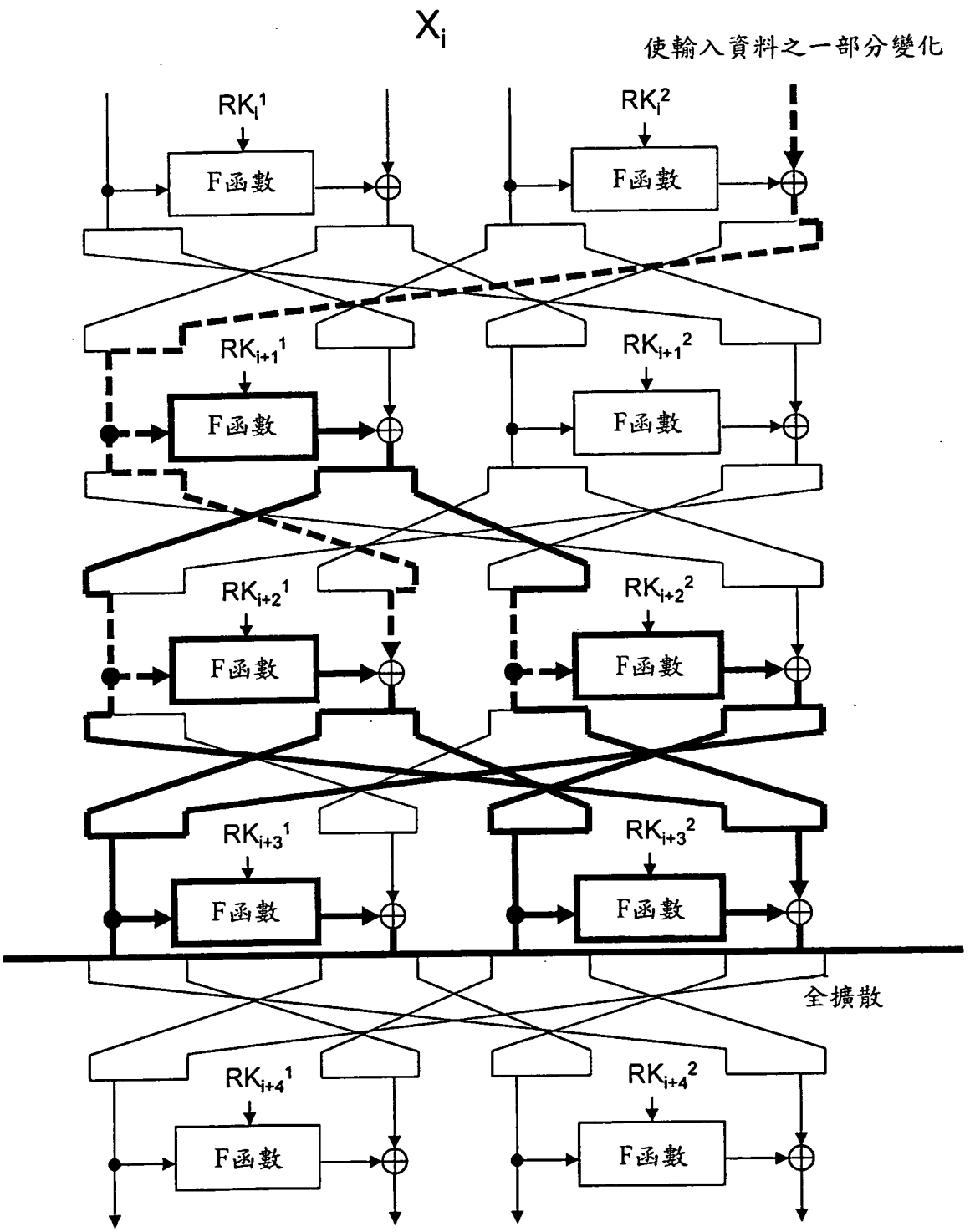
X_i
使輸入資料之一部分變化
RK_i^1
RK_i^2
F函數
RK_{i+1}^1
RK_{i+1}^2
RK_{i+2}^1
RK_{i+2}^2
RK_{i+3}^1
RK_{i+3}^2
全擴散
RK_{i+4}^1
RK_{i+4}^2

圖 22

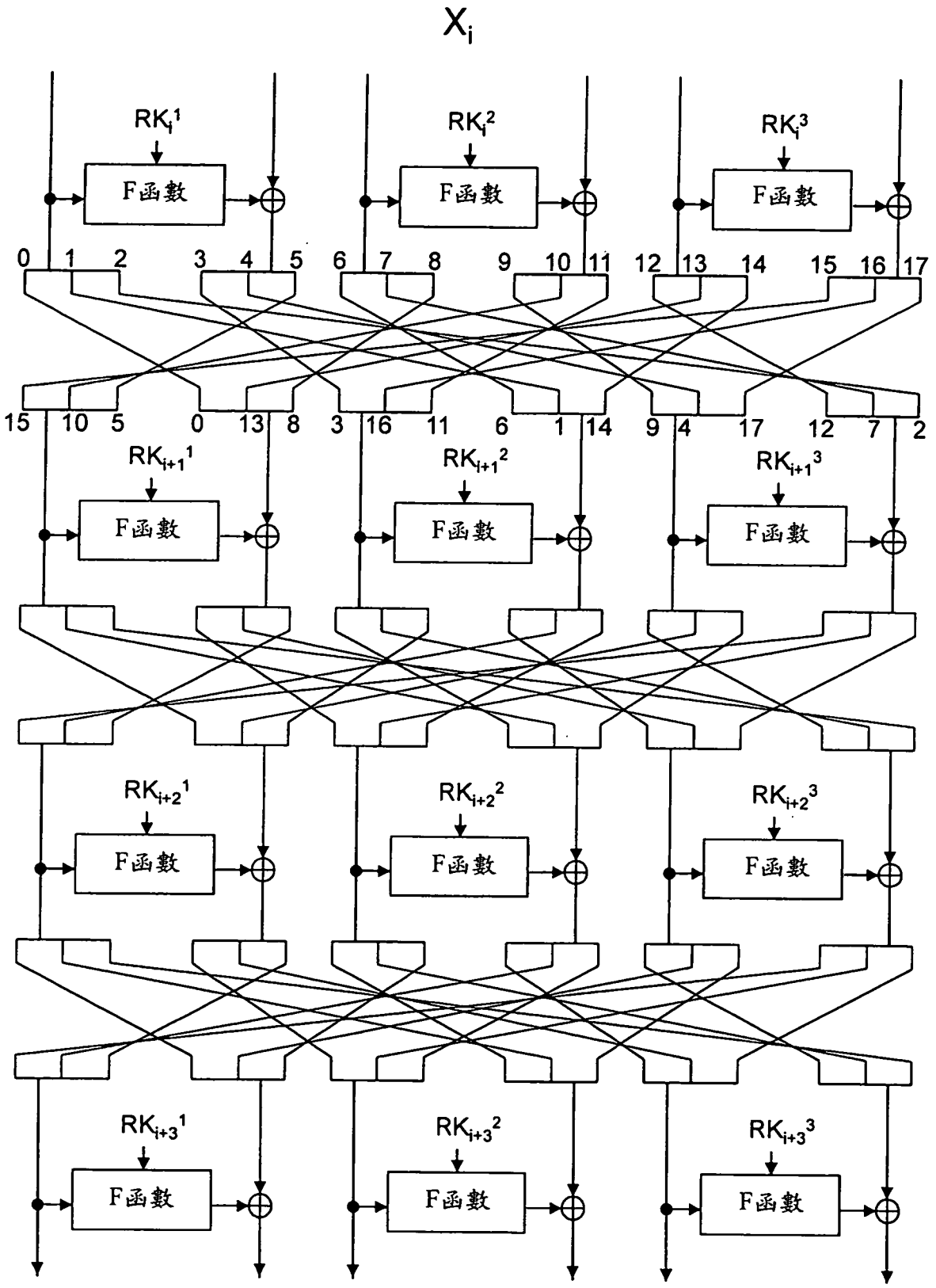
X_i
RK_i^1
RK_i^2
RK_i^3
F函數
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17
15 10 5 0 13 8 3 16 11 6 1 14 9 4 17 12 7 2
RK_{i+1}^1
RK_{i+1}^2
RK_{i+1}^3
RK_{i+2}^1
RK_{i+2}^2
RK_{i+2}^3
RK_{i+3}^1
RK_{i+3}^2
RK_{i+3}^3

圖 23

X_i

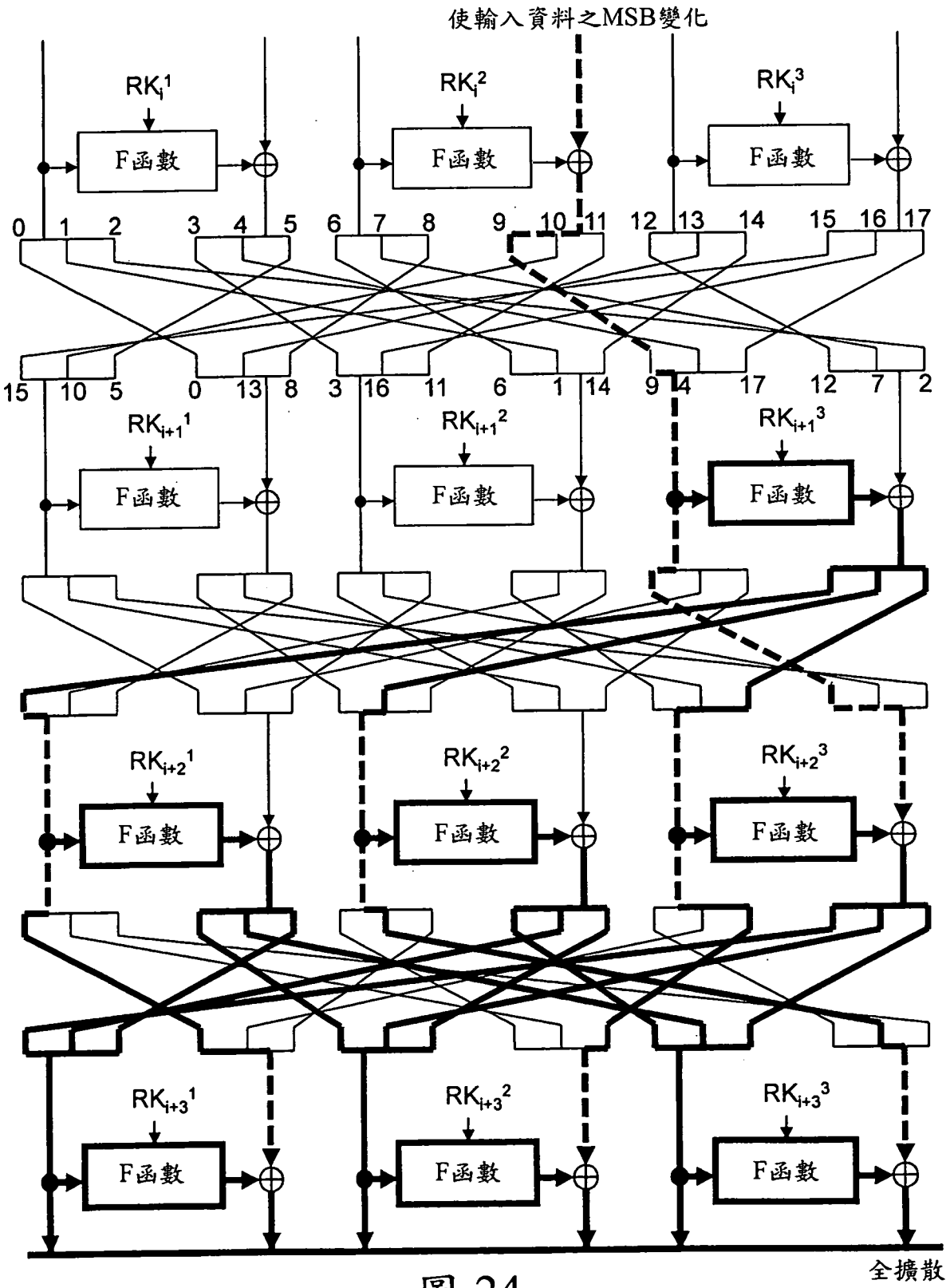
使輸入資料之MSB變化
RKi1
RKi2
RKi3
F函數
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17
15 10 5 0 13 8 3 16 11 6 1 14 9 4 17 12 7 2
RKi+11
RKi+12
RKi+13
RKi+21
RKi+22
RKi+23
RKi+31
RKi+32
RKi+33
全擴散

圖 24

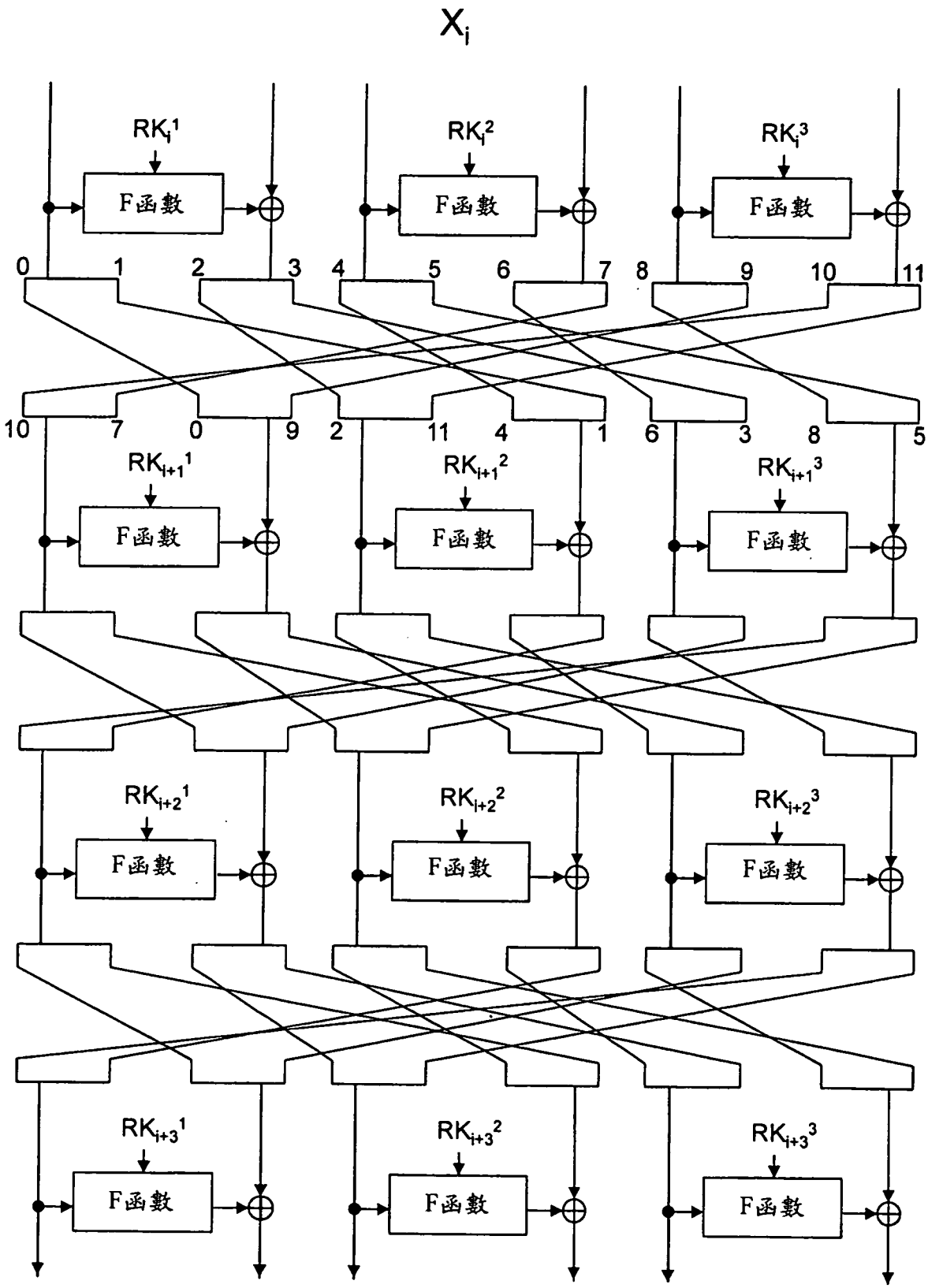
X_i
RK_i^1
RK_i^2
RK_i^3
F函數
0 1 2 3 4 5 6 7 8 9 10 11
10 7 0 9 2 11 4 1 6 3 8 5
RK_{i+1}^1
RK_{i+1}^2
RK_{i+1}^3
RK_{i+2}^1
RK_{i+2}^2
RK_{i+2}^3
RK_{i+3}^1
RK_{i+3}^2
RK_{i+3}^3

圖 25

n位元資料分割數d，d/n位元資料分
割數p與全擴散回合數之關係

d \ p	2	3	4	5	6	7	8	9	10	11	12
4	4	-	-	-	-	-	-	-	-	-	-
6	5	4	-	-	-	-	-	-	-	-	-
8	5	5	4	-	-	-	-	-	-	-	-
10	6	5	5	4	-	-	-	-	-	-	-
12	6	5	5	5	4	-	-	-	-	-	-
14	6	5	5	5	5	4	-	-	-	-	-
16	6	5	5	5	5	5	4	-	-	-	-
18	7	5	5	5	5	5	5	4	-	-	-
20	7	6	5	5	5	5	5	5	4	-	-
22	7	6	5	5	5	5	5	5	5	4	-
24	7	6	5	5	5	5	5	5	5	5	4

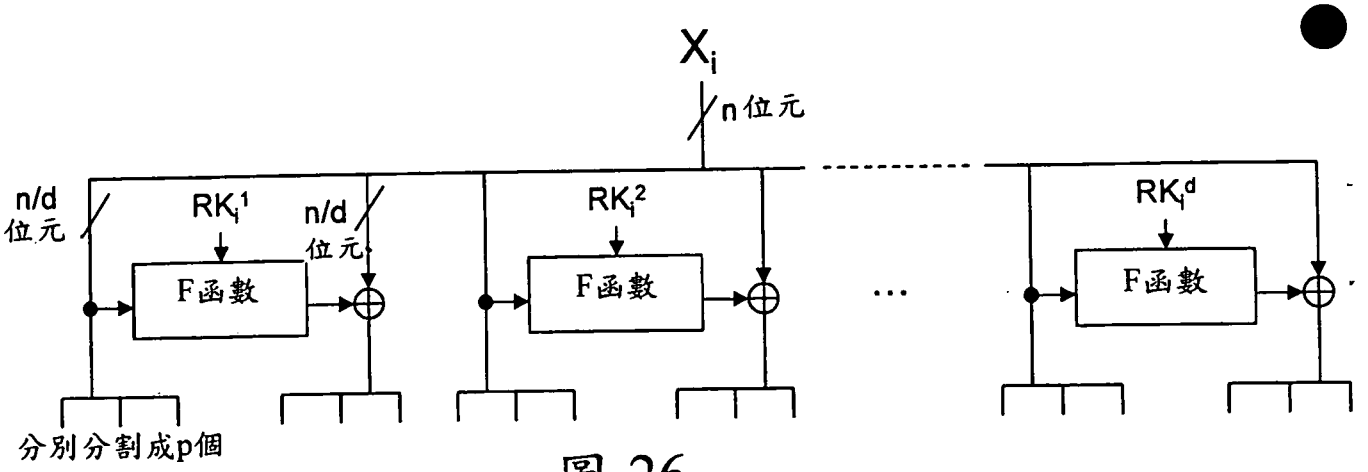

圖 26

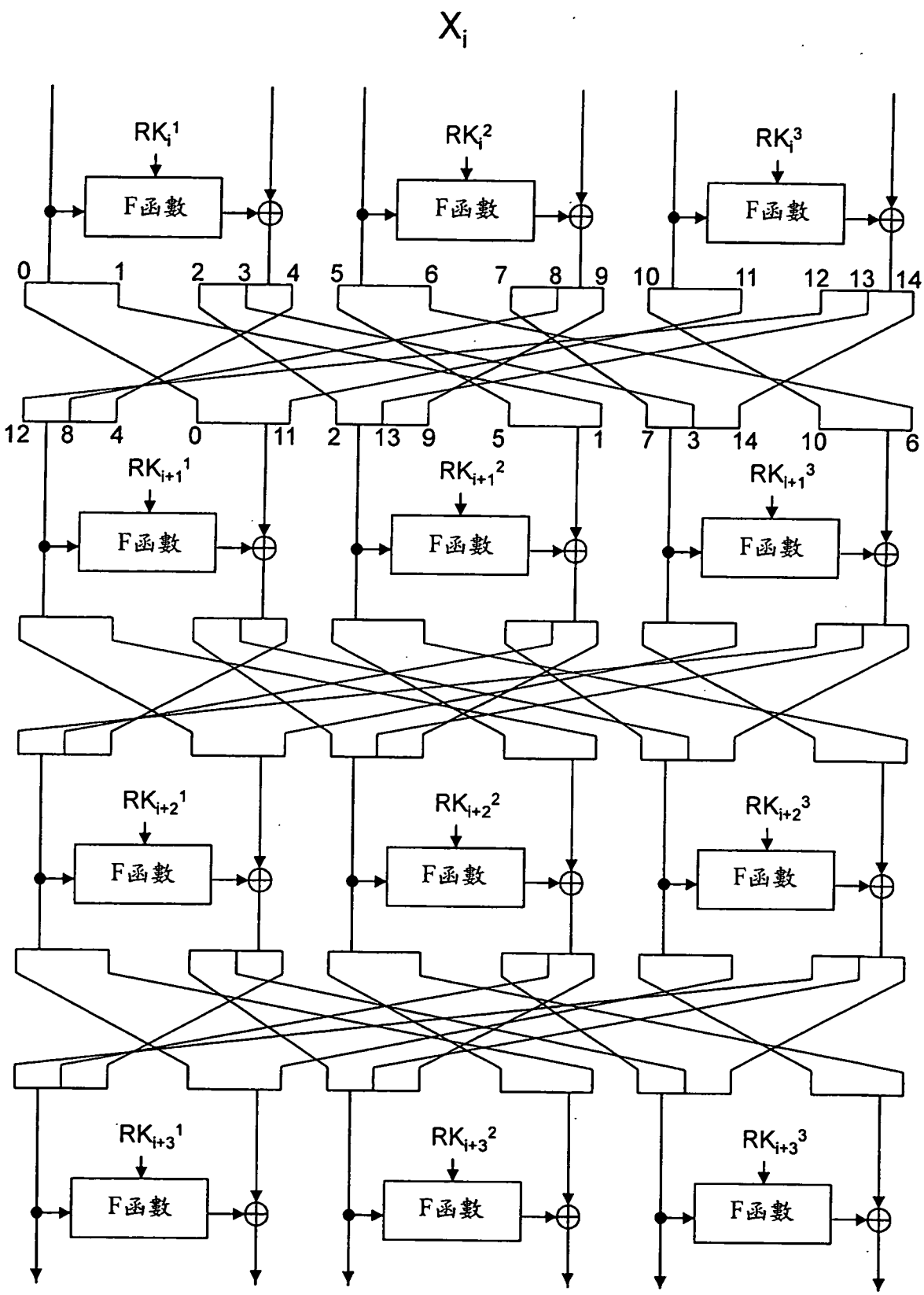
X_i
RK_i^1
RK_i^2
RK_i^3
F函數
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14
12 8 4 0 11 2 13 9 5 1 7 3 14 10 6
RK_{i+1}^1
RK_{i+1}^2
RK_{i+1}^3
RK_{i+2}^1
RK_{i+2}^2
RK_{i+2}^3
RK_{i+3}^1
RK_{i+3}^2
RK_{i+3}^3

圖 27

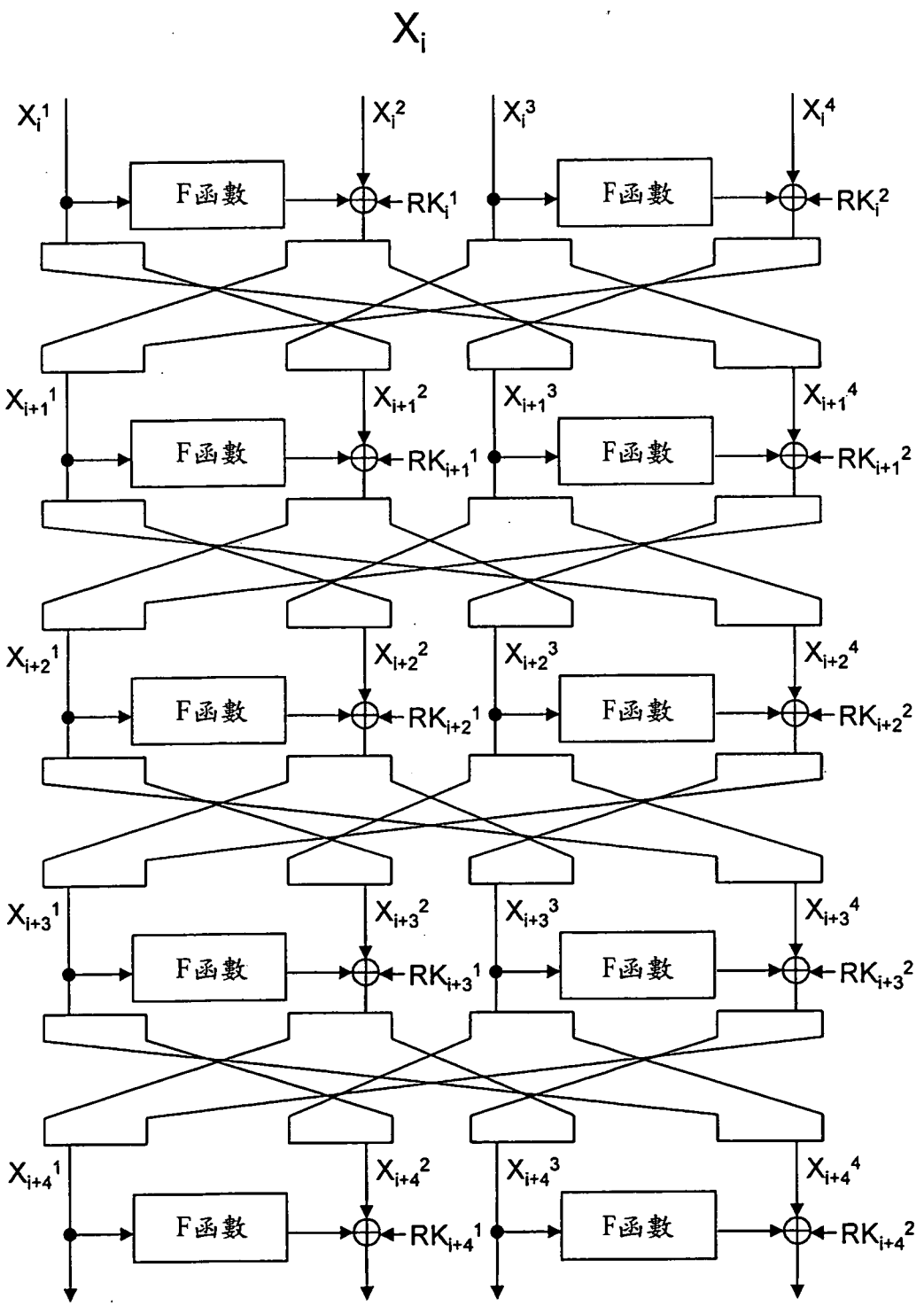
X_i
X_i^1
X_i^2
X_i^3
X_i^4
F函數
RK_i^1
RK_i^2
X_{i+1}^1
X_{i+1}^2
X_{i+1}^3
X_{i+1}^4
RK_{i+1}^1
RK_{i+1}^2
X_{i+2}^1
X_{i+2}^2
X_{i+2}^3
X_{i+2}^4
RK_{i+2}^1
RK_{i+2}^2
X_{i+3}^1
X_{i+3}^2
X_{i+3}^3
X_{i+3}^4
RK_{i+3}^1
RK_{i+3}^2
X_{i+4}^1
X_{i+4}^2
X_{i+4}^3
X_{i+4}^4
RK_{i+4}^1
RK_{i+4}^2

圖 28

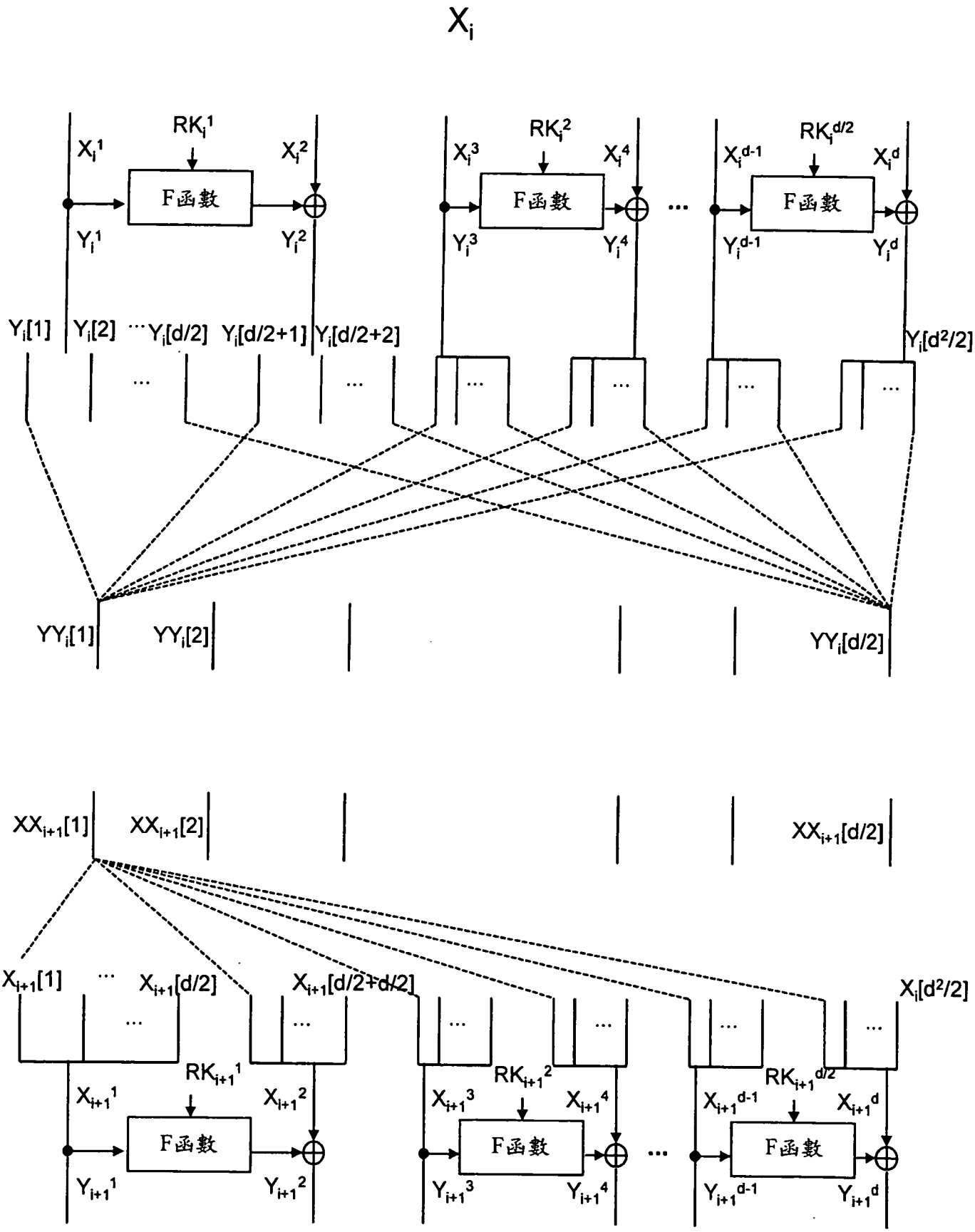
X_i
RK_i^1
X_i^1
X_i^2
F函數
Y_i^1
Y_i^2
RK_i^2
X_i^3
X_i^4
F函數
Y_i^3
Y_i^4
$RK_i^{d/2}$
X_i^{d-1}
X_i^d
F函數
Y_i^{d-1}
Y_i^d
$Y_i[1]$ $Y_i[2]$ $Y_i[d/2]$ $Y_i[d/2+1]$ $Y_i[d/2+2]$
$Y_i[d^2/2]$
$YY_i[1]$
$YY_i[2]$
$YY_i[d/2]$
$XX_{i+1}[1]$
$XX_{i+1}[2]$
$XX_{i+1}[d/2]$
$X_{i+1}[1]$ $X_{i+1}[d/2]$ $X_{i+1}[d/2+d/2]$
$X_i[d^2/2]$
RK_{i+1}^1
X_{i+1}^1
X_{i+1}^2
F函數
Y_{i+1}^1
Y_{i+1}^2
RK_{i+1}^2
X_{i+1}^3
X_{i+1}^4
F函數
Y_{i+1}^3
Y_{i+1}^4
$RK_{i+1}^{d/2}$
X_{i+1}^{d-1}
X_{i+1}^d
F函數
Y_{i+1}^{d-1}
Y_{i+1}^d

圖 29

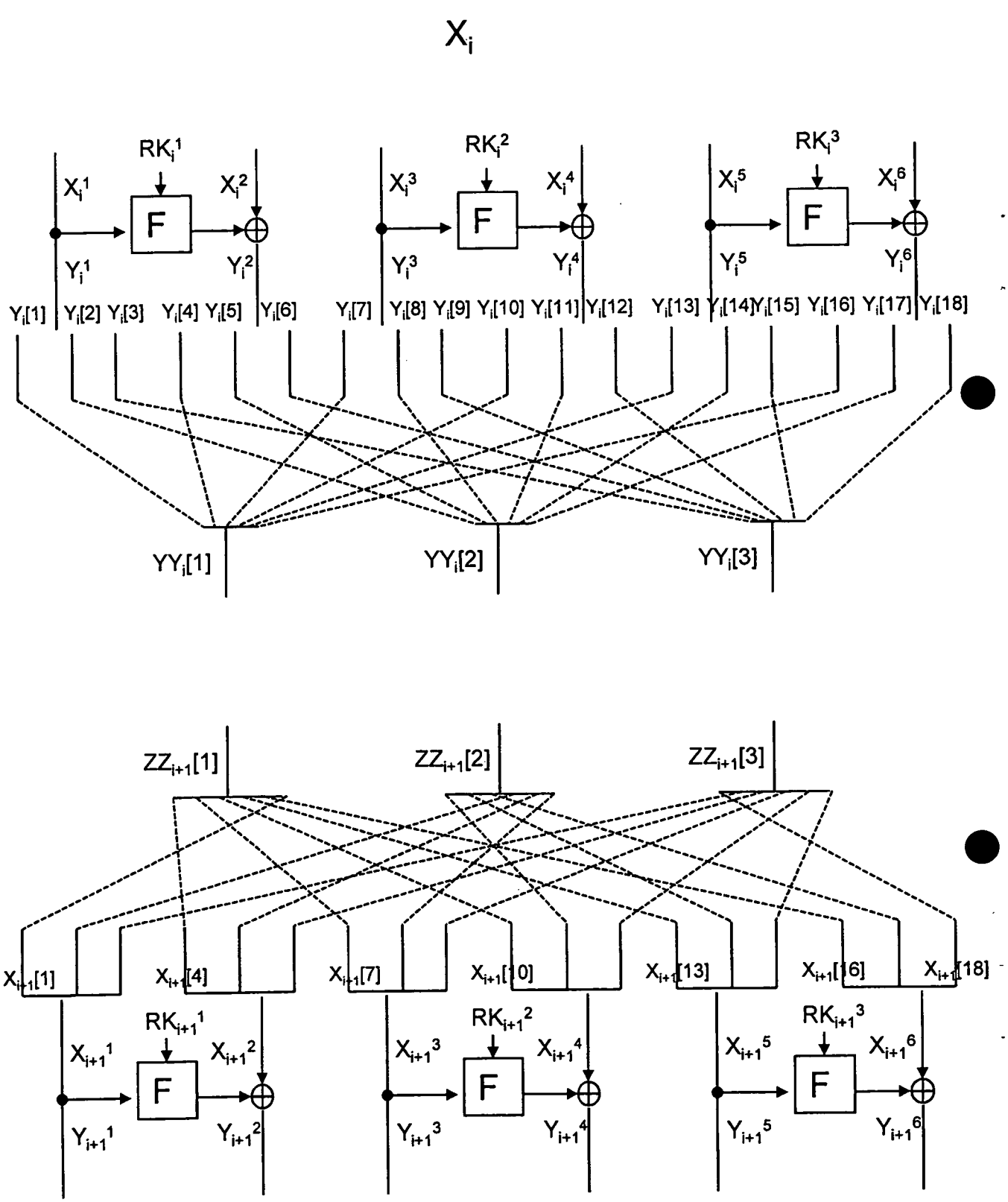
X_i
RK_i^1
RK_i^2
RK_i^3
F
X_i^1 X_i^2 X_i^3 X_i^4 X_i^5 X_i^6
Y_i^1 Y_i^2 Y_i^3 Y_i^4 Y_i^5 Y_i^6
$Y_i[1]$ $Y_i[2]$ $Y_i[3]$ $Y_i[4]$ $Y_i[5]$ $Y_i[6]$ $Y_i[7]$ $Y_i[8]$ $Y_i[9]$ $Y_i[10]$ $Y_i[11]$ $Y_i[12]$ $Y_i[13]$ $Y_i[14]$ $Y_i[15]$ $Y_i[16]$ $Y_i[17]$ $Y_i[18]$
$YY_i[1]$ $YY_i[2]$ $YY_i[3]$
$ZZ_{i+1}[1]$ $ZZ_{i+1}[2]$ $ZZ_{i+1}[3]$
$X_{i+1}[1]$ $X_{i+1}[4]$ $X_{i+1}[7]$ $X_{i+1}[10]$ $X_{i+1}[13]$ $X_{i+1}[16]$ $X_{i+1}[18]$
RK_{i+1}^1 RK_{i+1}^2 RK_{i+1}^3
X_{i+1}^1 X_{i+1}^2 X_{i+1}^3 X_{i+1}^4 X_{i+1}^5 X_{i+1}^6
Y_{i+1}^1 Y_{i+1}^2 Y_{i+1}^3 Y_{i+1}^4 Y_{i+1}^5 Y_{i+1}^6

圖 30

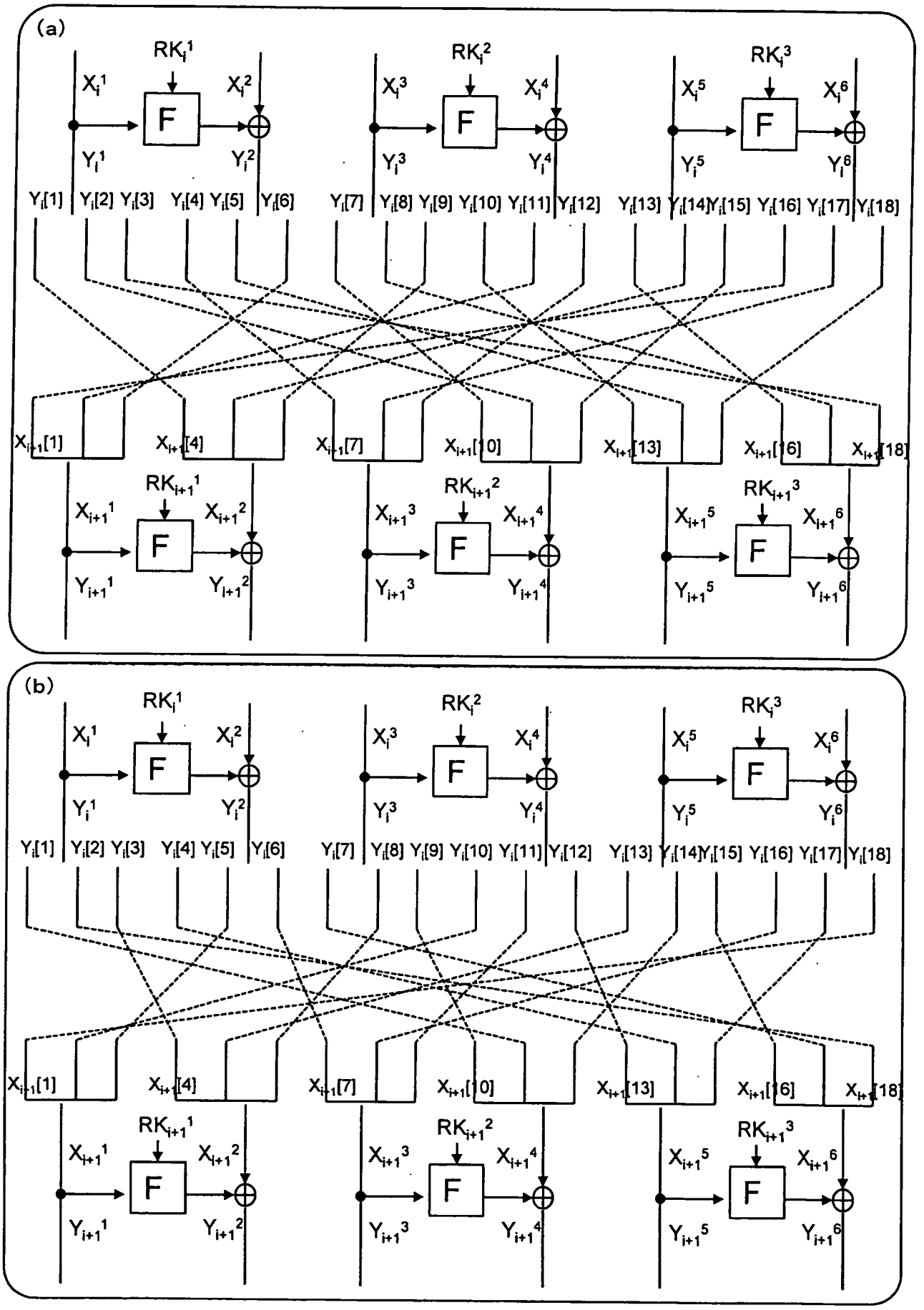

圖 31

Feistel 結構(加密函數)

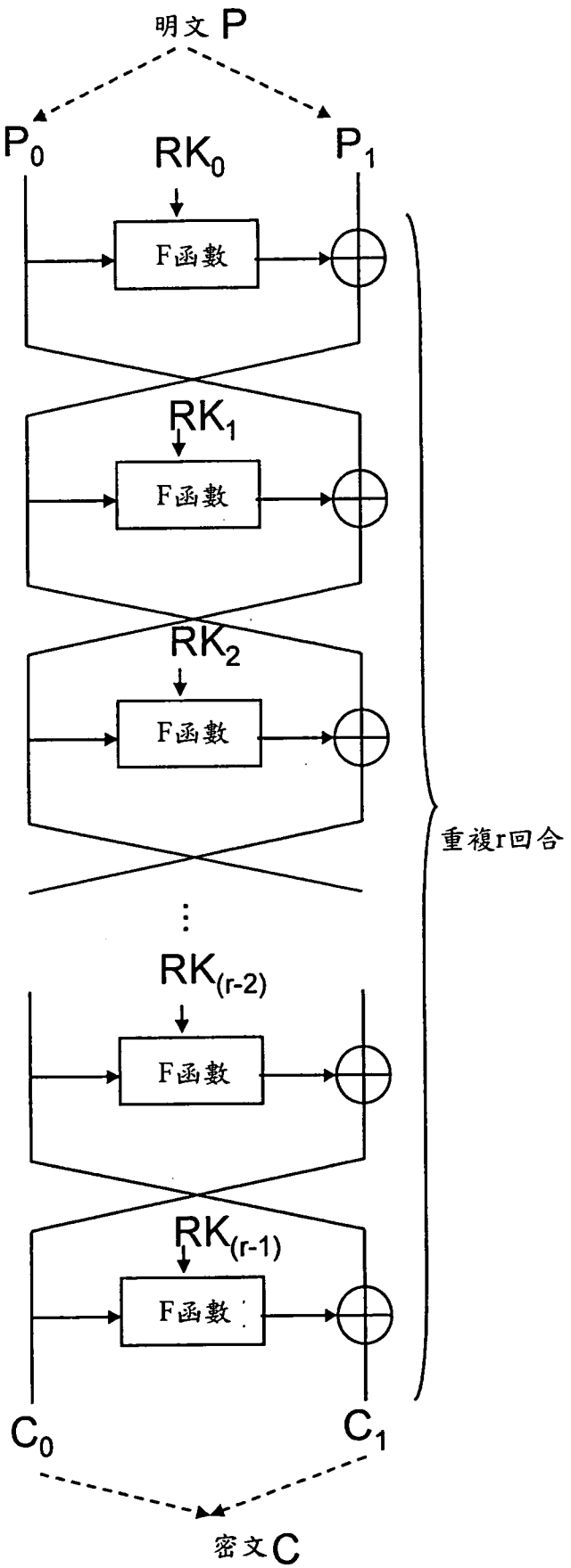

圖 32

Feistel 結構(解密函數)

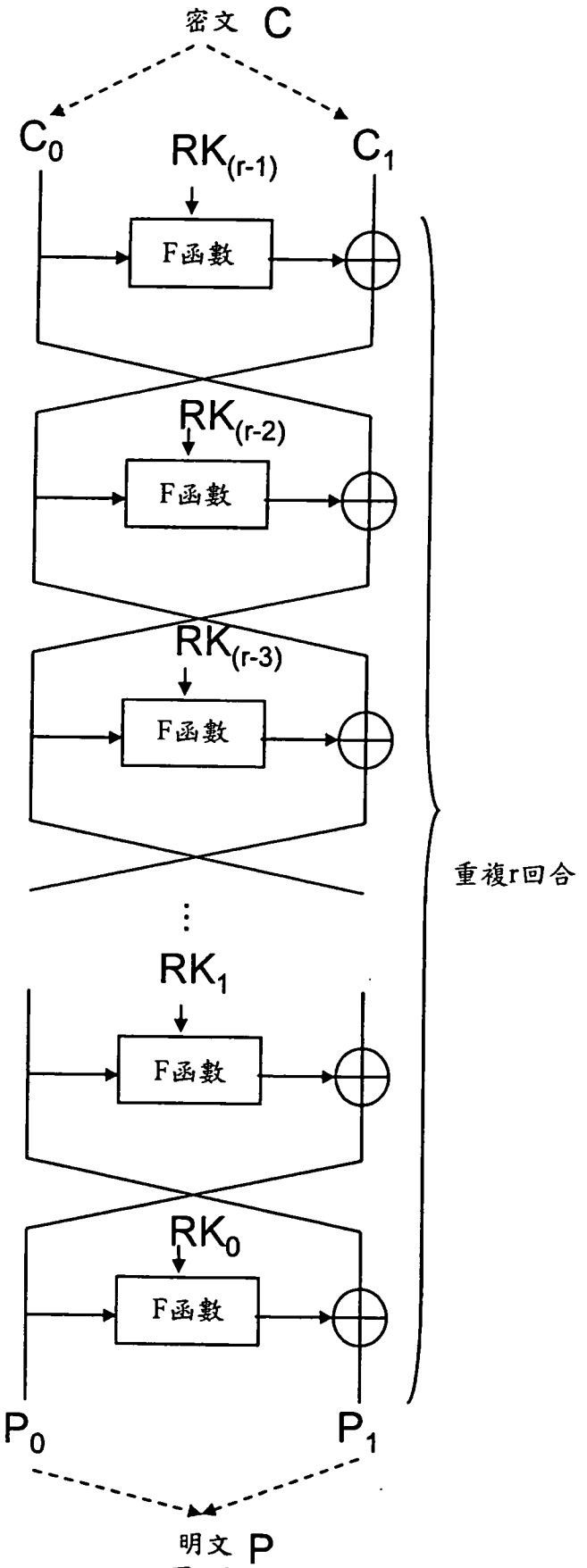

圖 33

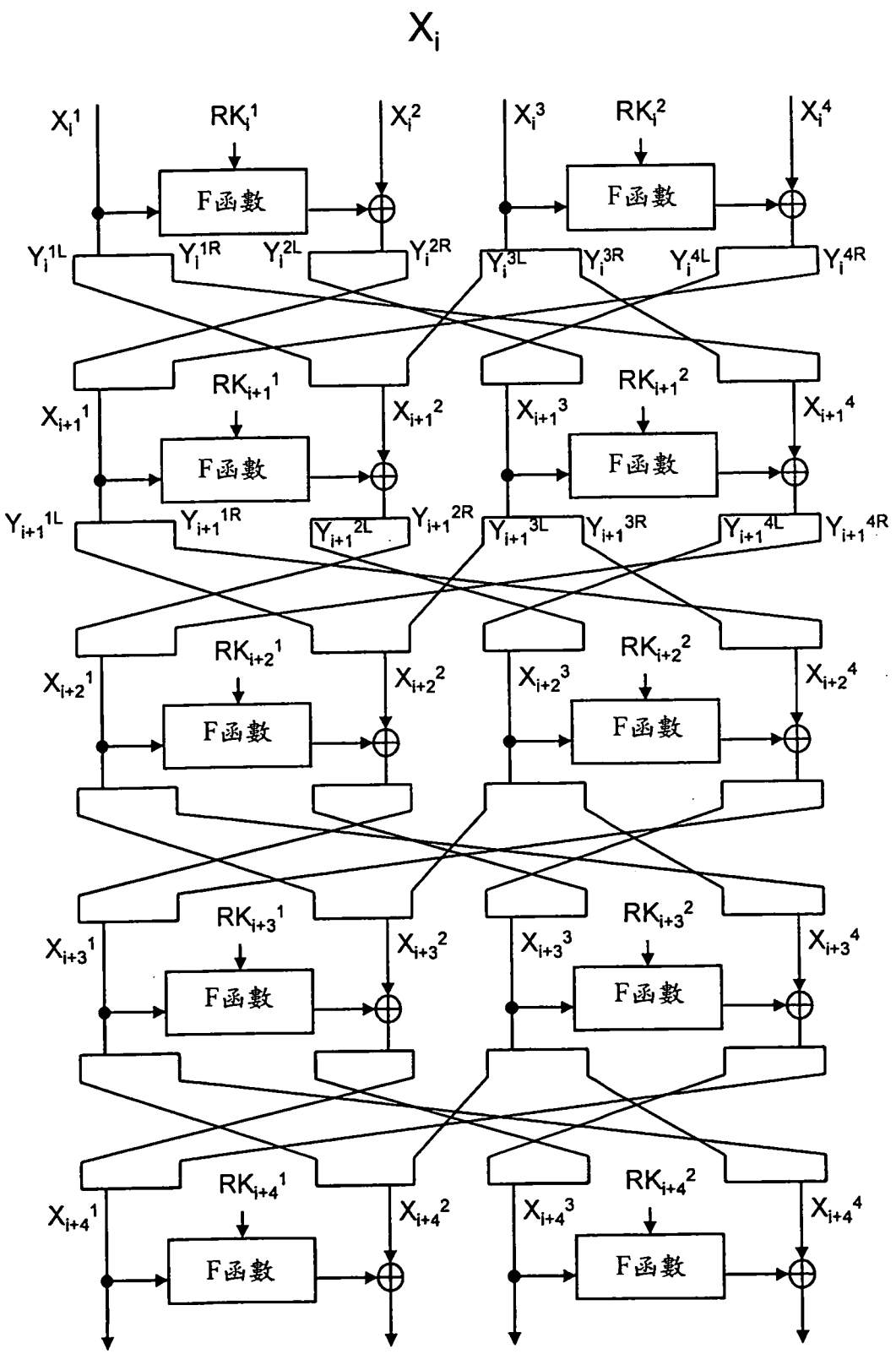
X_i
X_i^1
RK_i^1
X_i^2
X_i^3
RK_i^2
X_i^4
F函數
Y_i^{1L}
Y_i^{1R}
Y_i^{2L}
Y_i^{2R}
Y_i^{3L}
Y_i^{3R}
Y_i^{4L}
Y_i^{4R}
RK_{i+1}^1
X_{i+1}^1
X_{i+1}^2
RK_{i+1}^2
X_{i+1}^3
X_{i+1}^4
Y_{i+1}^{1L}
Y_{i+1}^{1R}
Y_{i+1}^{2L}
Y_{i+1}^{2R}
Y_{i+1}^{3L}
Y_{i+1}^{3R}
Y_{i+1}^{4L}
Y_{i+1}^{4R}
RK_{i+2}^1
X_{i+2}^1
X_{i+2}^2
RK_{i+2}^2
X_{i+2}^3
X_{i+2}^4
RK_{i+3}^1
X_{i+3}^1
X_{i+3}^2
RK_{i+3}^2
X_{i+3}^3
X_{i+3}^4
RK_{i+4}^1
X_{i+4}^1
X_{i+4}^2
RK_{i+4}^2
X_{i+4}^3
X_{i+4}^4

圖 34

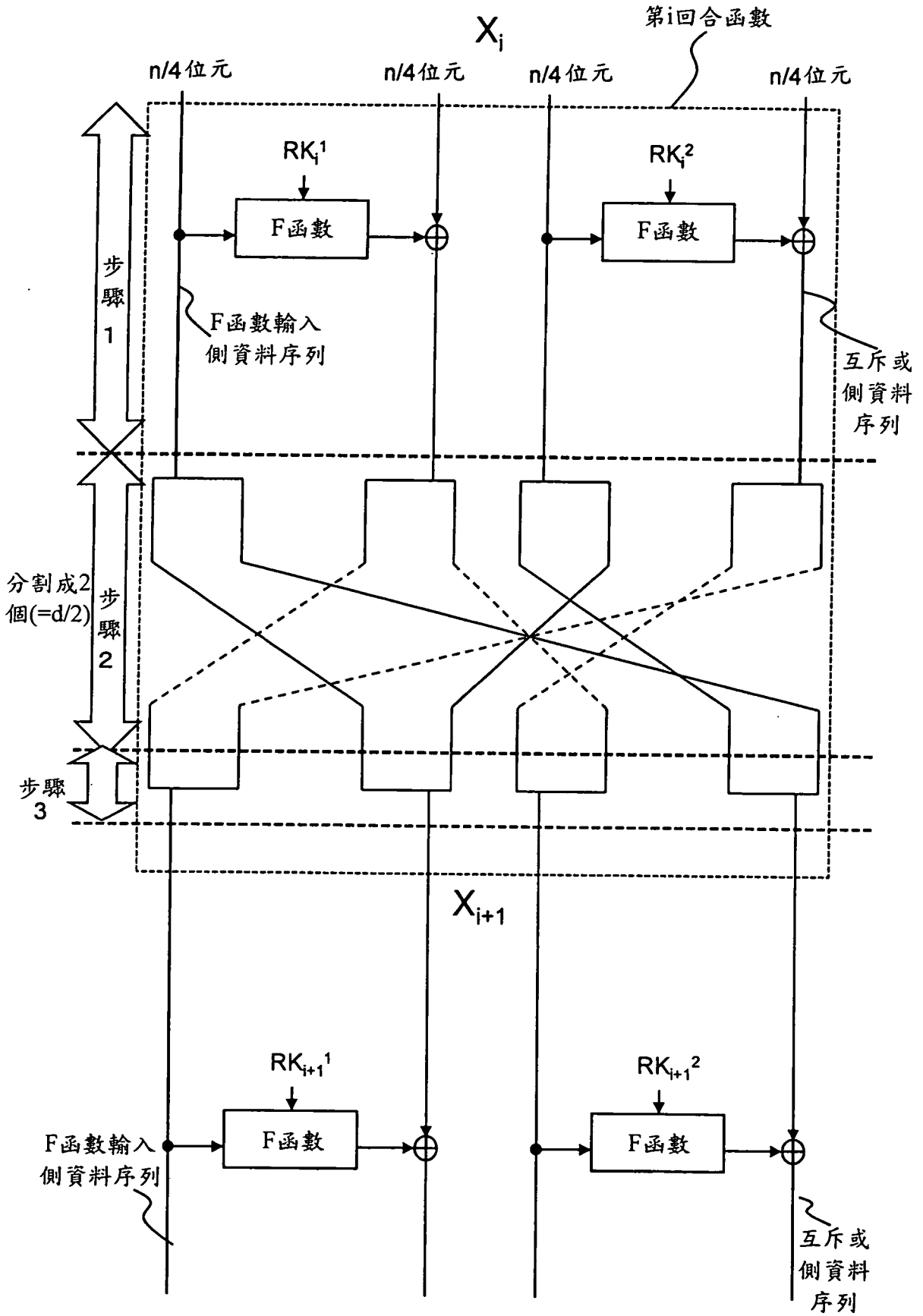
X_j
第i回合函數
n/4位元
n/4位元
n/4位元
n/4位元
RK_i^1
RK_i^2
F函數
F函數
步驟1
F函數輸入側資料序列
互斥或側資料序列
分割成2個(=d/2)
步驟2
步驟3
X_{i+1}
RK_{i+1}^1
RK_{i+1}^2
F函數
F函數
F函數輸入側資料序列
互斥或側資料序列

圖 35

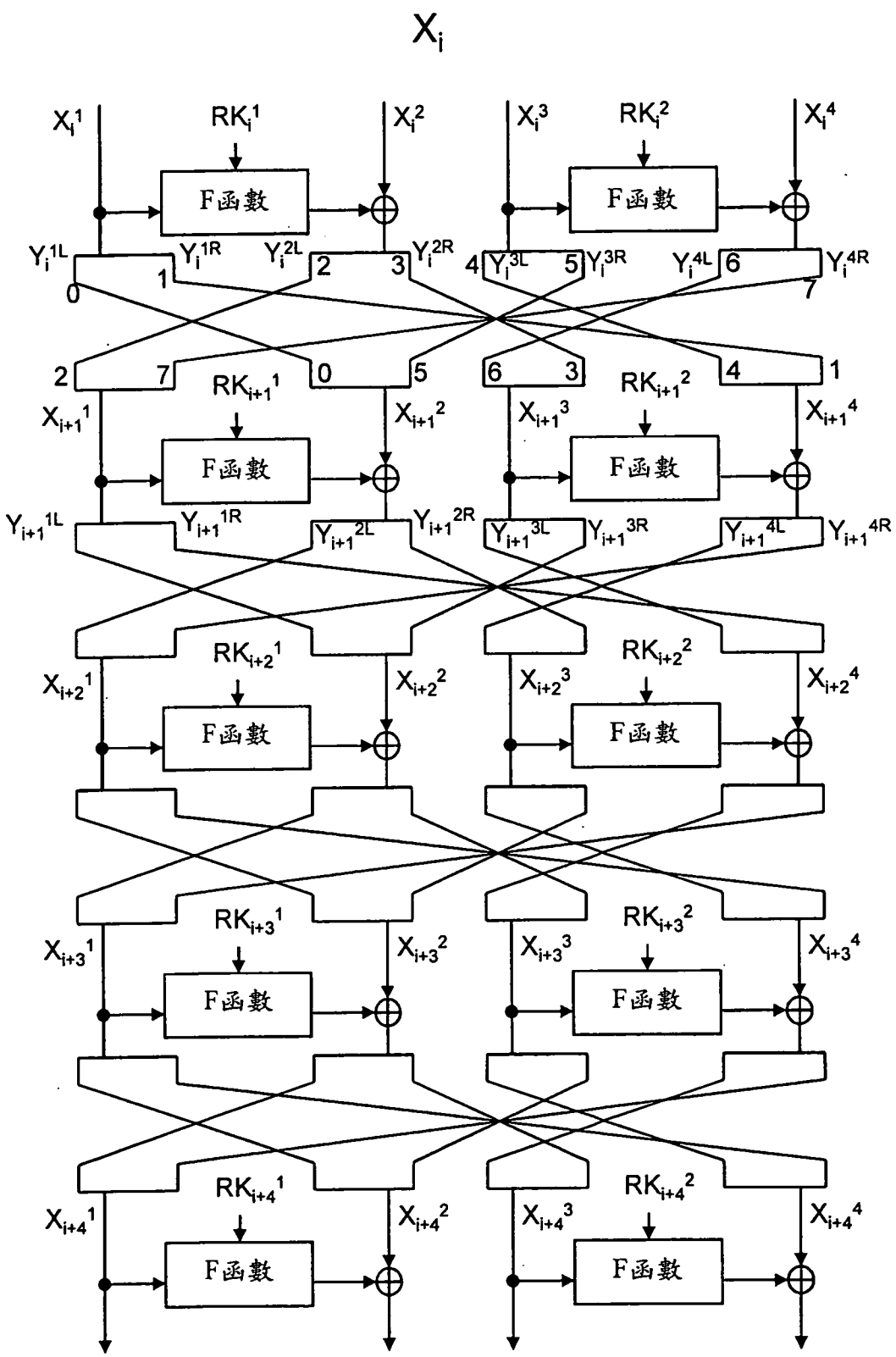
X_i
X_i^1
RK_i^1
X_i^2
X_i^3
RK_i^2
X_i^4
F函數
Y_i^{1L}
Y_i^{1R}
Y_i^{2L}
Y_i^{2R}
Y_i^{3L}
Y_i^{3R}
Y_i^{4L}
Y_i^{4R}
0
1
2
3
4
5
6
7
RK_{i+1}^1
RK_{i+1}^2
X_{i+1}^1
X_{i+1}^2
X_{i+1}^3
X_{i+1}^4
Y_{i+1}^{1L}
Y_{i+1}^{1R}
Y_{i+1}^{2L}
Y_{i+1}^{2R}
Y_{i+1}^{3L}
Y_{i+1}^{3R}
Y_{i+1}^{4L}
Y_{i+1}^{4R}
RK_{i+2}^1
RK_{i+2}^2
X_{i+2}^1
X_{i+2}^2
X_{i+2}^3
X_{i+2}^4
RK_{i+3}^1
RK_{i+3}^2
X_{i+3}^1
X_{i+3}^2
X_{i+3}^3
X_{i+3}^4
RK_{i+4}^1
RK_{i+4}^2
X_{i+4}^1
X_{i+4}^2
X_{i+4}^3
X_{i+4}^4

圖 36

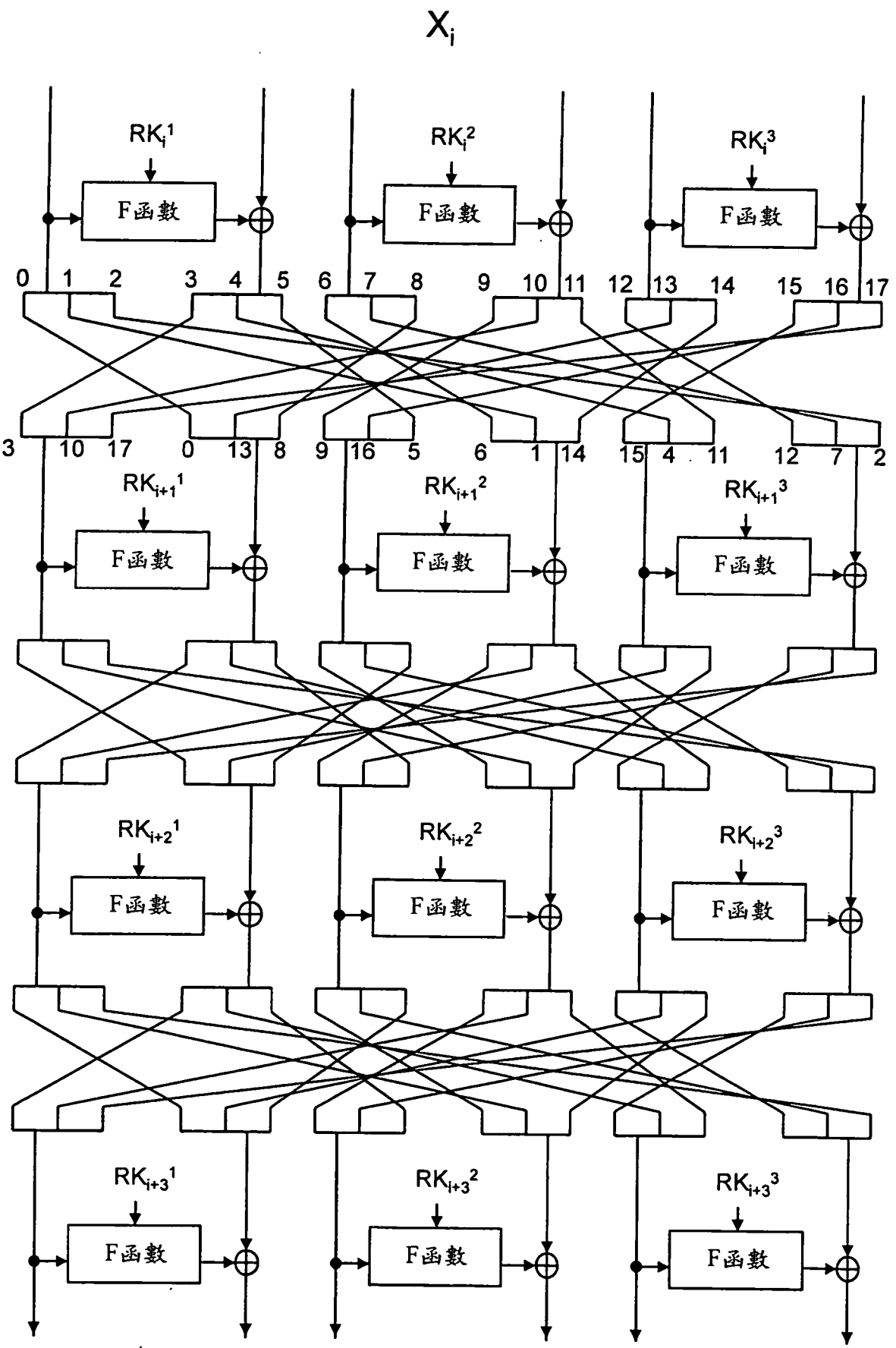
X_i
RK_i^1
RK_i^2
RK_i^3
F函數
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17
3 10 17 0 13 8 9 16 5 6 1 14 15 4 11 12 7 2
RK_{i+1}^1
RK_{i+1}^2
RK_{i+1}^3
RK_{i+2}^1
RK_{i+2}^2
RK_{i+2}^3
RK_{i+3}^1
RK_{i+3}^2
RK_{i+3}^3

圖 37

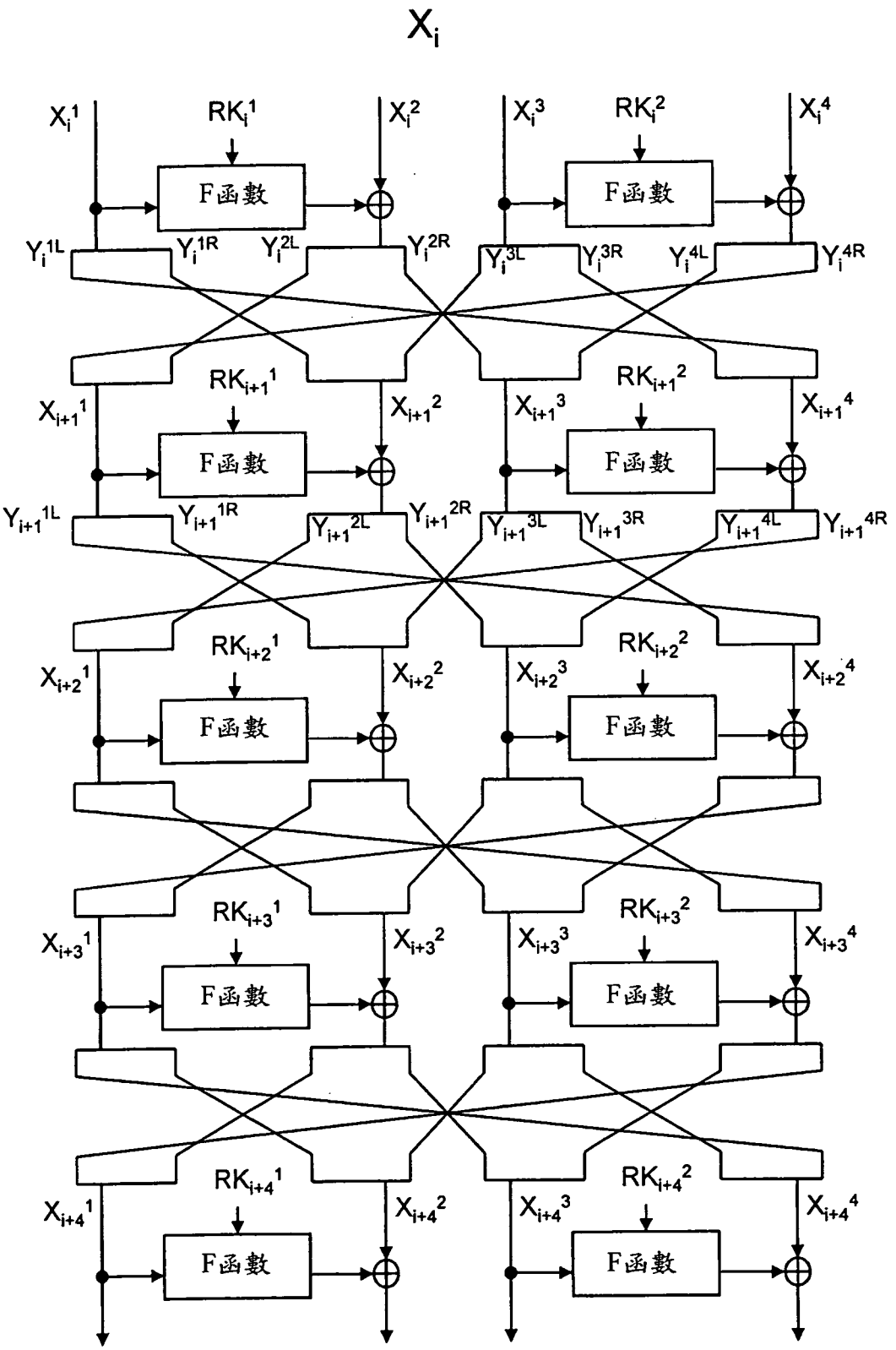
X_i
X_i^1
RK_i^1
X_i^2
X_i^3
RK_i^2
X_i^4
F函數
Y_i^{1L}
Y_i^{1R}
Y_i^{2L}
Y_i^{2R}
Y_i^{3L}
Y_i^{3R}
Y_i^{4L}
Y_i^{4R}
RK_{i+1}^1
X_{i+1}^1
X_{i+1}^2
X_{i+1}^3
RK_{i+1}^2
X_{i+1}^4
Y_{i+1}^{1L}
Y_{i+1}^{1R}
Y_{i+1}^{2L}
Y_{i+1}^{2R}
Y_{i+1}^{3L}
Y_{i+1}^{3R}
Y_{i+1}^{4L}
Y_{i+1}^{4R}
RK_{i+2}^1
X_{i+2}^1
X_{i+2}^2
X_{i+2}^3
RK_{i+2}^2
X_{i+2}^4
RK_{i+3}^1
X_{i+3}^1
X_{i+3}^2
X_{i+3}^3
RK_{i+3}^2
X_{i+3}^4
RK_{i+4}^1
X_{i+4}^1
X_{i+4}^2
X_{i+4}^3
RK_{i+4}^2
X_{i+4}^4

圖 38

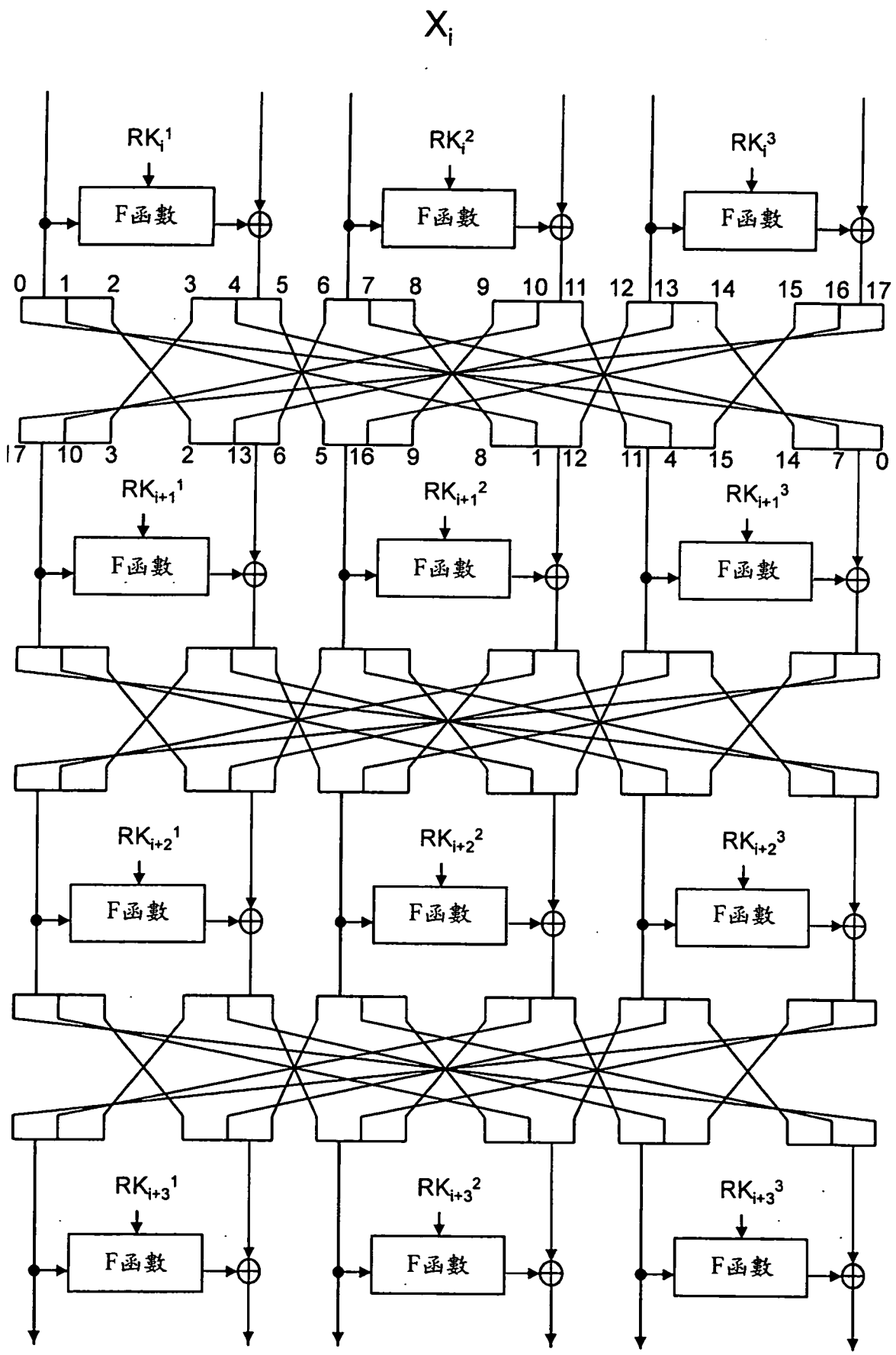
X_i
RK_i^1
RK_i^2
RK_i^3
F函數
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17
17 10 3 2 13 6 5 16 9 8 1 12 11 4 15 14 7 0
RK_{i+1}^1
RK_{i+1}^2
RK_{i+1}^3
RK_{i+2}^1
RK_{i+2}^2
RK_{i+2}^3
RK_{i+3}^1
RK_{i+3}^2
RK_{i+3}^3

圖 39

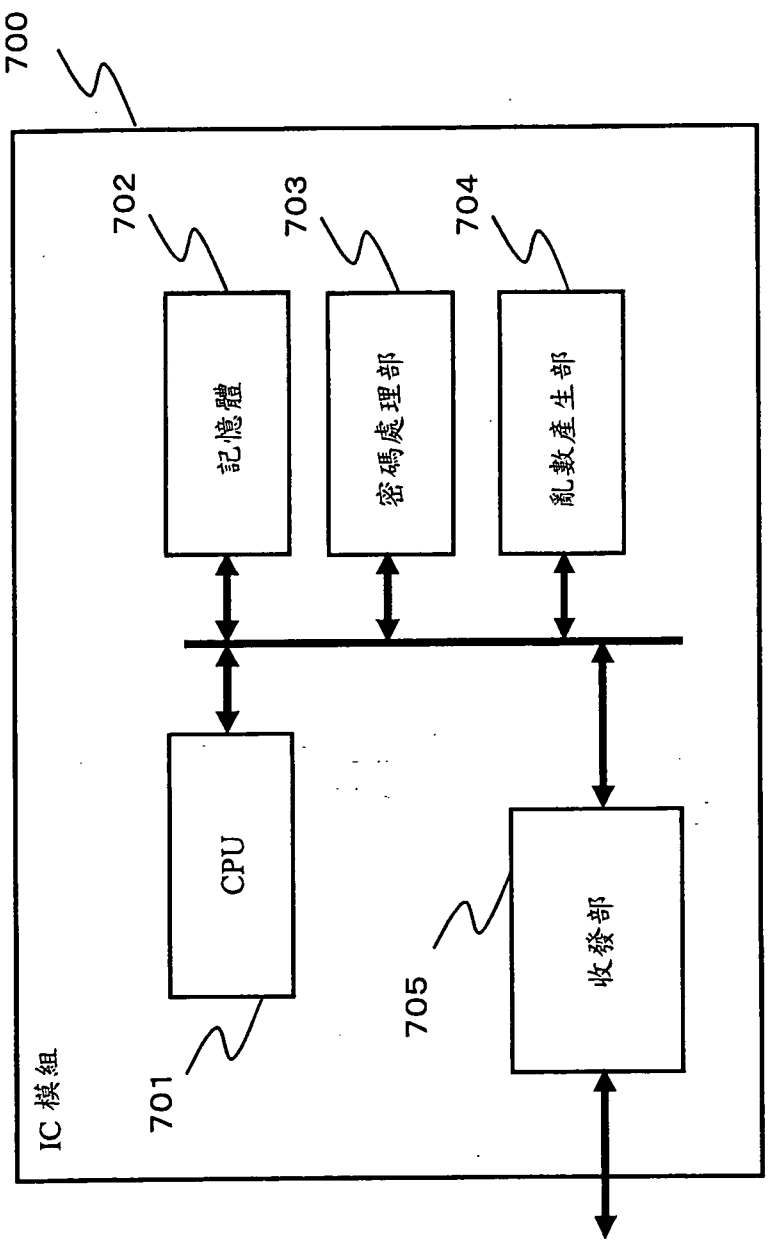

圖 40