(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2008 年1 月31 日 (31.01.2008)

PCT

(10) 国際公開番号
WO 2008/013076 A1

(51) 国際特許分類:
G09C 1/00 (2006.01) *H04L 9/06* (2006.01)

(21) 国際出願番号: PCT/JP2007/064089

(22) 国際出願日: 2007 年7 月17 日 (17.07.2007)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2006-206376 2006 年7 月28 日 (28.07.2006) JP
特願2006-224674 2006 年8 月21 日 (21.08.2006) JP

(71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒1080075 東京都港区港南１丁目７番１号 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 白井 太三 (SHIRAI, Taizo) [JP/JP]; 〒1080075 東京都港区港南１丁目７番１号 ソニー株式会社内 Tokyo (JP). 渋谷 香士 (SHIBUTANI, Kyoji) [JP/JP]; 〒1080075 東京都港区港南１丁目７番１号 ソニー株式会社内 Tokyo (JP).

(74) 代理人: 宮田 正昭, 外(MIYATA, Masaaki et al.); 〒1040041 東京都中央区新富一丁目１番７号 銀座ティーケイビル 澤田・宮田・山田・佐々木特許事務所 Tokyo (JP).

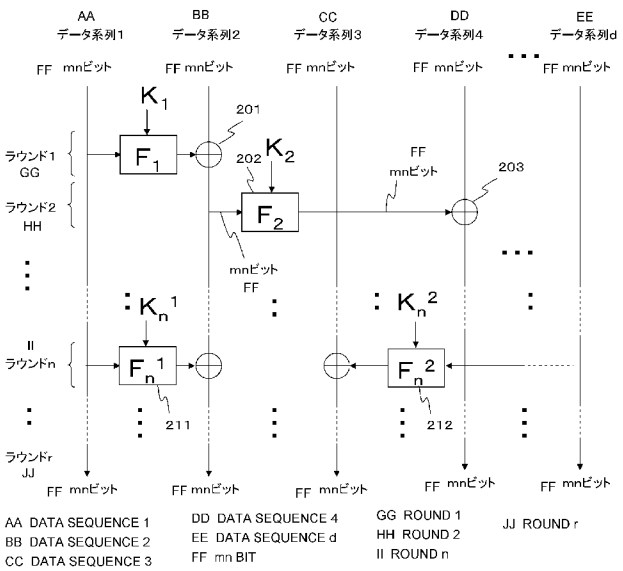
(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD,

[続葉有]

(54) **Title:** ENCRYPTION PROCESSING DEVICE, METHOD FOR BUILDING ENCRYPTION PROCESS ALGORITHM, ENCRYPTION PROCESSING METHOD, AND COMPUTER PROGRAM

(54) **発明の名称:** 暗号処理装置、暗号処理アルゴリズム構築方法、および暗号処理方法、並びにコンピュータ・プログラム



(57) **Abstract:** It is possible to realize an extended Feistel-type common key block encryption process configuration for realizing a diffusion matrix switching mechanism (DSM). In an encryption process configuration using the extended Feistel structure in which a data sequence number d is an integer not smaller than 2, a plurality of different matrixes are selectively applied in the linear conversion process of the F function unit by selecting a plurality of different matrixes which satisfy the condition that the minimum branching number in all the data sequence selected from the minimum branching number corresponding to a data sequence based on the linear conversion matrix contained in the F function inputted to each data sequence of the extended Feistel structure is a value not smaller than a predetermined value. The present invention realizes a common key block encryption having a high resistance for linear analysis and differential analysis based on the DSM.

[続葉有]

WO 2008/013076 A1

SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(57) 要約: 拡散行列切り替え機構（ＤＳＭ）を実現する拡張Ｆｅｉｓｔｅｌ型共通鍵ブロック暗号処理構成を実現する。データ系列数：ｄをｄ≧２の整数とした拡張Ｆｅｉｓｔｅｌ構造を適用した暗号処理構成において、Ｆ関数部の線形変換処理において複数の異なる複数の行列を選択的に適用する。行列としては、拡張Ｆｅｉｓｔｅｌ構造の各データ系列に入力するＦ関数に含まれる線形変換行列に基づくデータ系列対応の最小分岐数中から選択される全データ系列中の最小分岐数が予め定めた値以上となる条件を満足する複数の異なる行列が選択される。本発明によりＤＳＭに基づく線形解析や差分解析に対する耐性の高い共通鍵ブロック暗号が実現される。

明 細 書

暗号処理装置、暗号処理アルゴリズム構築方法、および暗号処理方法、並びにコンピュータ・プログラム

技術分野

[0001] 本発明は、暗号処理装置、暗号処理アルゴリズム構築方法、および暗号処理方法、並びにコンピュータ・プログラムに関する。さらに詳細には、Feistel型共通鍵ブロック暗号処理を実行する暗号処理装置、暗号処理アルゴリズム構築方法、および暗号処理方法、並びにコンピュータ・プログラムに関する。

背景技術

[0002] 昨今、ネットワーク通信、電子商取引の発展に伴い、通信におけるセキュリティ確保が重要な問題となっている。セキュリティ確保の1つの方法が暗号技術であり、現在、様々な暗号化手法を用いた通信が実際に行なわれている。

[0003] 例えばICカード等の小型の装置中に暗号処理モジュールを埋め込み、ICカードと、データ読み取り書き込み装置としてのリーダライタとの間でデータ送受信を行ない、認証処理、あるいは送受信データの暗号化、復号を行なうシステムが実用化されている。

[0004] 暗号処理アルゴリズムには様々なものがあるが、大きく分類すると、暗号化鍵と復号鍵を異なる鍵、例えば公開鍵と秘密鍵として設定する公開鍵暗号方式と、暗号化鍵と復号鍵を共通の鍵として設定する共通鍵暗号方式とに分類される。

[0005] 共通鍵暗号方式にも様々なアルゴリズムがあるが、その1つに共通鍵をベースとして複数の鍵を生成して、生成した複数の鍵を用いてブロック単位(64ビット, 128ビットなど)のデータ変換処理を繰り返し実行する方式がある。このような鍵生成方式とデータ変換処理を適用したアルゴリズムの代表的なものが共通鍵ブロック暗号方式である。

[0006] 代表的な共通鍵ブロック暗号のアルゴリズムとしては、例えば米国標準暗号としてのDES(Data Encryption Standard)アルゴリズムがあり、様々な分野において広く用いられている。

[0007] DESに代表される共通鍵ブロック暗号のアルゴリズムは、主として、入力データの変換を実行するラウンド関数部と、ラウンド関数(F関数)部の各ラウンドで適用する鍵を生成する鍵スケジュール部とに分けることができる。ラウンド関数部の各ラウンドで適用するラウンド鍵(副鍵)は、1つのマスター鍵(主鍵)に基づいて、鍵スケジュール部に入力されて生成され、各ラウンド関数部で適用される。

[0008] このようなラウンド関数を適用したアルゴリズムを実行する具体的な構造として、Feistel構造が知られている。Feistel構造はラウンド関数と呼ばれる変換関数の単純な繰り返しにより、平文を暗号文に変換する構造を持つ。Feistel構造を適用した暗号処理について記載した文献としては、例えば非特許文献1、非特許文献2がある。

[0009] しかし、例えばFeistel構造を適用する共通鍵暗号処理においては、暗号解析による鍵の漏洩が問題となっている。暗号解析または攻撃手法の代表的な手法として、ある差分を持つ入力データ(平文)とその出力データ(暗号文)を多数解析することにより各ラウンド関数における適用鍵を解析する差分解析(差分解読法または差分攻撃とも呼ばれる)や、平文と対応暗号文に基づく解析を行う線形解析(線形解読法または線形攻撃とも呼ばれる)が知られている。

[0010] 暗号解析による鍵の解析が容易であるということは、その暗号処理の安全性が低いということになる。従来の暗号アルゴリズムにおいては、ラウンド関数(F関数)部の線形変換部において適用する処理(変換行列)が、各段のラウンドにおいて等しいものであったため解析が行いやすく、結果として鍵の解析の容易性を招いていた。

[0011] このような問題に対処する構成として、Feistel構造のラウンド関数(F関数)部の線形変換部に2つ以上の異なる行列を配置する構成が提案された。この技術は拡散行列切り替え機構(DSM:Diffusion Switching Mechanism, 以下DSM)と呼ばれる。このDSMにより、差分攻撃や線形攻撃に対する耐性を向上させることが可能となる。

[0012] この拡散行列切り替え機構(DSM)は、通常の2つのデータ系列を持つFeistel構造に対する適用構成として示されている。一方、このような、一般的な2つのデータ系列を持つFeistel構造と異なり、3本以上のデータ系列を持つ拡張型のFeistel構造がある。しかし、このような3本以上のデータ系列を持つ拡張型のFeistel構造におい

て、上述の拡散行列切り替え機構(DSM)を適用して、差分攻撃や線形攻撃に対する耐性を向上させる構成についての開示はない。

非特許文献1:K. Nyberg, "Generalized Feistel networks", ASIACRYPT'96, Springer Verlag, 1996, pp.91--104.

非特許文献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

発明の開示

発明が解決しようとする課題

[0013] 本発明は、上記問題点に鑑みてなされたものであり、線形解析や差分解析に対する耐性の高い共通鍵ブロック暗号アルゴリズムを実現する暗号処理装置、暗号処理アルゴリズム構築方法、および暗号処理方法、並びにコンピュータ・プログラムを提供することを目的とする。

[0014] さらに具体的には、2つのデータ系列を持つFeistel構造を拡張したFeistel構造、すなわち、例えば3つ、4つなど、2以上の任意のデータ系列を持つ拡張型のFeistel構造において、複数の異なる線形変換行列を適用したラウンド関数部を設定して、線形解析や差分解析に対する耐性の高い共通鍵ブロック暗号アルゴリズムを実現する暗号処理装置、暗号処理アルゴリズム構築方法、および暗号処理方法、並びにコンピュータ・プログラムを提供することを目的とする。

課題を解決するための手段

[0015] 本発明の第1の側面は、

暗号処理装置であり、

非線形変換処理および線形変換処理を含むデータ変換処理を実行するSP型F関数を複数ラウンド繰り返すFeistel型共通鍵ブロック暗号処理を実行する暗号処理部を有し、

前記暗号処理部は、

データ系列数:dをd≧2の整数とした拡張Feistel構造を適用した暗号処理を実行する構成であり、各ラウンドにおけるF関数において実行する線形変換処理に、少な

くとも2以上の複数の異なる行列を選択的に適用する構成を有し、

前記2以上の複数の異なる行列は、拡張Feistel構造の各データ系列に入力するF関数に含まれる線形変換行列に基づくデータ系列対応の最小分岐数中から選択される全データ系列中の最小分岐数が予め定めた値以上となる条件を満足する複数の異なる行列であり、

前記複数の異なる行列を、拡張Feistel構造の各データ系列に入力するF関数に繰り返し配置した構成を有することを特徴とする暗号処理装置にある。

[0016] さらに、本発明の暗号処理装置の一実施態様において、前記暗号処理部において利用される前記複数の異なる行列は、拡張Feistel構造の各データ系列s(i)に入力する連続するk個(ただし、kは2以上の整数)のF関数に含まれる線形変換行列に基づいて算出されるデータ系列対応の最小分岐数[$B_k^D(s(i))$]中から選択される全データ系列中の最小分岐数[B_k^D]が3以上となる条件を満足する複数の異なる行列であることを特徴とする。

[0017] さらに、本発明の暗号処理装置の一実施態様において、前記暗号処理部において利用される前記複数の異なる行列は、拡張Feistel構造の各データ系列s(i)に入力する連続する2個のF関数に含まれる線形変換行列に基づいて算出されるデータ系列対応の最小分岐数[$B_2^D(s(i))$]中から選択される全データ系列中の最小分岐数[B_2^D]が3以上となる条件を満足する複数の異なる行列であることを特徴とする。

[0018] さらに、本発明の暗号処理装置の一実施態様において、前記暗号処理部において利用される前記複数の異なる行列は、拡張Feistel構造の各データ系列s(i)に入力する連続する2個のF関数に含まれる線形変換行列に基づいて算出されるデータ系列対応の最小分岐数[$B_2^L(s(i))$]中から選択される全データ系列中の最小分岐数[B_2^L]が3以上となる条件を満足する複数の異なる行列であることを特徴とする。

[0019] さらに、本発明の暗号処理装置の一実施態様において、前記暗号処理部は、前記複数の異なる行列を、n個(ただし、nは2以上の整数)の異なる行列、M_0, M_1, ・・M_{n-1}としたとき、これらの異なる行列M_0, M_1, ・・M_{n-1}を、拡張Feistel構造の各データ系列に入力するF関数に順番に繰り返し配置した構成を有することを特徴とする。

[0020] さらに、本発明の暗号処理装置の一実施態様において、前記暗号処理部は、1つ

のラウンドに1つのF関数のみを実行する拡張Feistel構造を適用した暗号処理を実行する構成であることを特徴とする。

[0021] さらに、本発明の暗号処理装置の一実施態様において、前記暗号処理部は、1つのラウンドに複数のF関数を並列に実行する拡張Feistel構造を適用した暗号処理を実行する構成であることを特徴とする。

[0022] さらに、本発明の暗号処理装置の一実施態様において、前記暗号処理部は、

a≧2の任意の整数、x≧1の任意の整数としたとき、前記複数の異なる行列による異なる線形変換処理を実行するa種類のF関数を利用したデータ系列数:d＝2axの拡張Fesitel構造を適用した暗号処理を実行する構成であり、

1つのラウンドにおいて、全種類(a種類)のF関数を均等にx個ずつ実行する構成であることを特徴とする。

[0023] さらに、本発明の暗号処理装置の一実施態様において、前記暗号処理部は、1つのラウンドにおいて並列に実行するax個のF関数を実行するF関数実行部と、前記F関数実行部に対するデータ入出力制御を実行する制御部とを備えた構成であることを特徴とする。

[0024] さらに、本発明の暗号処理装置の一実施態様において、前記暗号処理部は、前記複数の異なる行列による異なる線形変換処理を実行する複数のF関数実行部と、前記複数のF関数実行部の利用シーケンスを設定に応じて変更する制御部とを備え、前記制御部は、

(a)データ系列数d＝2としたFeistel構造による暗号処理、または、

(b1)データ系列数d≧2の任意数とした拡張Feistel構造であり、各ラウンドにおいて1つのF関数の実行のみを許容した暗号処理、または、

(b2)データ系列数d≧2の任意数とした拡張Feistel構造であり、各ラウンドにおいて複数のF関数の並列実行を許容した暗号処理、

上記(a),(b1),(b2)のいずれかの暗号処理を選択的に実行する構成であることを特徴とする。

[0025] さらに、本発明の暗号処理装置の一実施態様において、前記制御部は、暗号化または復号処理の対象となるデータのビット長に応じて、実行する処理形態を選択する

構成であることを特徴とする。

[0026] さらに、本発明の第2の側面は、

暗号処理装置において、暗号処理を実行する暗号処理方法であり、

暗号処理部において、非線形変換処理および線形変換処理を含むデータ変換処理を実行するSP型F関数を複数ラウンド繰り返すFeistel型共通鍵ブロック暗号処理を実行する暗号処理ステップを有し、

前記暗号処理ステップは、

データ系列数:dをd≧2の整数とした拡張Feistel構造を適用した暗号処理を実行するステップであり、各ラウンドにおけるF関数において実行する線形変換処理に、少なくとも2以上の複数の異なる行列を選択的に適用した演算を実行する演算ステップを有し、

前記演算ステップにおいて適用する複数の異なる行列は、拡張Feistel構造の各データ系列に入力するF関数に含まれる線形変換行列に基づくデータ系列対応の最小分岐数中から選択される全データ系列中の最小分岐数が予め定めた値以上となる条件を満足する複数の異なる行列であり、

前記演算ステップは、

拡張Feistel構造の各データ系列に入力するF関数において、前記複数の異なる行列に基づく線形変換演算を実行するステップであることを特徴とする暗号処理方法にある。

[0027] さらに、本発明の暗号処理方法の一実施態様において、前記複数の異なる行列は、拡張Feistel構造の各データ系列s(i)に入力する連続するk個(ただし、kは2以上の整数)のF関数に含まれる線形変換行列に基づいて算出されるデータ系列対応の最小分岐数[$B_k^D(s(i))$]中から選択される全データ系列中の最小分岐数[B_k^D]が3以上となる条件を満足する複数の異なる行列であることを特徴とする。

[0028] さらに、本発明の暗号処理方法の一実施態様において、前記複数の異なる行列は、拡張Feistel構造の各データ系列s(i)に入力する連続する2個のF関数に含まれる線形変換行列に基づいて算出されるデータ系列対応の最小分岐数[$B_2^D(s(i))$]中から選択される全データ系列中の最小分岐数[B_2^D]が3以上となる条件を満足する

複数の異なる行列であることを特徴とする。

[0029] さらに、本発明の暗号処理方法の一実施態様において、前記複数の異なる行列は、拡張Feistel構造の各データ系列s(i)に入力する連続する2個のF関数に含まれる線形変換行列に基づいて算出されるデータ系列対応の最小分岐数[$B_2^L(s(i))$]中から選択される全データ系列中の最小分岐数[B_2^L]が3以上となる条件を満足する複数の異なる行列であることを特徴とする。

[0030] さらに、本発明の暗号処理方法の一実施態様において、前記複数の異なる行列を、n個(ただし、nは2以上の整数)の異なる行列、M_0, M_1, ・・M_{n-1}としたとき、前記演算ステップは、拡張Feistel構造の各データ系列に入力するF関数において、これらの異なる行列M_0, M_1, ・・M_{n-1}を順番に繰り返し実行するステップであることを特徴とする。

[0031] さらに、本発明の暗号処理方法の一実施態様において、前記暗号処理ステップは、1つのラウンドに1つのF関数のみを実行する拡張Feistel構造を適用した暗号処理を実行するステップであることを特徴とする。

[0032] さらに、本発明の暗号処理方法の一実施態様において、前記暗号処理ステップは、1つのラウンドに複数のF関数を並列に実行する拡張Feistel構造を適用した暗号処理を実行するステップであることを特徴とする。

[0033] さらに、本発明の暗号処理方法の一実施態様において、前記暗号処理ステップは、

a≧2の任意の整数、x≧1の任意の整数としたとき、前記複数の異なる行列による異なる線形変換処理を実行するa種類のF関数を利用したデータ系列数:d=2axの拡張Fesitel構造を適用した暗号処理を実行するステップであり、

1つのラウンドにおいて、全種類(a種類)のF関数を均等にx個ずつ実行することを特徴とする。

[0034] さらに、本発明の暗号処理方法の一実施態様において、前記暗号処理ステップは、1つのラウンドにおいて並列に実行するax個のF関数を実行するF関数実行部を適用して、前記F関数実行部に対するデータ入出力制御を実行する制御部の制御に従った暗号処理を実行するステップであることを特徴とする。

[0035] さらに、本発明の暗号処理方法の一実施態様において、前記暗号処理ステップは、前記複数の異なる行列による異なる線形変換処理を実行する複数のF関数実行部と、前記複数のF関数実行部の利用シーケンスを設定に応じて変更する制御部とによって暗号処理を実行し、前記制御部の制御によって、

(a)データ系列数d＝2としたFeistel構造による暗号処理、または、

(b1)データ系列数d≧2の任意数とした拡張Feistel構造であり、各ラウンドにおいて1つのF関数の実行のみを許容した暗号処理、または、

(b2)データ系列数d≧2の任意数とした拡張Feistel構造であり、各ラウンドにおいて複数のF関数の並列実行を許容した暗号処理、

上記(a)，(b1)，(b2)のいずれかの暗号処理を選択的に実行することを特徴とする。

[0036] さらに、本発明の暗号処理方法の一実施態様において、前記制御部は、暗号化または復号処理の対象となるデータのビット長に応じて、実行する処理形態を選択することを特徴とする。

[0037] さらに、本発明の第3の側面は、

情報処理装置において暗号処理アルゴリズムを構築する暗号処理アルゴリズム構築方法であり、

情報処理装置における制御部が、データ系列数：dをd≧2の整数とした拡張Feistel構造を適用した暗号処理アルゴリズムの構成において、各ラウンドにおけるF関数において実行する線形変換処理に適用する少なくとも2以上の複数の異なる行列を決定する行列決定ステップと、

前記制御部が、前記行列決定ステップにおいて決定した複数の異なる行列を、拡張Feistel構造の各データ系列に入力するF関数に繰り返し配置する行列設定ステップを有し、

前記行列決定ステップは、

前記2以上の複数の異なる行列として、拡張Feistel構造の各データ系列に入力するF関数に含まれる線形変換行列に基づくデータ系列対応の最小分岐数中から選択される全データ系列中の最小分岐数が予め定めた値以上となる条件を満足する

複数の異なる行列を適用行列として決定する処理を実行するステップであることを特徴とする暗号処理アルゴリズム構築方法にある。

[0038] さらに、本発明の第4の側面は、

暗号処理装置において、暗号処理を実行させるコンピュータ・プログラムであり、

暗号処理部において、非線形変換処理および線形変換処理を含むデータ変換処理を実行するSP型F関数を複数ラウンド繰り返すFeistel型共通鍵ブロック暗号処理を実行させる暗号処理ステップを有し、

前記暗号処理ステップは、

データ系列数:dをd≧2の整数とした拡張Feistel構造を適用した暗号処理を実行させるステップであり、各ラウンドにおけるF関数において実行する線形変換処理に、少なくとも2以上の複数の異なる行列を選択的に適用した演算を実行する演算ステップを含み、

前記演算ステップにおいて適用する複数の異なる行列は、拡張Feistel構造の各データ系列に入力するF関数に含まれる線形変換行列に基づくデータ系列対応の最小分岐数中から選択される全データ系列中の最小分岐数が予め定めた値以上となる条件を満足する複数の異なる行列であり、

前記演算ステップは、

拡張Feistel構造の各データ系列に入力するF関数において、前記複数の異なる行列に基づく線形変換演算を実行するステップであることを特徴とするコンピュータ・プログラムにある。

[0039] さらに、本発明の第5の側面は、

情報処理装置において暗号処理アルゴリズムを構築させるコンピュータ・プログラムであり、

情報処理装置における制御部に、データ系列数:dをd≧2の整数とした拡張Feistel構造を適用した暗号処理アルゴリズムの構成において、各ラウンドにおけるF関数において実行する線形変換処理に適用する少なくとも2以上の複数の異なる行列を決定させる行列決定ステップと、

前記制御部に、前記行列決定ステップにおいて決定した複数の異なる行列を、拡

張Feistel構造の各データ系列に入力するF関数に繰り返し配置させる行列設定ステップを有し、

前記行列決定ステップは、

前記2以上の複数の異なる行列として、拡張Feistel構造の各データ系列に入力するF関数に含まれる線形変換行列に基づくデータ系列対応の最小分岐数中から選択される全データ系列中の最小分岐数が予め定めた値以上となる条件を満足する複数の異なる行列を適用行列として決定する処理を実行するステップであることを特徴とするコンピュータ・プログラムにある。

[0040] なお、本発明のコンピュータ・プログラムは、例えば、様々なプログラム・コードを実行可能なコンピュータ・システムに対して、コンピュータ可読な形式で提供する記憶媒体、通信媒体、例えば、CDやFD、MOなどの記録媒体、あるいは、ネットワークなどの通信媒体によって提供可能なコンピュータ・プログラムである。このようなプログラムをコンピュータ可読な形式で提供することにより、コンピュータ・システム上でプログラムに応じた処理が実現される。

[0041] 本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。なお、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

発明の効果

[0042] 本発明の一実施例の構成によれば、非線形変換部および線形変換部を有するSPN型のF関数を、複数ラウンド繰り返し実行するFeistel型共通鍵ブロック暗号処理において、2つのデータ系列を持つFeistel構造を拡張したFeistel構造、すなわち、例えば3つ、4つなど、2以上の任意のデータ系列を持つ拡張型のFeistel構造において、複数の異なる線形変換行列を適用したラウンド関数部を設定することで拡散行列切り替え機構(DSM)を実現し、線形解析や差分解析に対する耐性の高い共通鍵ブロック暗号アルゴリズムの構築および暗号処理の実行が可能となる。

[0043] 本発明の一実施例の構成によれば、データ系列数:dをd≧2の整数とした拡張Feistel構造を適用した暗号処理を実行する構成において、各ラウンドにおけるF関数に

おいて実行する線形変換処理に、少なくとも2以上の複数の異なる行列を選択的に適用する構成を有し、2以上の複数の異なる行列として、拡張Feistel構造の各データ系列に入力するF関数に含まれる線形変換行列に基づくデータ系列対応の最小分岐数中から選択される全データ系列中の最小分岐数が予め定めた値以上となる条件を満足する複数の異なる行列として設定することで、拡散行列切り替え機構(DSM)を実現し、線形解析や差分解析に対する耐性の高い共通鍵ブロック暗号アルゴリズムの構築および暗号処理の実行が可能となる。

[0044] さらに、本発明の一実施例の構成によれば、複数の異なる行列による異なる線形変換処理を実行するa(a≧2)種類のF関数を利用したデータ系列数:d=2axの拡張Fesitel構造(x≧1)を適用した暗号処理を実行する構成において、1つのラウンドにおいて、全種類(a種類)のF関数を均等にx個ずつ実行する構成としたので、無駄な回路を設けることのない小型の暗号処理装置が実現される。

[0045] さらに、本発明の一実施例の構成によれば、複数の異なる行列による異なる線形変換処理を実行する複数のF関数実行部を構成して、複数のF関数実行部の利用シーケンスを設定に応じて変更する構成としたことで、

(a)データ系列数d=2としたFeistel構造による暗号処理、または、

(b1)データ系列数d≧2の任意数とした拡張Feistel構造であり、各ラウンドにおいて1つのF関数の実行のみを許容した暗号処理、または、

(b2)データ系列数d≧2の任意数とした拡張Feistel構造であり、各ラウンドにおいて複数のF関数の並列実行を許容した暗号処理、

上記(a),(b1),(b2)のいずれかの暗号処理を選択的に実行することを可能とした暗号処理装置が実現される。

図面の簡単な説明

[0046] [図1]Feistel構造を持つ代表的な共通鍵ブロック暗号の構成を示す図である。

[図2]ラウンド関数部として設定されるF関数の構成について説明する図である。

[図3]2つの異なる線形変換行列を利用したFeistel型暗号アルゴリズムについて説明する図である。

[図4]3つの異なる線形変換行列を利用したFeistel型暗号アルゴリズムについて説

明する図である。

[図5]拡張Feistel構造の定義について説明する図である。

[図6]7つのデータ系列(d＝7)を持つ拡張Feistel構造例を示す図である。

[図7]拡張Feistel構造の各構成部および各構成部の入出力データの定義について説明する図である。

[図8]拡張Feistel構造のタイプ1に対するDSMの適用について説明する図である。

[図9]拡張Feistel構造のタイプ2に対するDSMの適用について説明する図である。

[図10]拡張Feistel構造のタイプ1に対するDSMの適用について説明する図である。

[図11]拡張Feistel構造のタイプ2に対するDSMの適用について説明する図である。

[図12]拡張Feistel構造の実装効率を高めた構成について説明する図である。

[図13]拡張Feistel構造の実装効率を高めたハードウェア構成例について説明する図である。

[図14]3種類のF関数を効率的な実装とするための配置例について説明する図である。

[図15]データ系列d＝2のFeistel構造とした2mnビットのブロック暗号構成を示す図である。

[図16]拡散行列切り替え機構(DSM)を満足するデータ系列数d＝4の拡張Feistel構造を示す図である。

[図17]異なるビット数のブロック暗号を実行することを可能とした回路共有構成について説明する図である。

[図18]3種類のF関数F1, F2, F3のF関数を適用したデータ系列d＝2のFeistel構造について説明する図である。

[図19]3種類のF関数F1, F2, F3を実行する暗号処理装置の構成例について説明する図である。

[図20]本発明に係る暗号処理を実行する暗号処理装置としてのICモジュールの構成例を示す図である。

発明を実施するための最良の形態

[0047] 以下、本発明の暗号処理装置、および暗号処理方法、並びにコンピュータ・プログラムの詳細について説明する。説明は、以下の項目に従って行なう。

1. SP型F関数を持つFeistel構造

2. 分岐数演算関数と耐性評価関数

2－1. 分岐数演算関数:Branch()

2－2. 差分攻撃に対する耐性評価指標

2－3. 線形攻撃に対する耐性評価指標

3. 2つのデータ系列を持つFeistel構造に対するDSMの設定法

4. 拡張Feistel構造におけるDSMの設定

4－1. 拡張Feistel構造について

4－2. 拡張Feistel構造において差分攻撃に対する耐性を向上させるための構成

4－2－1. 最小分岐数B_2^Dの値を3以上とするF関数中の行列選択構成

4－2－2. 最小分岐数B_k^Dの値を3以上とするF関数中の行列選択構成

4－3. 拡張Feistel構造において線形攻撃に対する耐性を向上させるための構成

4－3－1. 最小分岐数B_2^Lの値を3以上とするF関数中の行列選択構成

5. 特定の形を持つ拡張Feistel構造に対するDSMの利用構成

5－1. 拡張Feistel構造のタイプ1に対するDSMの適用

5－2. 拡張Feistel構造のタイプ2に対するDSMの適用

6. 拡張Feistel構造各タイプのアクティブS－box数と、F関数中の線形変換行列に基づく最小分岐数との関係式の証明

6－1. 拡張Feistel構造のタイプ1のアクティブS－box数と、F関数中の線形変換行列に基づく最小分岐数との関係式の証明

6－2. 拡張Feistel構造のタイプ2のアクティブS－box数と、F関数中の線形変換行列に基づく最小分岐数との関係式の証明

7. F関数の設定および利用処理の工夫に基づく実装における改良構成

7－1. 拡張Feistelのタイプ2の効率的なF関数配置方法

7－2. Feistel構造と拡張Feistel構造における部品の共通化

8. 本発明の暗号処理および暗号アルゴリズム構築処理のまとめ

9. 暗号処理装置の構成例

[0048] [1. SP型F関数を持つFeistel構造]

まず、SP型F関数を持つFeistel構造について説明する。共通鍵ブロック暗号のデザインとして、Feistel構造が知られている。Feistel構造はラウンド関数と呼ばれる基本処理単位の繰り返しにより、平文を暗号文に変換する構造を持つ。

[0049] 図1を参照して、Feistel構造の基本構成について説明する。図1には、rラウンドのラウンド数＝rを持つ2つのデータ系列を持つFeistel構造の例を示している。なお、ラウンド数rは、設計の段階で決定されるパラメータであり、例えば入力される鍵の長さに応じて変更可能な値である。

[0050] 図1に示すFeistel構造において、暗号化対象として入力される平文の長さを2mnビットとする。ただし、m, nは共に整数である。初めに、2mnビットの平文を、mnビットの2つの入力データP_L(Plain-Left)101, P_R(Plain-Right)102に分割し、これを入力値とする。

[0051] Feistel構造はラウンド関数とよばれる基本処理単位の繰り返しで表現され、各ラウンドに含まれるデータ変換関数はF関数120と呼ばれる。図1の構成では、F関数(ラウンド関数)120がr段繰り返された構成例を示している。

[0052] 例えば第1番目のラウンドでは、mnビットの入力データXと、鍵生成部(図示せず)から入力されるmnビットのラウンド鍵$K_1$103がF関数120に入力され、F関数120におけるデータ変換処理の後にmnビットのデータYを出力する。出力はもう片方の前段からの入力データ(第1段の場合は入力データP_L)と排他的論理和部104において、排他的論理和演算がなされ、mnビットの演算結果が次のラウンド関数へと出力される。この処理、すなわちF関数を定められたラウンド数(r)だけ繰り返し適用して暗号化処理が完了し、暗号文の分割データC_L(Cipher-Left)、C_R(Cipher-Right)が出力される。以上の構成より、Feistel構造の復号処理はラウンド鍵を挿入する順序を逆にするだけでよく、逆関数を構成する必要がないことが導かれる。

[0053] 各ラウンドの関数として設定されるF関数120の構成について、図2を参照して説明する。図2(a)は、1つのラウンドにおけるF関数120に対する入力および出力を示す

図であり、図2(b)は、F関数120の構成の詳細を示す図である。F関数120は、図2(b)に示すように、非線形変換層(S層)と線形変換層(P層)を接続したいわゆるSP型の構成を有する。

[0054] 図2に示すF関数120は、入出力ビット長がm×n(m, n:整数)ビットの設定を持つ関数である。SP型F関数内部では初めに鍵データK_iとデータX_iとの排他的論理和が実行され、次に非線形変換層(S層)が適用され、続いて線形変換層(P層)が適用される。

[0055] 具体的には非線形変換層(S層)は、Sボックス(S－box)121と呼ばれるnビット入力nビット出力の非線形変換テーブルがm個並んだものであり、mnビットのデータはnビットずつ分割されてそれぞれ対応するSボックス(S－box)121に入力されデータが変換される。各Sボックスでは、例えば変換テーブルを適用した非線形変換処理が実行される。

[0056] 線形変換層(P層)は線形変換部122によって構成され、線形変換部122は、Sボックス121からの出力データであるmnビットの出力値Zを入力し、この入力に対して線形変換を施しmnビットの結果を出力する。線形変換部122は、入力ビット位置の入れ替え処理などの線形変換処理を実行して、mnビットの出力値Yを出力する。この出力値Yが前段からの入力データと排他的論理和され、次のラウンドのF関数の入力値とされる。

[0057] なお、以下に説明する本実施例の構成では、線形変換層(P層)としての線形変換部122において実行する線形変換はGF(2)上で定義されるmn×mnの行列を適用して行なわれる線形変換であると定義し、また、第iラウンド目に含まれる行列をM_iと呼ぶものとする。なお、本発明において説明する構成における非線形変換部としてのSボックスと、線形変換は、いずれも全単射であるものとする。

[0058] [2. 分岐数演算関数と耐性評価関数]

次に、本発明を理解するために必要となる分岐数演算関数と耐性評価関数について説明する。

(2－1. 分岐数演算関数:Branch())

上述したF関数内の線形変換層(P層)としての線形変換部122において実行され

る線形変換の例としての最適拡散変換(Optimal Diffusion Mappings)の分岐数演算関数:Branch()を以下のように定義する。

[0059] n×aビットデータからn×bビットデータへの線形変換を行う写像、

$\theta : \{0, 1\}^{na} \rightarrow \{0, 1\}^{nb}$

に対して分岐数:$Branch_n(\theta)$を次のように定義する。

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

ただし、$\min_{\alpha \neq 0}\{X_\alpha\}$は、$\alpha \neq 0$を満たすすべての$X_\alpha$のうちの最小値を表すものとし、$hw_n(Y)$はビット列Yをnビットごとに区切って表したときに、nビットのデータすべてが0ではない(非ゼロ)要素の数を返す関数とする。

なお、このとき、$Branch_n(\theta)$がb+1であるような写像θを最適拡散変換と定義する。

[0060] (2－2. 差分攻撃に対する耐性評価指標)

Feistel構造を適用する共通鍵暗号処理においては、暗号解析による鍵の漏洩が問題となる。暗号解析または攻撃手法の代表的な手法として、ある差分(ΔX)を持つ入力データ(平文)とその出力データ(暗号文)を多数解析することにより各ラウンド関数における適用鍵を解析する差分解析(差分解読法または差分攻撃とも呼ばれる)や、平文と対応暗号文に基づく解析を行う線形解析(線形解読法または線形攻撃とも呼ばれる)が知られている。

[0061] 差分攻撃に対する耐性を図る指標として、差分の接続関係を表現した差分パスに含まれる差分アクティブS－boxの最小数が適用可能である。

差分パスとは、暗号化関数中の鍵データを除くすべてのデータ部分に対して特定の差分値を指定したものである。差分値は自由に決められるものではなく変換処理の前後の差分値は互いに関連しあっている。線形変換処理の前後では、入力差分と出力差分の関係は一対一に決定される。非線形変換の前後では、入力差分と出力差分の関係は一対一にはきまらないが、確率という概念が導入される。ある入力差分と出力差分に対する確率は事前に計算することができるものとする。すべての出力に対する確率をすべて足し合わせると1となっている。

[0062] SP型のF関数を持ったFeistel構造においては、非線形変換はS－boxによる処理

の部分のみである。したがって、この場合、0以外の確率をもつ差分パスとは平文(入力)に対する差分値から始まって暗号文(出力)の差分値までに至る差分データの集合であり、すべてのS－boxの前後で与えられる差分値は0以外の確率をもつものである。0以外の確率をもつある差分パスのS－boxに入力される差分値が0でないものを差分アクティブS－boxと呼ぶものとする。0以外の確率を持つすべての差分パスのアクティブS－boxの数のうちで最も少ない数を最小差分アクティブS－box数とよび、この数値が差分攻撃に対する安全性指標として知られている。なお、すべての差分値が0であるような差分パスは、確率が1となり攻撃として意味をなさないので、以降では考慮しない。

[0063] 本発明の一実施例においては、この最小差分アクティブS－box数を大きく保証することにより差分攻撃に対する安全性を高める構成を持つ。

[0064] (2－3. 線形攻撃に対する耐性評価指標)

さらに、線形攻撃に対する耐性を図る指標として、線形マスクの接続関係を表現した線形パス(線形近似と呼ばれることが多いが、差分と対応させるためここではパスという言葉を用いる)に含まれる線形アクティブS－boxの最小数が適用可能である。

[0065] 線形パスとは、暗号化関数中の鍵データを除くすべてのデータ部分に対して特定の線形マスク値を指定したものである。線形マスク値は自由に決められるものではなく変換処理の前後の線形値は互いに関連しあっている。線形変換処理の前後では、入力線形マスク値と出力線形マスク値の関係は一対一に決定される。非線形変換の前後では、入力線形マスク値と出力線形マスク値の関係は一対一にはきまらないが、確率という概念が導入される。入力線形マスク値に対して、出力されうるひとつ以上の線形マスク値の集合が存在し、それぞれが出力される確率を事前に計算することができる。すべての出力に対する確率をすべて足し合わせると1となっている。

[0066] SP型のF関数を持ったFeistel構造においては、非線形変換はS－boxによる処理の部分のみである。したがって、この場合、0以外の確率をもつ線形パスとは平文(入力)に対する線形値から始まって暗号文(出力)の線形値までに至る線形マスク値データの集合であり、すべてのS－boxの前後で与えられる線形値は0以外の確率をもつものである。0以外の確率をもつある線形パスのS－boxに入力される線形値が0

でないものを線形アクティブS－boxと呼ぶものとする。0以外の確率を持つすべての線形パスのアクティブS－boxの数のうちで最も少ない数を最小線形アクティブS－box数とよび、この数値が線形攻撃に対する安全性指標として知られている。なお、すべての線形マスク値が0であるような線形パスは、確率が1となり攻撃として意味をなさないので、以降では考慮しない。

[0067] 本発明の一実施例においては、この最小線形アクティブS－box数を大きく保証することにより線形攻撃に対する安全性を高める。

[0068] [3. 2つのデータ系列を持つFeistel構造に対するDSMの設定法]

先に説明したように、Feistel構造を適用した暗号処理において、上述した差分攻撃や線形攻撃に対する耐性を高める構成として、拡散行列切り替え機構(DSM:Diffusion Switching Mechanism, 以下DSM)を適用した構成が提案されている。DSMは、Feistel構造のラウンド関数(F関数)部の線形変換部に2つ以上の異なる行列を配置する構成である。このDSMにより、最小線形アクティブS－box数を大きく保証することが可能となり、差分攻撃や線形攻撃に対する耐性を向上させることが可能となる。

[0069] このDSMについて、その概要を説明する。Feistel構造において、拡散行列切り替え機構(DSM)を適用した場合、Feistel構造を構成するラウンド関数(F関数)部の線形変換部(P層)において適用する行列は、複数の異なる行列となる。例えば、図1に示すようなrラウンドのFeistel構造の各ラウンドにおける適用行列は、全て同じ線形変換行列として設定されるのではなく、少なくとも2種類以上の行列が、特定の規則に従って配列されることになる。

[0070] 例えば、2つの線形変換行列M_0, M_1によって、拡散行列切り替え機構(DSM)を実現したFeistel構造例を図3に、3つの線形変換行列M_0, M_1, M_2によって、拡散行列切り替え機構(DSM)を実現したFeistel構造例を図4に示す。

[0071] 図3に示すFeistel構造例において、2つの線形変換行列M_0, M_1は、異なる行列によって構成される。また、図4に示すFeistel構造例においては、3つの線形変換行列M_0, M_1, M_2は、異なる行列によって構成される。

[0072] 拡散行列切り替え機構(DSM)を実現するためには、適用する行列が所定の条件

を満たすことが必要となる。この条件の1つが、上述した分岐数（Branch）に関する制約である。以下、この制約について説明する。

[0073] Feistel構造におけるラウンド関数部の線形変換に適用する複数の異なる行列M_0～M_nそれぞれの分岐数において、

適用行列中の分岐数の最小値：B_1^Dと、

適用する複数の行列の結合行列に対応する分岐数の最小値：B_2^D, B_3^D, B_2^L

を以下のように定義する。

[数1]

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

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

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

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

[0074] 上記式において、

M_iは、Feistel構造における第iラウンドの線形変換処理に適用する線形変換行列を示し、

$[M_i \mid M_{i+2} \mid \cdot\cdot]$は、$M_i \mid M_{i+2} \mid \cdot\cdot$各行列の連結により得られる結合行列を示し、

${}^tM$は、行列Mの転値行列、M^{-1}は、行列Mの逆行列を示す。

[0075] 上記式において、：B_2^D, B_3^D, B_2^Lは、具体的には、Feistel構造における1つ飛びで連続する2ラウンドもしくは3ラウンドのF関数に含まれる行列を結合した行列の分岐数の最小値を表している。

[0076] 例えば、上記の各分岐数が以下の条件、すなわち、

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

上記条件を満足させるように各行列を設定することで、Feistel構造において、差分攻撃や線形攻撃に対する耐性を向上させることが出来ることが知られている。

なお、B_1^D, B_2^D, B_3^D, B_2^Lにおける各添え字は以下の意味を持つものである。

B_n^Dのnは結合する行列数、B_n^DのDは差分攻撃(Differential Attack)に対する耐性を持つための条件であることを示し、B_n^LのLは線形攻撃(Linear Attack)に対する耐性を持つための条件であることを示している。

[0077] [4. 拡張Feistel構造におけるDSMの設定]

本発明では、2つのデータ系列を持つFeistel構造ではなく、例えば3系列や、4系列など2以上の任意のデータ系列を持つFeistel構造に対して拡散行列切り替え機構(DSM)を実現する構成を提案する。以下、この構成について、詳細に説明する。

[0078] 本発明において取り扱うのはSP型のF関数を使う点では上記の2つのデータ系列を持つFeistel構造と同じであるが、データ系列数の分割数を一般化してdとした拡張Feistel構造を対象とする。ただしdは2以上の整数である。

[0079] 上述したように、データ系列数＝2に限定したFeistel構造に対するDSMの適用構成については提案されていたが、データ系列数dをd≧2とした任意数のdを持つ拡張Feistel構造に対して、DSMを適用して耐性を向上させる方法が知られていなかった。本発明は、d≧2とした任意数のデータ系列数dを持つ拡張Feistel構造に対して拡散行列切り替え機構(DSM)を適用して差分攻撃や線形攻撃に対する耐性を向上させる構成を実現するものである。

以下、本発明の具体的構成および処理例について説明する。

[0080] (4－1. 拡張Feistel構造について)

以下、拡張Feistel構造の定義について、図5を参照して説明する。本明細書では拡張Feistel構造を以下のように定義する。

1. d本(dは2以上)のデータ系列をもち、各データ系列のサイズはmnビット。

2. F関数の入出力サイズはmnビット。

3. ラウンドという処理単位をもち、ラウンド内では一つまたは複数のデータ系列に対してF関数による変換処理が施され、その結果は別のデータ系列に排他的論理和がなされる。ただし、2つ以上のF関数が1ラウンド内に含まれる場合はすべてのF関数の入出力となるデータ系列には重複する系列が存在しないものとする。

[0081] 上記の定義によって構築される拡張Feistel構造の例を図5を参照して説明する。

上記定義1．d本（dは2以上）のデータ系列をもち、各データ系列のサイズはmnビット。

この定義について図5を参照して説明する。図5において、データ系列1～dの各々の各データ系列の入出力サイズがmnビットであり、入出力の総ビット数はdmnビットであることを意味している。

[0082] 上記定義2．F関数の入出力サイズはmnビット。

この定義について図5を参照して説明する。例えばF関数202にはデータ系列2から上段の排他的論理和（XOR）演算部201から演算結果としてのmnビットが入力され、さらに、ラウンド鍵Kが入力されて演算処理が実行される。この演算処理は、図2（b）を参照して説明した処理であり、Sボックスにおける非線形変換と、線形変換部における線形変換行列Miを適用した線形変換処理が含まれる。F関数202の出力はmnビットであり、データ系列4の排他的論理和（XOR）演算部203に入力される。

[0083] 上記定義3．ラウンドという処理単位をもち、ラウンド内では一つまたは複数のデータ系列に対してF関数による変換処理が施され、その結果は別のデータ系列に排他的論理和がなされる。ただし、2つ以上のF関数が1ラウンド内に含まれる場合はすべてのF関数の入出力となるデータ系列には重複する系列が存在しないものとする。

この定義について図5を参照して説明する。図5にはrラウンドの構成を持つ拡張Feistel構造を示している。各ラウントには1つ以上のF関数が含まれ、その結果は別のデータ系列に排他的論理和がなされる。図5に示すラウンドnは、複数のF関数が1ラウンド内に含まれる。図5に示すF関数211とF関数212である。

[0084] このように、1つのラウンドに複数のF関数が含まれる場合、各F関数の入出力系列は、それぞれ異なるデータ系列であり、重複したデータ系列が入出力系列として適用されない設定とする。

図5に示すF関数211の入力データ系列はデータ系列1、出力データ系列はデータ系列2であり、

F関数212の入力データ系列はデータ系列5以上のいずれか、出力データ系列はデータ系列3であり、

いずれの入出力データ系列も重複しない設定とされる。

[0085] なお、図5にも示すように、本明細書では、F関数は[F]、ラウンド鍵は[K]として示す。これらの各識別子F，Kに設定した添え字は以下の意味を持つ。

F_i^n、K_i^nのiはラウンドを示し、nは、同一ラウンドにおけるF関数またはラウンド鍵の識別番号を示す。

なお、図には示していないが、以下の説明において、各ラウンドにおけるF関数の線形変換部において適用される線形変換行列は[M]として示し、Mに設定する添え字も上記と同様、

M_i^nのiはラウンドを示し、nは、同一ラウンドに設定された複数のF関数各々に対応する線形変換行列の識別番号を示すものとする。

[0086] 図6は、上述の定義を満足する7つのデータ系列(d＝7)を持つ拡張Feistel構造例を表したものである。なお、図6においては、各F関数の出力と、各データ系列との排他的論理和演算(XOR)部の記号を省略しているが、各F関数の出力と、各データ系列と各交差ポイントでは、それぞれの入力による排他的論理和演算(XOR)が実行され、その排他的論理和演算(XOR)結果が同一データ系列の下方向に出力される構成である。図6に示す例では、ラウンドi＋4、ラウンドi＋5、ラウンドi＋9、ラウンドi＋10が一つのラウンドに2つ以上のF関数が含まれるラウンドであり、これらのラウンドに示すF関数[F]と、ラウンド鍵[K]は、同一ラウンドにおけるF関数またはラウンド鍵の識別番号を示す番号が右上に示されている。

[0087] 上記定義1～3に従って、系列数dをd＝2としたFeistel構造を構築すると、2本のデータ系列からなるFeistel構造、すなわち、先に図1を参照して説明したFeistel構造となる。すなわち、2本の各データ系列交互にF関数が行き来するような結線構造になるが、3本以上のデータ系列を持つ拡張Feistel構造の場合はF関数の入力と出力として選ばれるデータ系列が複数存在するため結線構造が一意に定まることはない。つまり拡張Feistel構造ではdが大きくなればなるほど、F関数の設置場所の自由度が指数関数的に増大することとなる。

[0088] 本発明では、このような拡張Feistel構造において、差分攻撃や線形攻撃に対する耐性を向上させる拡散行列切り替え機構(DSM：Diffusion Switching Mechanism)を実現する構成を提案する。

[0089] 系列数dをd＝2としたFeistel構造では、例えば、図3や図4に示したように、Feistel構造を構成するラウンド関数（F関数）部の線形変換部（P層）において適用する行列を、2つの異なる線形変換行列M_0，M_1、あるいは、3つの異なる線形変換行列M_0，M_1，M_2とすることなどでDSMが実現される。ただし、DSMを実現するためには、適用する行列が所定の条件を満たすことが必要となる。この条件の1つが、前述した分岐数（Branch）に関する制約である。

[0090] データ系列数dを、

d：d≧2の任意の整数

とした拡張Feistel構造において、DSMを実現する構成の説明の前に、以下の説明において使用する拡張Feistel構造の各構成部および各構成部の入出力データの定義について、図7を参照して説明する。

図7は、例えば図6に示すような拡張Feistel構造を構成する1つのデータ系列のみを抽出して示す図である。図7に示すように、ある1つのデータ系列への入力データは1回以上のF関数の出力が排他的論理和（XOR）されて出力に至っていることがわかる。このことは拡張Feistel構造に含まれる任意のデータ系列にあてはまる。

[0091] 図7では、一本のデータ系列[s(i)]に対して複数のF関数[$F_{s(i),1}$，$F_{s(i),2}$，...]の出力が排他的論理和演算（XOR）により足しあわされていく様子を表している。

なお、拡張Feistel構造中のd本あるデータ系列を、それぞれs(i)（1≦i≦d）とし、データ系列s(i)に入力するF関数を、データ系列s(i)の入力に近い方から$F_{s(i),1}$，$F_{s(i),2}$，...と名づけることとする。

またデータ系列s(i)の入力データを$W_{s(i),0}$とし、

F関数$F_{s(i),j}$の出力が排他的論理和された後のデータを$W_{s(i),j}$とする。

また、F関数$F_{s(i),j}$への入力データを$X_{s(i),j}$とする。

各Xs(i)，jは、データ系列s(i)以外の別の系列に属するデータであるが、ここではそれらがどこの系列に属しているかは問わないものとする。

このとき、拡張Feistel構造は、このようなd本のデータ系列が相互に接続されて構成されるものと考えることができる。

[0092] 拡張Feistel構造において、DSMを実現するための構成

以下、d:d≧2の任意の整数

とした拡張Feistel構造において、DSMを実現するための構成について説明する。説明は、

(4－2)拡張Feistel構造において差分攻撃に対する耐性を向上させるための構成

(4－3)拡張Feistel構造において線形攻撃に対する耐性を向上させるための構成

これらの各構成について、順次、説明する。

[0093] (4－2. 拡張Feistel構造において差分攻撃に対する耐性を向上させるための構成)

まず、拡張Feistel構造において差分攻撃に対する耐性を向上させるための構成について説明する。

前述したように、差分攻撃は、ある差分(ΔX)を持つ入力データ(平文)とその出力データ(暗号文)を多数解析することにより各ラウンド関数における適用鍵を解析する攻撃であり、差分攻撃に対する耐性を図る指標として、差分の接続関係を表現した差分パスに含まれる差分アクティブS－boxの最小数が適用される。差分パスは、暗号化関数中の鍵データを除くデータ部分における差分値である。線形変換処理の前後では、入力差分と出力差分の関係は一対一に決定され、非線形変換処理の前後では、一対一とはならないが、ある入力差分に対する出力差分の出現確率が算出される。すべての出力に対する確率をすべて足し合わせると1となる。

[0094] SP型のF関数を持ったFeistel構造においては、非線形変換はS－boxのみである。この場合、0以外の確率をもつ差分パスは平文(入力)に対する差分値から始まって暗号文(出力)の差分値までに至る差分データの集合であり、すべてのS－boxの前後で与えられる差分値は0以外の確率をもつ。0以外の確率をもつある差分パスのS－boxに入力される差分値が0でないものを差分アクティブS－boxと呼ぶ。0以外の確率を持つすべての差分パスのアクティブS－boxの数のうちで最も少ない数を最小差分アクティブS－box数とよび、この数値が差分攻撃に対する安全性指標として用いられる。

[0095] 最小差分アクティブS－box数を大きくすることが、差分攻撃に対する耐性の向上をもたらす。以下では、データ系列数dをd≧2の任意整数とした拡張Feistel構造にお

いて、最小差分アクティブS－box数の数を大きくするDSM構造を構築する手法について説明する。

[0096] 拡張Feistel構造に含まれるF関数[$F_{s(i),x}$]で用いられる線形変換行列を[$M_{s(i),x}$]とする。このとき、分岐数演算関数:Branch()を適用した分岐数の算出式$B_2^D(s(i))$を次のように定義する、

[数2]

$$B_2^D(s(i)) = \min_j(Branch_n([M_{s(i),j} \mid M_{s(i),j+1}]))$$

[0097] 上記式は、拡張Feistel構造を構成する任意のデータ系列s(i)に入力する2つの隣り合うF関数[$F_{s(i),j}$, $F_{s(i),j+1}$]中で用いられる2つの線形変換行列[$M_{s(i),j}$, $M_{s(i),j+1}$]の結合行列[$M_{s(i),j} \mid M_{s(i),j+1}$]中の分岐数の最小値を求める式である。

[0098] 拡張Feistel構造を構成する任意のデータ系列s(i)において、データ系列s(i)に入力するF関数の上段からの個数に相当する[j]を任意のjとし、データ系列s(i)上のデータ[$W_{s(i),j}$]について考える。

データ系列s(i)に入力する2つのF関数[$F_{s(i),j+1}$], [$F_{s(i),j+2}$]のデータ系列s(i)に対する入力部を挟むデータ系列s(i)上の入出力データ[$W_{s(i),j}$]と、[$W_{s(i),j+2}$]について、

$W_{s(i),j}$＝0,

$W_{s(i),j+2}$＝0である場合を考える。

[0099] このとき、

データ系列s(i)に入力するF関数中、隣り合うF関数[$F_{s(i),j+1}$]と[$F_{s(i),j+2}$]への各々の入力差分値[$\Delta X_{s(i),j+1}$]と、[$\Delta X_{s(i),j+2}$]との間に、

[数3]

$$hw_n(\Delta X_{s(i),j+1}) + hw_n(\Delta X_{s(i),j+2}) \geq B_2^D(s(i))$$

という関係式が成立している。

[0100] なお、上記式において、hwはハミングウェイトであり、上記式の左辺はF関数の入力差分データにおける非ゼロの要素数つまりアクティブS－box数の和を表している。この数が大きな値に保証されることが差分攻撃への耐性向上が期待できる条件である。従ってそれ以外の条件が同じであれば、$B_2^D(s(i))$をできるだけ大きくするように、拡張Feistel構造を構成する各F関数内の行列を選択することが望ましいことが導かれる。

[0101] これまでの拡張Feistel型暗号ではひとつの線形変換行列をすべてのF関数内の線形変換部で利用する構成が一般的である。

しかしながら、データ系列s(i)に入力する2つの隣り合うF関数$[F_{s(i),j}, F_{s(i),j+1}]$中で用いられる2つの線形変換行列$[M_{s(i),j}]$、$[M_{s(i),j+1}]$とが、同一の行列であると、前述の分岐数演算関数:Branch()を適用した分岐数の算出式、すなわち、

$B_2^D(s(i))$

は必ず最低の値である2となってしまう。このため耐性向上の効果は見込めない。

[0102] また異なる行列を用いている場合でも不用意に2つの行列を選択してしまうと$B_2^D(s(i))$が2となってしまう場合がある。

前述の分岐数算出式によって定義される$B_2^D(s(i))$をより大きな分岐数とすることが、局所的な最小差分アクティブS－box数を大きく保証することになり、差分攻撃に対する耐性を向上させることが可能となる。従って、例えば、$B_2^D(s(i))$が3以上となるように行列を選択することで、差分攻撃に対する耐性を向上させることが可能となる。

[0103] 拡張Feistel構造のすべてのデータ系列に対して$B_2^D(s(i))$を計算し、それらの中で最小の値のものをB_2^Dとする。このB_2^Dを3以上とするように、F関数中の行列を選択する方法について以下説明する。

[0104] （4－2－1．最小分岐数B_2^Dの値を3以上とするF関数中の行列選択構成）

まず、拡張Feistel構造のすべてのデータ系列における最小分岐数$[B_2^D(s(i))]$中、最小の分岐数$[B_2^D]$を3以上とするためには、最低2種類の行列があれば実現できることを以下に説明する。

[0105] まず、2つの異なる行列$[A_0]$と$[A_1]$の結合行列$[A_0 | A_1]$の分岐数が3以上となる

、すなわち、

$Branch_n([A_0 \mid A_1]) \geqq 3$

を満たす2つの異なる行列$[A_0]$と$[A_1]$を用意する。

[0106] 次に、拡張Feistel構造のデータ系列s(i)に入力する複数のF関数の線形変換部の線形変換行列を以下のように設定する。

最初のF関数$F_{s(i),1}$の線形変換部に設定する線形変換行列をA_0、

第2番目のF関数$F_{s(i),2}$の線形変換部に設定する線形変換行列をA_1、

第3番目のF関数$F_{s(i),3}$の線形変換部に設定する線形変換行列をA_0、

:

というように2つの異なる行列$[A_0]$と$[A_1]$をデータ系列s(i)に入力する複数のF関数に対して、上から順に交互に配置していく。

[0107] このように線形変換行列を設定した場合、任意のデータ系列s(i)に入力する2つの隣り合うF関数$[F_{s(i),j}, F_{s(i),j+1}]$中で用いられる2つの線形変換行列$[M_{s(i),j}, M_{s(i),j+1}]$の結合行列$[M_{s(i),j} \mid M_{s(i),j+1}]$中の分岐数の最小値を求める上述した式は、

[数4]

$$B_2^D(s(i)) = \min_j(Branch_n([M_{s(i),j} \mid M_{s(i),j+1}])) \geq 3$$

である。すなわち、最小分岐数が3以上であることが保証される。

[0108] もちろん行列$[A_0]$と$[A_1]$を入れ替えても効果は同じである。また、拡張Feistel構造のすべてのデータ系列s(i)について同様に行列を設定すれば、2つの行列を用いただけでB_2^Dの値を3以上にすることが可能である。

[0109] このように、$Branch_n([A_0 \mid A_1]) \geqq 3$

を満たす2つの異なる行列$[A_0]$と$[A_1]$を用意して、これらの各行列を、拡張Feistel構造の各データ系列s(i)に入力するF関数に交互に配置する設定とすることで、最小分岐数B_2^Dの値を3以上にすることが可能となり、拡散行列切り替え機構(DSM)による差分攻撃に対する耐性の向上が実現される。

[0110] 上述した説明は、2つの異なる行列[A_0]と[A_1]を適用した例である。

次に、異なる行列を2以上の任意の数[k]として一般化した例について、以下、説明する。

[0111] 拡張Feistel構造に含まれるF関数[$F_{s(i),j}$]で用いられる線形変換行列を[$M_{s(i),j}$]とする。このとき、分岐数演算関数:Branch()を適用した分岐数の算出式$B_2^D(s(i))$を次のように定義する、

[数5]

$$B_k^D(s(i)) = \min_j(Branch_n([M_{s(i),j} \mid M_{s(i),j+1} \mid M_{s(i),j+2} \mid \cdots \mid M_{s(i),j+k-1}]))$$

[0112] 上記式は、拡張Feistel構造を構成する任意のデータ系列s(i)に入力するk個の隣り合うF関数[$F_{s(i),j}$, $F_{s(i),j+1}$, ・・・, $F_{s(i),j+k-1}$]中で用いられるk個の線形変換行列[$M_{s(i),j}$, $M_{s(i),j+1}$, ・・・, $M_{s(i),j+k-1}$]の結合行列[$M_{s(i),j} \mid M_{s(i),j+1} \mid \cdots \mid M_{s(i),j+k-1}$]中の分岐数の最小値を求める式である。

[0113] 拡張Feistel構造を構成する任意のデータ系列s(i)において、データ系列s(i)に入力するF関数の上段からの個数に相当する[j]を任意のjとし、データ系列s(i)上のデータ[$W_{s(i),j}$]について考える。

データ系列s(i)に入力するk個のF関数[$F_{s(i),j+1}$]・・・[$F_{s(i),j+k}$]のデータ系列s(i)に対する入力部を挟むデータ系列s(i)上の入出力データ[$W_{s(i),j}$]と、[$W_{s(i),j+k}$]について、

$W_{s(i),j}=0$,

$W_{s(i),j+k}=0$である場合を考える。

[0114] このとき、

データ系列s(i)に入力するF関数中、隣り合うk個のF関数[$F_{s(i),j+1}$]・・・[$F_{s(i),j+k}$]への各々の入力差分値[$\Delta X_{s(i),j+1}$]・・・[$\Delta X_{s(i),j+k}$]との間に、

[数6]

$$\sum_{l=j+1}^{j+k} hw_n(\Delta X_{s(i),l}) \geq B_k^D(s(i))$$

という関係式が得られる。

[0115] なお、上記式において、hwはハミングウェイトであり、上記式の左辺はF関数の入力差分データにおける非ゼロの要素数つまりアクティブS－box数の和を表している。この数が大きな値に保証されることが差分攻撃への耐性向上が期待できる条件である。従ってそれ以外の条件が同じであれば、$B_k^D(s(i))$をできるだけ大きくするように、拡張Feistel構造を構成する各F関数内の行列を選択することが望ましいことが導かれる。

[0116] しかしながら、データ系列s(i)に入力するk個の隣り合うF関数$[F_{s(i),j}]\cdots[F_{s(i),j+k-1}]$中で用いられるk個の線形変換行列$[M_{s(i),j}]\cdots[M_{s(i),j+k-1}]$中に、同じ行列が1つでも存在すると、前述の分岐数演算関数:Branch()を適用した分岐数の算出式、すなわち、

$B_k^D(s(i))$

は必ず最低の値である2となってしまう。このため耐性向上の効果は見込めない。

[0117] またk個の線形変換行列$[M_{s(i),j}]\cdots[M_{s(i),j+k-1}]$に異なる行列を用いている場合でも不用意に行列を選択してしまうと$B_k^D(s(i))$が2となってしまう場合がある。

[0118] 前述の分岐数算出式によって定義される$B_k^D(s(i))$をより大きな分岐数とすることが、局所的な最小線形アクティブS－box数を大きく保証することになり、差分攻撃に対する耐性を向上させることが可能となる。従って、例えば、$B_k^D(s(i))$が3以上となるように行列を選択することで、差分攻撃に対する耐性を向上させることが可能となる。

[0119] 拡張Feistel構造のすべてのデータ系列に対して$B_k^D(s(i))$を計算し、それらの中で最小の値のものをB_k^Dとする。このB_k^Dを3以上とするように、F関数中の行列を選択する方法について以下説明する。

[0120] (4－2－2. 最小分岐数B_k^Dの値を3以上とするF関数中の行列選択構成)

拡張Feistel構造のすべてのデータ系列における最小分岐数$[B_k^D(s(i))]$中、最

小の分岐数[B_k^D]を3以上とするためには、最低k種類の行列があれば実現できることを以下に説明する。

[0121] まず、k個の異なる行列[A_0], [A_1], [A_2], ・・・[A_{k-1}]の結合行列[A_0 | A_1 | ・・・ | A_{k-1}]の分岐数が3以上となる、すなわち、

$Branch_n([A_0 | A_1 | \cdots | A_{k-1}]) \geqq 3$

を満たすk個の異なる行列[A_0], [A_1], [A_2], ・・・[A_{k-1}]を用意する。

[0122] 次に、拡張Feistel構造のデータ系列s(i)に入力する複数のF関数の線形変換部の線形変換行列を以下のように設定する。

最初のF関数$F_{s(i),1}$の線形変換部に設定する線形変換行列をA_0、

第2番目のF関数$F_{s(i),2}$の線形変換部に設定する線形変換行列をA_1、

第3番目のF関数$F_{s(i),3}$の線形変換部に設定する線形変換行列をA_2、

:

第k番目のF関数$F_{s(i),k}$の線形変換部に設定する線形変換行列をA_{k-1}、

第k＋1番目のF関数$F_{s(i),k+1}$の線形変換部に設定する線形変換行列をA_0、

第k＋2番目のF関数$F_{s(i),k+2}$の線形変換部に設定する線形変換行列をA_1、

:

というようにk個の異なる行列[A_0], [A_1], [A_2], ・・・[A_{k-1}]をデータ系列s(i)に入力する複数のF関数に対して、上から順に、繰り返し配置していく。

[0123] このように線形変換行列[A_0], [A_1], [A_2], ・・・[A_{k-1}]を設定した場合、任意のデータ系列s(i)に入力するk個の隣り合うF関数[$F_{s(i),j}$, $F_{s(i),j+1}$ ・・・$F_{s(i),j+k-1}$]中で用いられるk個の線形変換行列[$M_{s(i),j}$, $M_{s(i),j+1}$ ・・・$M_{s(i),j+k-1}$]の結合行列[$M_{s(i),j}$ | $M_{s(i),j+1}$ | ・・・$M_{s(i),j+k-1}$]中の分岐数の最小値を求める式は、

[数7]

$$B_k^D(s(i)) = \min_j(Branch_n([M_{s(i),j} | M_{s(i),j+1} | M_{s(i),j+2} | \cdots | M_{s(i),j+k-1}])) \geq 3$$

である。すなわち、最小分岐数が3以上であることが保証される。

[0124] もちろん行列$[A_0]$, $[A_1]$, $[A_2]$, ・・・$[A_{k-1}]$を入れ替えても効果は同じである。また、拡張Feistel構造のすべてのデータ系列s(i)について同様に行列を設定すれば、k個の行列を用いただけでB_2^Dの値を3以上にすることが可能である。

[0125] このように、

$$Branch_n([A_0 \mid A_1 \mid \cdots \mid A_{k-1}]) \geqq 3$$

を満たすk個の異なる行列$[A_0]$, $[A_1]$, $[A_2]$, ・・・$[A_{k-1}]$を用意して、これらの各行列を、拡張Feistel構造の各データ系列s(i)に入力するF関数に順番に繰り返し配置する設定とすることで、最小分岐数B_k^Dの値を3以上にすることが可能となり、拡散行列切り替え機構(DSM)による差分攻撃に対する耐性の向上が実現される。

[0126] なお、kの値の選択に関しては、最低でもkが2以上であれば効果が見込まれる。kが大きくなればなるほど、保証される範囲が大きくなるため、耐性の向上がより期待できる。しかし、一方で、必要となる行列の種類の最小数が大きくなるため効率的な実装に不向きとなる可能性がある。よってkの値は設計の段階で状況に応じて選択されるべき値である。

[0127] (4－3. 拡張Feistel構造において線形攻撃に対する耐性を向上させるための構成)

次に、拡張Feistel構造において線形攻撃に対する耐性を向上させる構成について説明する。

先に、説明したように、線形攻撃に対する耐性を図る指標としては、線形マスクの接続関係を表現した線形パス(線形近似と呼ばれることが多いが、差分と対応させるためここではパスという言葉を用いる)に含まれる線形アクティブS－boxの最小数が適用可能である。線形パスは、暗号化関数中の鍵データを除くすべてのデータ部分に対して特定の線形マスク値を指定したものである。線形変換処理の前後では、入力線形マスク値と出力線形マスク値の関係は一対一に決定され、非線形変換処理の前後では、一対一とはならないが、ある入力線形マスクに対する出力線形マスクの出現確率が算出される。すべての出力に対する確率をすべて足し合わせると1となる。

[0128] SP型のF関数を持ったFeistel構造においては、非線形変換はS－boxによる処理の部分のみである。したがって、この場合、0以外の確率をもつ線形パスとは平文(入

力)に対する線形値から始まって暗号文(出力)の線形値までに至る線形マスク値データの集合であり、すべてのS－boxの前後で与えられる線形値は0以外の確率をもつものである。0以外の確率をもつある線形パスのS－boxに入力される線形値が0でないものを線形アクティブS－boxと呼ぶ。0以外の確率を持つすべての線形パスのアクティブS－boxの数のうちで最も少ない数を最小線形アクティブS－box数とよび、この数値が線形攻撃に対する安全性指標として用いられる。

[0129] 最小線形アクティブS－box数を大きくすることが、線形攻撃に対する耐性の向上をもたらす。以下では、データ系列数dをd≧2の任意整数とした拡張Feistel構造において、最小線形アクティブS－box数の数を大きくするDSM構造を構築する手法について説明する。

[0130] 拡張Feistel構造に含まれるF関数[$F_{s(i),x}$]で用いられる線形変換行列を[$M_{s(i),x}$]とする。このとき、分岐数演算関数:Branch()を適用した分岐数の算出式$B_2^L(s(i))$を次のように定義する、

[数8]

$$B_2^L(s(i)) = \min_j(Branch_n([{}^tM^{-1}_{s(i),j} | {}^tM^{-1}_{s(i),j+1}]))$$

[0131] 上記式は、拡張Feistel構造を構成する任意のデータ系列s(i)に入力する2つの隣り合うF関数[$F_{s(i),j}$, $F_{s(i),j+1}$]中で用いられる2つの線形変換行列[$M_{s(i),j}$]、[$M_{s(i),j+1}$]各々の逆行列の転置行列[${}^tM^{-1}_{s(i),j}$]、[${}^tM^{-1}_{s(i),j+1}$]の結合行列[${}^tM^{-1}_{s(i),j} | {}^tM^{-1}_{s(i),j+1}$]中の分岐数の最小値を求める式である。

[0132] 拡張Feistel構造を構成する任意のデータ系列s(i)において、データ系列s(i)に入力するF関数の上段からの個数に相当する[j]を任意のjとし、あるjに対して、

j番目のF関数に対する入力:$X_{s(i),j}$、

j番目のF関数の出力と、データ系列s(i)上のデータとの排他的論理和(XOR)結果:$W_{s(i),j}$、

j＋1番目のF関数に対する入力:$X_{s(i),j+1}$、

これらの各データの線形マスクをそれぞれ、

$\Gamma X_{s(i),j}$、

$\Gamma W_{s(i),j}$、

$\Gamma X_{s(i),j+1}$、

とすると、それらのうちどれかひとつでも0でないものがあれば、以下の式を満たす。すなわち、

[数9]

$$hw_n(\Gamma X_{s(i),j}) + hw(\Gamma W_{s(i),j}) + hw(\Gamma X_{s(i),j+1}) \geq B_2^L(s(i))$$

[0133] 上記式を満足する。上記式の左辺の値が大きいほど局所的な線形アクティブS－box数が多くなることを意味している。従って、$B_2^L(s(i))$を大きくするように行列を選択することが望ましいといえる。

[0134] しかしながら、データ系列s(i)に入力する2つの隣り合うF関数[$F_{s(i),j}$, $F_{s(i),j+1}$]中で用いられる2つの線形変換行列[$M_{s(i),j}$]、[$M_{s(i),j+1}$]とが、同一の行列であると、上記の分岐数算出式、すなわち、

$B_2^L(s(i))$

は必ず最低の値である2となってしまう。このため耐性向上の効果は見込めない。$B_2^L(s(i))$をより大きな分岐数とすることが、最小線形アクティブS－box数を大きく保証することになり、線形攻撃に対する耐性を向上させることが可能となる。従って、例えば、$B_2^L(s(i))$が3以上となるように行列を選択することで、線形攻撃に対する耐性を向上させることが可能となる。

[0135] 拡張Feistel構造のすべてのデータ系列に対して$B_2^L(s(i))$を計算し、それらの中で最小の値のものをB_2^Lとする。このB_2^Lを3以上とするように、F関数中の行列を選択する方法について以下説明する。

[0136] （4－3－1．最小分岐数B_2^Lの値を3以上とするF関数中の行列選択構成）

拡張Feistel構造のすべてのデータ系列における最小分岐数[$B_2^L(s(i))$]中、最小の分岐数[B_2^L]を3以上とするためには、最低2種類の行列があれば実現できるこ

とを以下に説明する。

[0137] まず、2つの異なる行列[A_0]と[A_1]の結合行列[${}^tA_0^{-1} \mid {}^tA_1^{-1}$]の分岐数が3以上となる、すなわち、

$Branch_n([{}^tA_0^{-1} \mid {}^tA_1^{-1}]) \geqq 3$

を満たす2つの異なる行列[A_0]と[A_1]を用意する。

[0138] 次に、拡張Feistel構造のデータ系列s(i)に入力する複数のF関数の線形変換部の線形変換行列を以下のように設定する。

最初のF関数$F_{s(i),1}$の線形変換部に設定する線形変換行列をA_0、

第2番目のF関数$F_{s(i),2}$の線形変換部に設定する線形変換行列をA_1、

第3番目のF関数$F_{s(i),3}$の線形変換部に設定する線形変換行列をA_0、

:

というように2つの異なる行列[A_0]と[A_1]をデータ系列s(i)に入力する複数のF関数に対して、上から順に交互に配置していく。

[0139] このように線形変換行列を設定した場合、任意のデータ系列s(i)に入力する2つの隣り合うF関数[$F_{s(i),j}$, $F_{s(i),j+1}$]中で用いられる2つの線形変換行列[$M_{s(i),j}$]、[$M_{s(i),j+1}$]各々の逆行列の転置行列[${}^tM^{-1}_{s(i),j}$]、[${}^tM^{-1}_{s(i),j+1}$]の結合行列[${}^tM^{-1}_{s(i),j} \mid {}^tM^{-1}_{s(i),j+1}$]中の分岐数の最小値を求める上述した式は、

[数10]

$$B_2^L(s(i)) = \min_j(Branch_n([{}^tM^{-1}_{s(i),j} \mid {}^tM^{-1}_{s(i),j+1}])) \geq 3$$

となる。すなわち、最小分岐数が3以上であることが保証される。

[0140] もちろん行列[A_0]と[A_1]を入れ替えても効果は同じである。また、拡張Feistel構造のすべてのデータ系列s(i)について同様に行列を設定すれば、2つの行列を用いただけでB_2^Lの値を3以上にすることが可能である。

[0141] このように、$Branch_n([{}^tA_0^{-1} \mid {}^tA_1^{-1}]) \geqq 3$

を満たす2つの異なる行列[A_0]と[A_1]を用意して、これらの各行列を、拡張Feiste

l構造の各データ系列s(i)に入力するF関数に交互に配置する設定とすることで、最小分岐数B_2^Lの値を3以上にすることが可能となり、拡散行列切り替え機構(DSM)による線形攻撃に対する耐性の向上が実現される。

[0142] [5. 特定の形を持つ拡張Feistel構造に対するDSMの利用構成]

上述したように、データ系列数dをd≧2の任意整数とした拡張Feistel構造においてDSM技術を適用することで、差分攻撃や線形攻撃に対する耐性を向上させることが可能である。以下、差分攻撃や線形攻撃についての安全性指標を高いレベルで保証できる具体的な拡張Feistel構造について説明する。

[0143] 先に図5、図6を参照して説明したように、データ系列数dをd≧2の任意整数とした拡張Feistel構造は、1つのデータ系列に対する入力が、他の様々なデータ系列から入力可能であり、また、1つのラウンドにおいて、複数のF関数が並列に実行可能であるなど、様々な構成がある。以下では、拡張Feistel構造を、大きく2つのタイプ(タイプ1、タイプ2)に分類して、各タイプ毎に、差分攻撃や線形攻撃についての安全性指標を高いレベルで保証できる具体的な拡張Feistel構造を説明する。

[0144] (5－1. 拡張Feistel構造のタイプ1に対するDSMの適用)

まず、拡張Feistel構造のタイプ1に対するDSMの適用について、図8を参照して説明する。

拡張Feistel構造のタイプ1は、以下のパラメータを持つものとする。

パラメータ

(a)データ分割数:d(dは3以上)

(b)入出力データ長:dmnビット

(c)分割データ長:mnビット

(d)1ラウンドあたりのF関数の数:1

[0145] 図8に示すように、各ラウンド内では、図8に示す左端のデータ系列上のmnビットデータに対してF関数が適用され、F関数の処理結果は、すぐ隣のデータ系列に出力され、排他的論理和される。なお、図8においては排他的論理和の演算記号を省略してある。

[0146] 図8に示すように、各ラウンドにおいて、F関数に対するデータ入力を行なった左端

のデータ系列は、次のラウンドでは、右端に移動し、それ以外のデータ系列は左にひとつずつずれる構成をとる。

[0147] このように各ラウンド毎に1つのF関数が実行される拡張Feistel構造にDSMを適用して差分攻撃および線形攻撃に対する耐性を向上させる構成について説明する。

[0148] 先に説明した(4－2. 拡張Feistel構造において差分攻撃に対する耐性を向上させるための構成)において、拡張Feistel構造のすべてのデータ系列に対して$B_2^D(s(i))$を計算し、それらの中で最小の値のものをB_2^Dとし、このB_2^Dを3以上とするように、F関数中の行列を選択することで、差分攻撃に対する耐性が高められることを説明した。

さらに、先に説明した(4－3. 拡張Feistel構造において線形攻撃に対する耐性を向上させるための構成)において、拡張Feistel構造のすべてのデータ系列に対して$B_2^L(s(i))$を計算し、それらの中で最小の値のものをB_2^Lとし、このB_2^Lを3以上とするように、F関数中の行列を選択することで、線形攻撃に対する耐性が高められることを説明した。

[0149] このB_2^DとB_2^Lに加えて、さらに、

B_1^Dを、図8に示すようなタイプ1の拡張Feistel構造中に含まれるF関数中の線形変換行列の分岐数中の最小の分岐数とする。

[0150] このとき、図8に示すようなタイプ1の拡張Feistel構造における連続するpラウンドに含まれる差分アクティブS－box数をActD(p)と表記し、線形アクティブS－box数をActL(p)と表記するものとすると、以下の関係式が存在する。

$ActD(3d) \geqq B_1^D + B_2^D$

$ActL(3d) \geqq 2B_2^L$

上記式において、

ActD(3d)は、連続する3dラウンドに含まれる差分アクティブS－box数、

ActL(3d)は、連続する3dラウンドに含まれる線形アクティブS－box数、

を示している。

これらの関係式が成立することの証明は後述する。

[0151] このことから、B_1^D, B_2^D, B_2^Lが大きくなるような行列を利用することによって、アクティ

ブS－box数を多く確保することが出来ることになり、結果として、差分攻撃および線形攻撃に対する耐性を向上させることが可能となる。

なお、これらB_1^D, B_2^D, B_2^Lの理論上の最大値はm＋1になることが知られている。

[0152] 上述の式、すなわち、

$ActD(3d) \geqq B_1^D + B_2^D$

$ActL(3d) \geqq 2B_2^L$

これらの式の右辺には、先に説明した最小分岐数B_2^DまたはB_2^Lが含まれており、これらの最小分岐数の値を大きくすることが、アクティブS－box数を多く確保することに貢献することになり、差分攻撃および線形攻撃に対する耐性を向上させるために有効となる。したがって、図8に示すような拡張Feistel構造のタイプ1の構成においては、先に説明した最小分岐数B_2^DまたはB_2^Lを3以上とする構成が、有効であることになり、この構成とすることで、差分攻撃と線形攻撃に対する耐性をこれまでよりも高く保証することが可能となる。

[0153] （5－2. 拡張Feistel構造のタイプ2に対するDSMの適用）

次に、拡張Feistel構造のタイプ2に対するDSMの適用について、図9を参照して説明する。

拡張Feistel構造のタイプ2は、以下のパラメータを持つものとする。

パラメータ

(a)データ分割数：d（ただしdは4以上の偶数）

(b)入出力データ長：dmnビット

(c)分割データ長：mnビット

(d)1ラウンドあたりのF関数の数：d／2

[0154] 図9に示すように、各ラウンド内では左端から数えて奇数番目にあるmnビットのデータ系列に対してF関数が適用され、F関数の処理結果は、すぐ隣のデータに出力が排他的論理和される。なお、図9においては排他的論理和の演算記号を省略してある。

[0155] 図9に示すように、各ラウンドにおいて、F関数に対するデータ入力を行なった左端のデータ系列は、次のラウンドでは、右端に移動し、それ以外のデータ系列は左に

ひとつずつずれる構成をとる。

[0156] このように各ラウンド毎にd／2個のF関数が実行される拡張Feistel構造にDSMを適用して差分攻撃および線形攻撃に対する耐性を向上させる構成について説明する。

[0157] 先に説明した(4－2. 拡張Feistel構造において差分攻撃に対する耐性を向上させるための構成)において、拡張Feistel構造のすべてのデータ系列に対して$B_2^D(s(i))$を計算し、それらの中で最小の値のものをB_2^Dとし、このB_2^Dを3以上とするように、F関数中の行列を選択することで、差分攻撃に対する耐性が高められることを説明した。

さらに、先に説明した(4－3. 拡張Feistel構造において線形攻撃に対する耐性を向上させるための構成)において、拡張Feistel構造のすべてのデータ系列に対して$B_2^L(s(i))$を計算し、それらの中で最小の値のものをB_2^Lとし、このB_2^Lを3以上とするように、F関数中の行列を選択することで、線形攻撃に対する耐性が高められることを説明した。

[0158] このB_2^DとB_2^Lに加えて、さらに、

B_1^Dを、図9に示すようなタイプ2の拡張Feistel構造中に含まれるF関数中の線形変換行列の分岐数中の最小の分岐数とする。

[0159] このとき、図9に示すようなタイプ2の拡張Feistel構造における連続するpラウンドに含まれる差分アクティブS－box数をActD(p)と表記し、線形アクティブS－box数をActL(p)と表記するものとすると、以下の関係式が存在する。

$ActD(6) \geqq B_1^D + B_2^D$

$ActL(6) \geqq 2B_2^L$

上記式において、

ActD(6)は、連続する6ラウンドに含まれる差分アクティブS－box数、

ActL(6)は、連続する6ラウンドに含まれる線形アクティブS－box数、

を示している。

これらの関係式が成立することの証明は後述する。

[0160] このことから、B_1^D, B_2^D, B_2^Lが大きくなるような行列を利用することによって、アクティ

ブS－box数を多く確保することが出来ることになり、結果として、差分攻撃および線形攻撃に対する耐性を向上させることが可能となる。

なお、これらB_1^D, B_2^D, B_2^Lの理論上の最大値はm＋1になることが知られている。

[0161] 上述の式、すなわち、

$ActD(6) \geqq B_1^D + B_2^D$

$ActL(6) \geqq 2B_2^L$

これらの式の右辺には、先に説明した最小分岐数B_2^DまたはB_2^Lが含まれており、これらの最小分岐数の値を大きくすることが、アクティブS－box数を多く確保することに貢献することになり、差分攻撃および線形攻撃に対する耐性を向上させるために有効となる。したがって、図9に示すような拡張Feistel構造のタイプ2の構成においては、先に説明した最小分岐数B_2^DまたはB_2^Lを3以上とする構成が、有効であることになり、この構成とすることで、差分攻撃と線形攻撃に対する耐性をこれまでよりも高く保証することが可能となる。

[0162] ［6．拡張Feistel構造各タイプのアクティブS－box数と、F関数中の線形変換行列に基づく最小分岐数との関係式の証明］

次に、上述した

（5－1．拡張Feistel構造のタイプ1に対するDSMの適用）

（5－2．拡張Feistel構造のタイプ2に対するDSMの適用）

において説明したアクティブS－box数と、F関数中の線形変換行列に基づく最小分岐数との関係式の証明について説明する。

[0163] （6－1．拡張Feistel構造のタイプ1のアクティブS－box数と、F関数中の線形変換行列に基づく最小分岐数との関係式の証明）

まず、先に図8を参照して説明した拡張Feistel構造のタイプ1のアクティブS－box数と、F関数中の線形変換行列に基づく最小分岐数との関係式の証明について説明する。

[0164] すなわち、タイプ1の拡張Feistel構造における連続するpラウンドに含まれる差分アクティブS－box数をActD(p)と表記し、線形アクティブS－box数をActL(p)と表記した場合の関係式、

$ActD(3d) \geqq B_1^D + B_2^D$

$ActL(3d) \geqq 2B_2^L$

この関係式が成立することを証明する。

[0165] 先に図8を参照して説明した拡張Feistel構造のタイプ1の構成を、別の形で示すと、図10のように示すことができる。図8では、F関数への入力を行なうデータ系列が左端になるように各データ系列の並びをラウンド毎に入れ替えて示していたが、図10は、データ系列のラウンド毎の入れ替えを行なわず、1つの直線で示している。図10では、ラウンド1～6dまでを示している。d個のラウンド(ラウンド1～d, d＋1～2d, ・・・, 5d＋1～6d)を1つの横ラインに並べて示してあるが、これらは並列に実行されるのではなく、各ラウンド、例えばラウンド1～dは、順次実行される。

[0166] また、図には、F関数の出力と各データ系列の交点における排他的論理和(XOR)演算を省略しているが、F関数の出力と各データ系列の交点では排他的論理和(XOR)演算が実行され、その結果が、次のラウンドのF関数の入力となる。

[0167] この拡張Feistel構造のタイプ1の構成において、先に、(5－1. 拡張Feistel構造のタイプ1に対するDSMの適用)において説明した関係式、

$ActD(3d) \geqq B_1^D + B_2^D$

$ActL(3d) \geqq 2B_2^L$

が成立することを証明する。

上記式において、

ActD(3d)、ActL(3d)は、図8または図10に示すタイプ1の拡張Feistel構造における連続する3dラウンドに含まれる差分アクティブS－box数と、線形アクティブS－box数を意味する。

B_1^Dは、タイプ1の拡張Feistel構造中に含まれるF関数中の線形変換行列の分岐数中の最小の分岐数、

B_2^D, B_2^Lは、先に(4－2), (4－3)において説明した拡張Feistel構造中に含まれる1つのデータ系列に入力する連続するF関数中の線形変換行列の結合行列の最小分岐数、および逆行列の転置行列の結合行列の最小分岐数である。

[0168] B_1^D, B_2^D, B_2^Lは、以下のように定義される。

[数11]

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

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

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

[0169] なお、上記定義において、

$B_1^D \geqq B_2^D$

の関係が成立している。

また、図8または図10に示すタイプ1の拡張Feistel構造における第k番目のF関数に含まれる差分アクティブS—boxの数をD_kで表し、線形アクティブS—boxの数をL_kで表すものとする。

[0170] (証明1. $ActD(3d) \geqq B_1^D + B_2^D$の証明)

まず、$ActD(3d) \geqq B_1^D + B_2^D$の証明を行なう。

すなわち、図8、図10に示すタイプ1の拡張Feistel構造において、連続する3dラウンドに含まれる差分アクティブS－boxの個数は$B_1^D + B_2^D$以上であることを証明する。

[0171] タイプ1の拡張Feistel構造において、入力がゼロでない差分(Δx)を与えた場合について考察する。この場合、タイプ1の拡張Feistel構造は、以下の4つの性質を持つ。

(性質1)連続するdラウンドの中に最低ひとつのラウンドでは差分アクティブS－boxが0ではないものが存在する

(性質2)$D_k = 0$ならば、$D_{k-d+1} = D_k + 1$

(性質3)$D_k \neq 0$ならば、$D_{k-d+1} + D_k + D_k + 1 \geqq B_1^D$

(性質4)$D_k + D_{k+d} \neq 0$ならば、$D_{k-d+1} + D_k + D_{k+d} + D_{k+d+1} \geqq B_2^D$

[0172] 以上の4つの性質を利用して、

$ActD(3d) \geqq B_1^D + B_2^D$

の証明、すなわち、

「連続する3dラウンドに含まれる差分アクティブS－boxの個数は$B_1^D+B_2^D$以上である」

ことを証明する。

[0173] 対象とするラウンドをi＋1番目からi＋3d番目のラウンドとして考える。

場合1:もしも、i＋d＋2ラウンド目からi＋2d－1ラウンド目までに0でないアクティブS－boxが存在する場合。

0でないアクティブS－boxが存在するラウンドをkとすると$D_k \neq 0$と表せる。

[0174] 場合1－1:場合1に加えて、$D_{k+d-1} \neq 0$である場合、

性質3から$D_k+D_{k+1}+D_{k-d+1} \geqq B_1^D$

性質4から$D_{k+d-1}+D_{k-2d}+D_{k-1}+D_{k+d} \geqq B_2^D$

であるから、

[数12]

$$\sum_{j=i+1}^{i+3d} D_j \geq B_1^D + B_2^D$$

となる。

[0175] 場合1－2:場合1に加えて、$D_{k+1} \neq 0$である場合、

性質3から$D_{k+1}+D_{k+2}+D_{k-d+2} \geqq B_1^D$

性質4から$D_k+D_{k-d+1}+D_{k+d}+D_{k+d+1} \geqq B_2^D$

であるから、

[数13]

$$\sum_{j=i+1}^{i+3d} D_j \geq B_1^D + B_2^D$$

となる。

[0176] 場合1－3:場合1に加えて、D_{k+d-1}＝0かつD_{k+1}＝0である場合、

性質2から$D_k = D_{k+d} \neq 0$

性質3から$D_k + D_{k+1} + D_{k-d+1} \geqq B_1^D$

性質3から$D_{k+d} + D_{k+d+1} + D_{k+1} \geqq B_2^D$

D_{k+1}＝0であるため、

[数14]

$$\sum_{j=i+1}^{i+3d} D_j \geq 2B_1^D$$

となる。

[0177] 場合2:もしも、i＋d＋2ラウンド目からi＋2d－1ラウンド目までに0でないアクティブS－boxが存在しない場合。

性質1から、$D_{i+d+1} \neq 0$、または$D_{i+2d} \neq 0$である。

[0178] 場合2－1:$D_{i+d+1} \neq 0$であるがD_{i+2d}＝0の場合、

性質2から$D_{i+d+1} = D_{i+2d+1} \neq 0$

性質3から$D_{i+d+1} + D_{i+d+2} + D_{i+2} \geqq B_1^D$

性質3から$D_{i+2d+1} + D_{i+2d+2} + D_{i+d+2} \geqq B_1^D$

D_{i+d+2}＝0であるため、

[数15]

$$\sum_{j=i+1}^{i+3d} D_j \geq 2B_1^D$$

である。

[0179] 場合2－2:D_{i+d+1}＝0であるがD_{i+2d}≠0の場合、

性質2からD_{i+2d}＝D_{i+d}≠0

性質3からD_{i+d}＋D_{i+d+1}＋D_{i+1}≧B_1^D

性質3からD_{i+2d}＋D_{i+2d+1}＋D_{i+d+1}≧B_1^D

D_{i+d+1}＝0であるため、

[数16]

$$\sum_{j=i+1}^{i+3d} D_j \geq 2B_1^D$$

である。

[0180] 場合2－3:D_{i+d+1}≠0かつD_{i+2d}≠0の場合、

性質3からD_{i+d+1}＋D_{i+d+2}＋D_{i+2}≧B_1^D

性質3からD_{i+2d}＋D_{i+2d+1}＋D_{i+d}＋D_{i+1}≧B_2^D

であるため、

[数17]

$$\sum_{j=i+1}^{i+3d} D_j \geq B_1^D + B_2^D$$

である。

[0181] 以上の場合1と場合2を総合すると、

[数18]

$$\sum_{j=i+1}^{i+3d} D_j \geq B_1^D + B_2^D$$

であることが証明される。すなわち、

$ActD(3d) \geqq B_1^D + B_2^D$

が成立し、図8、図10に示すタイプ1の拡張Feistel構造において、連続する3dラウンドに含まれる差分アクティブS－boxの個数は$B_1^D + B_2^D$以上であることが証明される。

[0182] (証明2. $ActL(3d) \geqq 2B_2^L$の証明)

次に、$ActL(3d) \geqq 2B_2^L$の証明を行なう。

すなわち、図8、図10に示すタイプ1の拡張Feistel構造において、連続する3dラウンドに含まれる線形アクティブS－boxの個数は$2B_2^L$以上であることを証明する。

なお、B_2^Lは、前述したように、

[数19]

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

と定義する。

またk番目のF関数に含まれる線形アクティブS－boxの数をL_kで表すものとする。

[0183] タイプ1の拡張Feistel構造において、入力がゼロでない線形マスクを与えた場合には、以下の2つの性質を持つ。

(性質5)連続するdラウンドの中の最低ひとつのラウンドでは線形アクティブS－boxが0ではないものが存在する

(性質6)$L_k+L_{k+1}+L_{k+d}\geqq B_2^L$、または、$L_k+L_{k+1}+L_{k+d}=0$である。なお、$L_k+L_{k+1}+L_{k+d}\geqq B_2^L$の場合は左辺に含まれる2つ以上の項が同時に0となることはない。

以上の2つの性質を利用して、

$ActL(3d)\geqq 2B_2^L$

の証明、すなわち、

「連続する3dラウンドに含まれる線形アクティブS－boxの個数は$2B_2^L$以上である」

ことを証明する。

[0184] 対象とするラウンドをi＋1番目からi＋3d番目のラウンドとして考える。

場合1:もしも、i＋d＋2ラウンド目からi＋2dラウンド目までに0でないアクティブS－boxが存在する場合。

0でないアクティブS－boxが存在するラウンドをkとすると$L_k\neq 0$である。

[0185] 場合1－1:場合1に加えて、$L_{k+d}\neq 0$または$L_{k-1}\neq 0$である場合、

性質6から$L_k+L_{k+d}+L_{k+1}\geqq B_2^L$

性質6から$L_{k-1}+L_{k-1-d}+L_{k-d}\geqq B_2^L$

であるから、

[数20]

$$\sum_{j=i+1}^{i+3d} L_j \geq 2B_2^L$$

となる。

[0186] 場合1－2:場合1に加えて、$L_{k+d}=0$かつ$L_{k-1}=0$である場合、

性質6から$L_{k-d+1}\neq 0$

性質6から$L_k+L_{k-1}+L_{k+d-1}\geqq B_2^L$

性質6から$L_{k-d+1}+L_{k+1}+L_{k-d+2}\geqq B_2^L$

[0187] このときd≧4であれば、

[数21]

$$\sum_{j=i+1}^{i+3d} L_j \geq 2B_2^L$$

である。

[0188] d＝3であれば、L_{k-1}が重なるがすでにL_{k-1}＝0であることがわかっているため、同様に、

[数22]

$$\sum_{j=i+1}^{i+3d} L_j \geq 2B_2^L$$

である。

[0189] 場合2:もしも、i＋d＋2ラウンド目からi＋2d－1ラウンド目までに0でないアクティブS－boxが存在しない場合。

性質1から、$L_{i+d+1} \neq 0$となる。

性質6から$L_{i+d} \neq 0$

性質6から$L_{i+d+1} + L_{i+d+2} + L_{i+2d+1} \geqq B_2^L$

性質6から$L_{i+d} + L_{i+d-1} + L_{i+2d-1} \geqq B_2^L$

[0190] このときd≧4であれば、

[数23]

$$\sum_{j=i+1}^{i+3d} L_j \geq 2B_2^L$$

である。

[0191] d＝3であれば、L_{i+5}が重なるがすでにL_{i+5}＝0であることがわかっているため、同様に、

[数24]

$$\sum_{j=i+1}^{i+3d} L_j \geq 2B_2^L$$

である。

[0192] 以上の場合1と場合2を総合すると、

[数25]

$$\sum_{j=i+1}^{i+3d} L_j \geq 2B_2^L$$

であることが証明される。すなわち、

$ActL(3d) \geqq 2B_2^L$

が成立し、図8、図10に示すタイプ1の拡張Feistel構造において、連続する3dラウンドに含まれる線形アクティブS－boxの個数は$2B_2^L$以上であることが証明される。

[0193] （6－2. 拡張Feistel構造のタイプ2のアクティブS－box数と、F関数中の線形変換行列に基づく最小分岐数との関係式の証明）

次に、図9を参照して説明した拡張Feistel構造のタイプ2のアクティブS－box数と、F関数中の線形変換行列に基づく最小分岐数との関係式の証明について説明する。

[0194] すなわち、タイプ2の拡張Feistel構造における連続するpラウンドに含まれる差分

アクティブS－box数をActD(p)と表記し、線形アクティブS－box数をActL(p)と表記した場合の関係式、

$ActD(6) \geqq B_1^D + B_2^D$

$ActL(6) \geqq 2B_2^L$

この関係式が成立することを証明する。

[0195] 先に図9を参照して説明した拡張Feistel構造のタイプ2の構成を、別の形で示すと、図11のように示すことができる。図9では、ラウンド毎に各データ系列の並びを入れ替えて示していたが、図11は、データ系列の入れ替えを行なわず、1つの直線で示している。図11では、ラウンド1～12までを示している。2つのラウンド(1～2, 3～4, ・・)のF関数を1つの横ラインに並べて示してある。例えば、図11に示すラウンド1～2の横ラインに示されたF関数F1, 0～F1, d－1中、$F_{1,0}$、$F_{1,2}$、・・・、$F_{1,d-2}$の1つおきのF関数(出力の矢印が上向き)が第1ラウンドにおいて並列に実行される。次の第2ラウンドにおいて、残りの$F_{1,1}$、$F_{1,3}$、・・・、$F_{1,d-1}$の1つおきのF関数(出力の矢印が下向き)が並列に実行される。

[0196] 図11において、F関数を識別するための番号は証明をわかりやすくするために新たに導入したものであり、2つの数字を使ってF関数の位置を決定している。

$F_{i,j}$のiは、ラウンド数(1＝1, 2ラウンド、2＝3, 4ラウンド・・)を示し、yは、2つのラウンドにおけるF関数の一を示している。なお、jが0, 2, 4, の偶数であれば、先行ラウンドにおけるF関数であり、jが1, 3, 5, の奇数であれば、後続ラウンドにおけるF関数である。なお、F関数$F_{i,j}$に含まれる線形変換行列を$[M_{i,j}]$と呼ぶものとする。

[0197] この拡張Feistel構造のタイプ2の構成において、先に、(5－2. 拡張Feistel構造のタイプ2に対するDSMの適用)において説明した関係式、

$ActD(6) \geqq B_1^D + B_2^D$

$ActL(6) \geqq 2B_2^L$

が成立することを証明する。

上記式において、

ActD(6)、ActL(6)は、図9または図11に示すタイプ2の拡張Feistel構造における連続する6ラウンドに含まれる差分アクティブS－box数と、線形アクティブS－box

数を意味する。

B_1^Dは、タイプ2の拡張Feistel構造中に含まれるF関数中の線形変換行列の分岐数中の最小の分岐数、

B_2^D, B_2^Lは、先に(4－2), (4－3)において説明した拡張Feistel構造中に含まれる1つのデータ系列に入力する連続するF関数中の線形変換行列の結合行列の最小分岐数、および逆行列の転置行列の結合行列の最小分岐数である。

[0198] B_1^D, B_2^D, B_2^Lは、以下のように定義される。

[数26]

$$B_1^D = \min_{i,j}(Branch_n(M_{i,j}))$$

$$B_2^D = \min_{i,j}(Branch_n([M_{i,j} \mid M_{i+1,j}]))$$

$$B_2^L = \min_{i,j}(Branch_n([{}^tM_{i,j}^{-1} \mid {}^tM_{i+1,j}^{-1}]))$$

[0199] なお、上記定義において、

$B_1^D \geqq B_2^D$

の関係が成立している。

また、$F_{p,q}$に含まれるアクティブS－boxの数を$D_{p,q}$で表すものとする。なお以降で、添え字qの部分が負の値やd以上の値を持つ場合には、dによる剰余演算(q mod d)を行い常に$0 \leqq q < d$となるように補正するものとする。

[0200] (証明3. ActD(6)$\geqq B_1^D + B_2^D$の証明)

まず、ActD(6)$\geqq B_1^D + B_2^D$の証明を行なう。

すなわち、図9、図11に示すタイプ2の拡張Feistel構造において、連続する6ラウンドに含まれる差分アクティブS－boxの個数は$B_1^D + B_2^D$以上であることを証明する。

[0201] タイプ2の拡張Feistel構造において、入力がゼロでない差分(Δx)を与えた場合

について考察する。この場合、タイプ2の拡張Feistel構造は、以下の4つの性質を持つ。

(性質1)あるiに対して、$F_{p,q}$ ($p=i$, $q\in\{0,..d-1\}$)の中には差分アクティブS－boxが0ではないものが存在する

(性質2)$D_{p,q}=0$ならば、

$D_{p-1,q+1}=D_{p,q+1}$ (qが偶数のとき)

$D_{p,q+1}=D_{p+1,q+1}$ (qが奇数のとき)

(性質3)$D_{p,q}\neq 0$ならば、

$D_{p,q}+D_{p-1,q+1}+D_{p,q+1}\geqq B_1^D$ (qが偶数のとき)

$D_{p,q}+D_{p,q+1}+D_{p+1,q+1}\geqq B_1^D$ (qが奇数のとき)

(性質4)$D_{p,q}+D_{p+1,q}\neq 0$ならば、

$D_{p,q}+D_{p+1,q}+D_{p-1,q+1}+D_{p+1,q+1}\geqq B_2^D$ (qが偶数のとき)

$D_{p,q}+D_{p+1,q}+D_{p,q+1}+D_{p+2,q+1}\geqq B_2^D$ (qが奇数のとき)

[0202] 以上の4つの性質を利用して、

$ActD(6)\geqq B_1^D+B_2^D$

の証明、すなわち、

「1以上の任意の整数iに対して、$p\in\{i, i+1, i+2\}$, $q\in\{0, 1, ..d-1\}$を満たす3d個のF関数Fp, qに含まれる差分アクティブS－boxの総数は$B_1^D+B_2^D$以上である」

ことを証明する。

[0203] $D_{p,q}$ ($p=i+1$, $q\in\{0,..d-1\}$)の0でない要素を任意に取り出したとき、それが$D_{j,k}\neq 0$であったとする。上述の(性質1)より必ず存在することが示される。

[0204] 場合1:$D_{j,k-1}\neq 0$である場合、

性質3から

$D_{j,k}+D_{j-1,k+1}+D_{j,k+1}\geqq B_1^D$ (kが偶数のとき)

$D_{j,k}+D_{j,k+1}+D_{j+1,k+1}\geqq B_1^D$ (kが奇数のとき)

性質4から

$D_{j-1,k-1}+D_{j,k-1}+D_{j-1,k}+D_{j+1,k}\geqq B_2^D$ (kが偶数のとき)

$D_{j,k-1}+D_{j+1,k-1}+D_{j-1,k}+D_{j+1,k}\geqq B_2^D$ (kが奇数のとき)

であるから、

[数27]

$$\sum_{p=i}^{i+2}\sum_{q=0}^{d-1} D_{p,q} \geq B_1^D + B_2^D$$

が成立する。

[0205] 場合2:$D_{j,k+1}\neq 0$である場合、

性質3から

$D_{j,k+1}+D_{j,k+2}+D_{j+1,k+2}\geqq B_1^D$ (kが偶数のとき)

$D_{j,k+1}+D_{j-1,k+2}+D_{j,k+2}\geqq B_1^D$ (kが奇数のとき)

性質4から

$D_{j,k}+D_{j+1,k}+D_{j-1,k+1}+D_{j+1,k+1}\geqq B_2^D$ (kが偶数のとき)

$D_{j-1,k}+D_{j,k}+D_{j-1,k+1}+D_{j+1,k+1}\geqq B_2^D$ (kが奇数のとき)

であるから、

[数28]

$$\sum_{p=i}^{i+2}\sum_{q=0}^{d-1} D_{p,q} \geq B_1^D + B_2^D$$

が成立する。

[0206] 場合3:$D_{j,k-1}=0$かつ$D_{j,k+1}=0$である場合、

性質2から、$D_{j,k-1}=0$であるので

$D_{j+1,k}=D_{j,k}\neq 0$ (kが偶数のとき)

$D_{j-1,k}=D_{j,k}\neq 0$ (kが奇数のとき)

性質3から、

$D_{j,k}+D_{j-1,k+1}+D_{j,k+1}\geqq B_1^D$ （kが偶数のとき）

$D_{j,k}+D_{j,k+1}+D_{j+1,k+1}\geqq B_1^D$ （kが奇数のとき）

さらに性質3から

$D_{j+1,k}+D_{j,k+1}+D_{j+1,k+1}\geqq B_1^D$ （kが偶数のとき）

$D_{j-1,k}+D_{j-1,k+1}+D_{j,k+1}\geqq B_1^D$ （kが奇数のとき）

$D_{j,k+1}=0$であるから、

[数29]

$$\sum_{p=i}^{i+2}\sum_{q=0}^{d-1}D_{p,q}\geq B_1^D+B_2^D$$

が成立する。

[0207] 以上を総合すると、

[数30]

$$\sum_{p=i}^{i+2}\sum_{q=0}^{d-1}D_{p,q}\geq B_1^D+B_2^D$$

であることが証明される。すなわち、

$ActD(6)\geqq B_1^D+B_2^D$

が成立し、図9、図11に示すタイプ2の拡張Feistel構造において、連続する6ラウンドに含まれる差分アクティブS－boxの個数は$B_1^D+B_2^D$以上であることが証明される。

[0208] （証明4. $ActL(6)\geqq 2B_2^L$の証明）

次に、$ActL(6)\geqq 2B_2^L$の証明を行なう。

すなわち、図9、図11に示すタイプ2の拡張Feistel構造において、連続する6ラウンドに含まれる線形アクティブS－boxの個数は$2B_2^L$以上であることを証明する。

なお、B_2^Lは、前述したように、

[数31]

$$B_2^L = \min_{i,j}(Branch_n([{}^tM_{i,j}^{-1}|{}^tM_{i+1,j}^{-1}]))$$

と定義する。

また$F_{p,q}$番目のF関数に含まれる線形アクティブS－boxの数を$L_{p,q}$で表すものとする。

[0209] タイプ2の拡張Feistel構造において、入力がゼロでない線形マスクを与えた場合には、以下の2つの性質を持つ。

(性質5)あるiに対して、$F_{p,q}$ (p＝i, q∈{0, . . d－1})の中には線形アクティブS－boxが0ではないものが存在する

(性質6)

$L_{j,k}+L_{j+1,k}+L_{j,k+1} \geqq B_2^L$ または、$L_{j,k}+L_{j+1,k}+L_{j,k+1}=0$ (kが偶数のとき)

$L_{j,k}+L_{j+1,k}+L_{j+1,k+1} \geqq B_2^L$ または、$L_{j,k}+L_{j+1,k}+L_{j+1,k+1}=0$ (kが奇数のとき)

[0210] なお、$L_a+L_b+L_c \geqq B_2^L$の形の場合は左辺に含まれる2つ以上の項が同時に0となることはない。

以上の2つの性質を利用して、

$ActL(6) \geqq 2B_2^L$

の証明、すなわち、

「1以上の任意の整数iに対して、p∈{i, i＋1, i＋2}, q∈{0, 1, . . d－1}を満たす3d個のF関数$F_{p,q}$に含まれる線形アクティブS－boxの総数は$2B_2^L$以上である」

ことを証明する。

[0211] $L_{p,q}$ (p＝i＋1, q∈{0, . . d－1})の0でない要素を任意に取り出したとき、それが$L_{j,k} \neq 0$であったとする。そのような$L_{j,k}$は性質5より必ず存在することが示される。

[0212] 性質6から、

$L_{j-1,k}+L_{j,k}+L_{j-1,k+1} \geqq B_2^L$ (kが偶数のとき)

$L_{j,k}+L_{j+1,k}+L_{j+1,k+1} \geqq B_2^L$ (kが奇数のとき)

[0213] 場合1:$L_{j,k-1}\neq 0$である場合、

性質6から

$L_{j,k-1}+L_{j+1,k-1}+L_{j+1,k}\geqq B_2^L$ (kが偶数のとき)

$L_{j-1,k-1}+L_{j,k-1}+L_{j-1,k}\geqq B_2^L$ (kが奇数のとき)

従って、この場合、

[数32]

$$\sum_{p=i}^{i+2}\sum_{q=0}^{d-1}L_{p,q}\geq B_2^L$$

が成立する。

[0214] 場合2:$L_{j,k-1}=0$である場合、

性質6から

$L_{j-1,k-1}\neq 0$ (kが偶数のとき)

$L_{j+1,k-1}\neq 0$ (kが奇数のとき)

であるので、

$L_{j-1,k-2}+L_{j,k-2}+L_{j-1,k-1}\geqq B_2^L$ (kが偶数のとき)

$L_{j,k-2}+L_{j+1,k-2}+L_{j+1,k-1}\geqq B_2^L$ (kが奇数のとき)

このときd≧4であるので、この場合、

[数33]

$$\sum_{p=i}^{i+2}\sum_{q=0}^{d-1}L_{p,q}\geq B_2^L$$

が成立する。

[0215] 以上の場合1と場合2を総合すると、

[数34]

$$\sum_{p=i}^{i+2}\sum_{q=0}^{d-1} L_{p,q} \geq B_2^L$$

であることが証明される。すなわち、

$\mathrm{ActL}(6) \geqq 2B_2^L$

が成立し、図9、図11に示すタイプ2の拡張Feistel構造において、連続する6ラウンドに含まれる線形アクティブS－boxの個数は$2B_2^L$以上であることが証明される。

[0216] ［7. F関数の設定および利用処理の工夫に基づく実装における改良構成］

上述したように、本発明では、データ系列数：dをd≧2の整数とした拡張Feistel構造において、各ラウンドのF関数の線形変換処理として、少なくとも2以上の異なる行列を選択的に適用する、いわゆる拡散行列切り替え機構（DSM）を適用することで、線形解析や差分解析に対する耐性を向上させた構成を実現している。

[0217] このように、異なる複数の行列を選択適用させる演算処理を実行する構成をハードウェアで実現する場合、それぞれの行列に対応する演算を行なうハードウェア構成を持つ異なるF関数処理部が必要となる。特に、1つのラウンドにおいて、複数のF関数を並列に実行させようとした場合には、並列処理を行なうための複数のF関数用回路が必要となる。

[0218] すなわち、先に図9や図11を参照して説明したタイプ2の拡張Feistel構造では、同一ラウンドに複数のF関数を適用したデータ変換処理を並列に実行する構成であり、このタイプ2の構成に従った処理をハードウェアで実行する場合、1つのラウンドで並列に実行する個数分のF関数のハードウェアを実装することが必要となる。このような並列実行の要求されるF関数は、同一構成である場合でも、その同一構成を持つF関数を複数、備えなければならない。

[0219] 前述したように、本発明の暗号処理構成は、各ラウンドにおけるF関数において実行する線形変換処理に、少なくとも2以上の複数の異なる行列を選択的に適用する

構成とすることで各種の攻撃に対する耐性を高めた構成を持つ。すなわち、拡散行列切り替え機構(DSM:Diffusion Switching Mechanism)を備えた構成としたものである。

[0220] この拡散行列切り替え機構(DSM)を満足させるためには、拡張Feistel構造の各データ系列s(i)に入力する連続するk個(ただし、kは2以上の整数)のF関数に含まれる線形変換行列に基づいて算出されるデータ系列対応の最小分岐数[$B_k^D(s(i))$]中から選択される全データ系列中の最小分岐数[B_k^D]が3以上となる条件を満足する複数の異なる行列に設定することなどの条件が満足されればよく、各ラウンドにおいて並列に実行されるF関数における制約は特にない。

[0221] 以下では、この特性に基づいて、拡張Feistel構造において拡散行列切り替え機構(DSM)に基づく耐性を維持しつつ、実装効率を高めた構成例について説明する。

[0222] (7－1. 拡張Feistelのタイプ2の効率的なF関数配置方法)

まず、先に、図9、図11を参照して説明した拡張Feistelのタイプ2の効率的なF関数配置構成について説明する。タイプ2の拡張Feistel構造は、先に説明した項目(5－2. 拡張Feistel構造のタイプ2に対するDSMの適用)において述べたように、以下のパラメータを持つ。

パラメータ

(a)データ分割数:d(ただしdは4以上の偶数)

(b)入出力データ長:dmnビット

(c)分割データ長:mnビット

(d)1ラウンドあたりのF関数の数:d／2

[0223] すなわち、図9に示すように、各ラウンド内では左端から数えて奇数番目にあるmnビットのデータ系列に対してF関数が適用され、F関数の処理結果は、すぐ隣のデータに出力が排他的論理和される。なお、図9においては排他的論理和の演算記号を省略してある。

[0224] 以下では、このような構成を持つタイプ2の拡張Feistel構造に対する実装効率を高めた構成について説明する。一例として、データ系列数(分割数)d＝4の場合に

ついて、図12を参照して説明する。図12において、2つの異なる線形変換行列M1，M2によって線形変換を実行することなる2つのF関数をそれぞれF1，F2とする。

[0225] 図12に示すFeistel構造は、F関数F1，F2の2つのF関数を用いたd＝4の拡張Feistel構造のタイプ2である。すなわち、

(a)データ分割数：4

(b)入出力データ長：4mnビット

(c)分割データ長：mnビット

(d)1ラウンドあたりのF関数の数：4／2＝2

を持つ構成である。

[0226] この図12に示す構成の場合、2つのF関数を用いてDSM条件を満たすようにするにはいくつかの配置が考えられる。すなわち、DSM条件を満足させるためには、前述したように、各データ系列s(i)に入力する連続するk個（ただし、kは2以上の整数）のF関数に含まれる線形変換行列に基づいて算出されるデータ系列対応の最小分岐数[$B_k^D(s(i))$]中から選択される全データ系列中の最小分岐数[B_k^D]が3以上となる条件を満足する複数の異なる行列に設定することなどの条件が満足されればよく、各ラウンドにおいて並列に実行されるF関数における制約は特にない。

[0227] 従って、F関数の設定態様としては、

(a)1つのラウンドに設定する複数のF関数を同一のF関数とする設定、

(b)1つのラウンドに設定する複数のF関数を異なるF関数とする設定、

上記2つの態様が可能となる。

[0228] ここでは、図12に示すように、1つのラウンドに存在する2つのF関数が互いにF1，F2となるように選択する構成をとる。この構成によるメリットは、1ラウンド分の処理を基本としてハードウェア（H／W）実装を行った場合に顕著に現れる。

[0229] すなわち、ハードウェア（H／W）実装として、1つのラウンド分の処理だけを実行可能な構成、すなわち、図13に示すように、F関数F1と、関数F2を並列に実行可能な構成を持つハードウェアを設定する。図13は、図12に示す拡張Feistel構造に従った暗号処理を実行するハードウェア構成を持つ暗号処理装置250を示すブロック図である。

[0230] 暗号処理装置250は、F関数F1を実行する第1F関数(F1)専用処理回路251と、F関数F2を実行する第2F関数(F2)専用処理回路252と、制御回路253、および補助回路254から構成される。第1F関数(F1)専用処理回路251と、第2F関数(F2)専用処理回路252は並列に動作可能な構成であり、各ラウンドにおいて、これらの2つの回路を適用して2つの異なるF関数に基づくデータ変換が実行される。

[0231] 制御回路253は、各F関数専用処理回路251, 252、および補助回路254に対する入出力データの制御を実行する。補助回路254はF関数以外の演算処理などを実行する。

[0232] この構成を適用することで、必要なラウンド数分だけ、第1F関数(F1)専用処理回路251と、第2F関数(F2)専用処理回路252を適用してラウンド演算を行なうことが可能となる。すべてのラウンドにおいて2つのF関数専用回路が並列に実行され、無駄な回路を設けることのない実装が可能となる。

[0233] 図12に示すように各ラウンドで並列に実行するF関数が2つの場合、これらを異なるF関数に設定することで、図13に示すハードウェア実装により、すべてのラウンド演算を行なうことが可能となる。ちなみに、1つのラウンドにおいて実行するF関数を同じ設定、例えば第1ラウンドで、F1, F1を並列に実行し、第2ラウンドでF2, F2を実行するような構成とした場合、ハードウェアとしては、F1実行回路とF2実行回路を各々2つ設けることが必要となり、図13に示す構成に比較して回路規模を大きなものとすることが必要となる。

[0234] 図12に示すように各ラウンドで実行するF関数の組み合わせをすべてF1, F2の設定とすることで、図13に示すハードウェアを適用して、各ラウンドにおいて、常にF1, F2が同時に実行でき、回路上の無駄を発生させることなく回路規模を小さくした小型の装置が実現される。

[0235] 図12に示す構成は、データ系列d＝4の場合であるが、その他のデータ系列数の場合も、同様な設定とすることで、効率的な実装が可能となる。例えばデータ系列数d＝8の場合、1つのラウンドには、4つのF関数が設定されることになるが、この4つのF関数を、2つの異なるF関数F1, F2を2つずつ設定する構成とする。

[0236] この場合の実装構成は、F関数F1, F2をそれぞれ2つずつ設けて、4つのF関数(

F1, F1, F2, F2)を並列実行可能な構成とする。この構成により、すべてのラウンドにおいて4つのすべてのF関数が並列に実行され、無駄な回路を設けることのない実装が可能となる。

[0237] また、データ系列数d＝16の場合、1つのラウンドに存在する8つのF関数をF1, F2を4つずつ設定する。さらに一般化して、データ系列数d＝4xの場合には、各ラウンドにおいて、F関数F1, F2がx個づつ利用される構成にするようにして、ハードウェア実装として、F関数F1, F2を各々x個設定した構成とすれば、毎ラウンドで必要とされるF1, F2の個数が同じであるため過不足無く実行でき実装効率を高めることができる。

[0238] 上述した処理例は、拡散行列切り替え機構(DSM)を満足させるために、2つの線形変換行列を適用した2つの異なるF関数を設定した例であるが、3種類以上の線形変換行列を用いて3種類以上のF関数を設定した場合でも同様のことが言える。

[0239] 3種類のF関数を効率的な実装とするための配置例を図14に示す。図14は、データ系列数d＝6の拡張Feistelのタイプ2の構造例である。この図14に示す構成では、1つのラウンドに存在する3つのF関数がF1, F2, F3とかならずひとつずつ利用される構成になるように設定されている。

[0240] この構成により、ハードウェア(H／W)実装時にF1, F2, F3をそれぞれひとつずつ実装するのみで、各ラウンドにおいて、F関数を並列に実行させる構成とすることができ、H／W的に見て無駄のない回路構成が実現される。

[0241] さらに、データ系列数d＝12の場合は1つのラウンドに存在する6つのF関数をF1, F2, F3各々2つずつの設定とする。また、データ系列数d＝18の場合は、1つのラウンドに設定する9つのF関数について、F1, F2, F3を3つずつの設定とする。これらを一般化して、データ系列数d＝6xの場合には、各ラウンドに設定するF関数をF1, F2, F3の各々がx個ずつとなるようにする。すなわち、各ラウンドにおいて、異なるFは関数が均等に利用される構成とする。

[0242] このようなF関数の設定構成とすることで、毎ラウンドで必要とされるF1, F2, F3の個数を同じ数に設定することができ、ハードウェア実装において過不足無く利用する回路の設定が可能となり、実装効率を高めることができる。ソフトウェアの場合にも、

入出力値を取得するためのテーブルの利用態様が各ラウンドにおいて均一となるので、様々なパターンを想定したテーブルを構成することなく、1つの利用態様に応じたテーブルを設定してメモリに格納することが可能となる。

[0243] 上述した各処理例をさらに、一般化すると以下のように言える。

(1)a種類のF関数を利用したType2の拡張Fesitel構造を構成する場合、データ系列数(分割数)d＝2ax、ただしaは2以上の整数，xは1以上の整数、としたとき、1つのラウンド内に設定されるax個のF関数として、全種類のF関数が均等にx個ずつ設定する構成とすることで実装効率を向上させることが可能となる。

[0244] なお、上述したF関数の設定においては、各データ系列に入力されるF関数の設定を、前述したDSM条件を満足させる設定とすることで耐性の維持が可能である。

[0245] (7－2. Feistel構造と拡張Feistel構造における部品の共通化)

前述したように、これまで説明してきたFeistel構造、拡張Feistelのタイプ1、拡張Feistelのタイプ2のいずれに対してもDSMメカニズムを利用することにより、攻撃に対する耐性を向上させるメリットがある。

[0246] すなわち、Feistel構造を大きく分類すると、

(a)データ系列数(分割数)d＝2としたFeistel構造

(b)データ系列数(分割数)d≧2の任意数とした拡張Feistel構造

に分類され、さらに、拡張Feistel構造は、

(b1)各ラウンドにおいて1つのF関数の実行のみを許容したタイプ1、

(b2)各ラウンドにおいて複数のF関数の並列実行を許容したタイプ2、

これら(a)，(b1)，(b2)の3種類に分類できる。

これらの3種類のFeistel構造のいずれにおいても、DSMメカニズムの適用による耐性向上が実現される。

[0247] DSMメカニズムの適用のためには、少なくとも2つ以上の異なる線形変換行列を実行する異なるF関数を実装することが必要となるが、この異なる複数のF関数を持つ実装構成によって、上述の複数の異なるFeistel構造(a)，(b1)，(b2)を選択的に実行可能な装置を実現することができる。このような選択的な処理を実行する装置構成について以下、説明する。

[0248] 拡散行列切り替え機構(DSM)を満足する線形変換行列を実行する複数の異なるF関数を決定し、これらの各F関数における入出力データのデータサイズをmnビットとする。このようなF関数を適用することで、例えば、図15に示すような、データ系列d＝2のFeistel構造では2mnビットのブロック暗号が実行される。

[0249] 図15に示すデータ系列d＝2のFeistel構造の各F関数F1，F2は、入出力データサイズがmnビットである。このデータ系列d＝2のFeistel構造は、2mnビットの平文を2mnビットの暗号文にする処理、またはその逆の復号処理を行い、2mnビットのブロック暗号を実行する。

[0250] また、この図15に示す入出力データサイズがmnビットのF関数F1，F2を利用することで、拡散行列切り替え機構(DSM)を満足するデータ系列数d＝4の拡張Feistel構造を構成することができる。図16にこの構成を示す。

[0251] 図16に示すデータ系列d＝4の拡張Feistel構造の各F関数F1，F2は、入出力データサイズがmnビットであり、図15に示すF関数F1，F2をそのまま適用したものである。このデータ系列d＝4の拡張Feistel構造は、4mnビットの平文を4mnビットの暗号文にする処理、またはその逆の復号処理を行い、4mnビットのブロック暗号を実行する。

[0252] さらに、一般化して、データ系列数d＝x、ただしxは2以上の整数、とした場合、xmnビットの暗号化または復号処理を実行するブロック暗号構成を、同じF関数実行構成を用いて構築することができる。

[0253] 例えば、入出力ビットが64ビットの異なるF関数F1，F2のみを用いて、DSM機構を実現する入出力128ビットブロック暗号処理と、256ビットブロック暗号処理を選択的に実行可能な装置を構成することが可能となる。

[0254] すなわちF関数としては、入出力ビットが64ビットの異なる2つのF関数F1，F2を実装し、これらの利用態様を制御する。例えば、データ系列数d＝2としたFeistel構造(図15)に基づく暗号処理を実行する場合は、各F関数F1，F2を各ラウンドにおいて1つ実行する構成とする。一方、データ系列数d＝4とした拡張Feistel構造(図16)に基づく暗号処理を実行する場合は、各F関数F1，F2を各ラウンドにおいて並列に実行する構成とする。このように、2種類のF関数を装着することで、入出力128ビット

ブロック暗号と256ビットブロック暗号を選択的に実行可能な装置が実現される。すなわち、同じF関数を使って接続方法を変えることで異なるビット数のブロック暗号を実行することが可能であり、S／W，H／W両者において回路・コードの共有化などによる実装効率の向上が期待できる。

[0255] このような構成を持つ暗号処理装置の構成例を図17に示す。図17に示す暗号処理装置270は、F関数F1を実行する第1F関数（F1）専用処理回路271と、F関数F2を実行する第2F関数（F2）専用処理回路272と、制御回路273、および補助回路274から構成される。第1F関数（F1）専用処理回路271と、第2F関数（F2）専用処理回路272は並列に動作可能な構成である。制御回路273は、各処理部に対するデータ入出力制御を行うとともに、Feistel構造選択処理を実行する。補助回路254はF関数以外の演算処理などを実行する。

[0256] 制御回路273は、Feistel構造選択処理として、

(a)データ系列数（分割数）d＝2としたFeistel構造

(b1)データ系列数（分割数）d≧2の任意数とした拡張Feistel構造であり、各ラウンドにおいて1つのF関数の実行のみを許容したタイプ1、

(b2)データ系列数（分割数）d≧2の任意数とした拡張Feistel構造であり、各ラウンドにおいて複数のF関数の並列実行を許容したタイプ2、

これらのいずれの構造に基づく暗号処理を実行するかを選択する。なお、設定情報は、例えば外部から入力する。あるいは暗号化または復号処理の対象となるデータのビット長に応じて実行する処理形態を選択する構成としてもよい。制御回路273は、選択に応じて、各F関数専用回路の適用シーケンスを変更し、各Feistel構造に従ったラウンド関数を実行させる制御を行う。

[0257] この構成を適用することで、第1F関数（F1）専用処理回路251と、第2F関数（F2）専用処理回路252を適用して様々なFeistel構造を適用した暗号処理が可能となり、暗号化処理、または復号処理の処理ビットが異なる様々なビット対応の暗号処理を実行可能となる。

[0258] また、図17には2つのF関数を持つ例を示しているが、2つのF関数を用いた例にはとどまらず、任意の個数のF関数を用いた構成でも同様の結果が期待できる。例え

ば、先に図14を参照して説明した拡張Feistel構造では、3つの異なるF関数F1，F2．F3を適用して拡散行列切り替え機構（DSM）を満足するデータ系列数d＝6の拡張Feistel構造を構成している。これと同じ3種類のF関数F1，F2，F3のF関数を適用して図18に示すデータ系列d＝2のFeistel構造を持つ暗号処理構成が構築できる。このデータ系列d＝2の構成においても、各行列F1，F2，F3は、DSM機構を満足する設定で配置される。

[0259] このような3種類のF関数F1，F2，F3を実行する暗号処理装置の構成例を図19に示す。図19に示す暗号処理装置280は、F関数F1を実行する第1F関数（F1）専用処理回路281と、F関数F2を実行する第2F関数（F2）専用処理回路282と、F関数F3を実行する第3F関数（F3）専用処理回路283と、制御回路284、および補助回路275から構成される。第1F関数（F1）専用処理回路281と、第2F関数（F2）専用処理回路282と、第3F関数（F3）専用処理回路283とは並列に動作可能な構成である。制御回路284は、各処理部に対するデータ入出力制御を行うとともに、Feistel構造選択処理を実行する。補助回路285はF関数以外の演算処理などを実行する。

[0260] 制御回路284は、Feistel構造選択処理として、

(a)データ系列数（分割数）d＝2としたFeistel構造

(b1)データ系列数（分割数）d≧2の任意数とした拡張Feistel構造であり、各ラウンドにおいて1つのF関数の実行のみを許容したタイプ1、

(b2)データ系列数（分割数）d≧2の任意数とした拡張Feistel構造であり、各ラウンドにおいて複数のF関数の並列実行を許容したタイプ2、

これらのいずれの構造に基づく暗号処理を実行するかを選択する。なお、設定情報は、例えば外部から入力する。制御回路284は、設定に応じて、各F関数専用回路の適用シーケンスを変更し、各Feistel構造に従ったラウンド関数を実行させる制御を行う。

[0261] この構成を適用することで、第1F関数（F1）専用処理回路281～第3F関数（F3）専用処理回路283を適用して様々なFeistel構造を適用した暗号処理が可能となり、暗号化処理、または復号処理の処理ビットが異なる様々なビット対応の暗号処理を実行可能となる。なお、4つ以上のF関数実行部を持つ構成も可能である。

[0262] 上述したように、拡散行列切り替え機構(DSM)を満足する線形変換行列を実行する複数の異なるF関数を決定し、これらの各F関数を実装して、F関すを適用した処理シーケンスを変更することで、

(a)データ系列数(分割数)d＝2としたFeistel構造

(b1)データ系列数(分割数)d≧2の任意数とした拡張Feistel構造であり、各ラウンドにおいて1つのF関数の実行のみを許容したタイプ1、

(b2)データ系列数(分割数)d≧2の任意数とした拡張Feistel構造であり、各ラウンドにおいて複数のF関数の並列実行を許容したタイプ2、

これらのいずれかの構造に基づく暗号処理を選択的に実行する構成が実現され、暗号化処理または復号処理における処理ビット数を変更可能な装置が実現される。

[0263] 例えば、a種類(aは2以上の整数)のF関数を構成して、上記3種類のFeistel構造に基づく暗号処理を実行し、かつ拡散行列切り替え機構(DSM)を満足させた処理構成により耐性の高い暗号処理を行なうことが可能となる。

[0264] [8. 本発明の暗号処理および暗号アルゴリズム構築処理のまとめ]

最後に、上述した本発明の暗号処理および暗号アルゴリズム構築処理についてまとめて説明する。

[0265] 本発明の暗号処理装置は、図1、図2を参照して説明したように、非線形変換処理および線形変換処理を含むデータ変換処理を実行するSP型F関数を複数ラウンド繰り返すFeistel型共通鍵ブロック暗号処理を実行する暗号処理部を有する。さらに、図5以下を参照して説明したように、暗号処理部は、データ系列数:dをd≧2の整数とした拡張Feistel構造を適用した暗号処理を実行する構成であり、各ラウンドにおけるF関数において実行する線形変換処理に、少なくとも2以上の複数の異なる行列を選択的に適用する構成を有する。

[0266] これらの2以上の複数の異なる行列は、拡散行列切り替え機構(DSM:Diffusion Switching Mechanism)を実現するように設定され、DSMにより、差分攻撃や線形攻撃に対する耐性を向上させた暗号処理が実現される。このDSMによる耐性向上の実現のため特定の条件に従った行列の選択、配置が行なわれる。

[0267] すなわち、F関数において実行する線形変換処理に適用される複数の行列として、

拡張Feistel構造の各データ系列に入力するF関数に含まれる線形変換行列に基づくデータ系列対応の最小分岐数中から選択される全データ系列中の最小分岐数が予め定めた値以上となる条件を満足する複数の異なる行列が選択され、これらの複数の異なる行列が、拡張Feistel構造の各データ系列に入力するF関数に繰り返し配置される。

[0268] さらに、具体的には、暗号処理部において利用される複数の異なる行列は、拡張Feistel構造の各データ系列s(i)に入力する連続するk個(ただし、kは2以上の整数)のF関数に含まれる線形変換行列に基づいて算出されるデータ系列対応の最小分岐数[$B_k^D(s(i))$]中から選択される全データ系列中の最小分岐数[B_k^D]が3以上となる条件を満足する複数の異なる行列である。

あるいは、拡張Feistel構造の各データ系列s(i)に入力する連続する2個のF関数に含まれる線形変換行列に基づいて算出されるデータ系列対応の最小分岐数[$B_2^L(s(i))$]中から選択される全データ系列中の最小分岐数[B_2^L]が3以上となる条件を満足する複数の異なる行列である。

[0269] 本発明の暗号処理装置の暗号処理部は、これらの複数の異なる行列を、n個(ただし、nは2以上の整数)の異なる行列を、M_0, M_1, ・・M_{n-1}としたとき、これらを、拡張Feistel構造の各データ系列に入力するF関数に順番に繰り返し配置した構成を有する。具体的な拡張Feistel構造の例としては、例えば図8、図10を参照して説明した1つのラウンドに1つのF関数のみを実行するタイプ1の拡張Feistel構造や、図9、図11を参照して説明した1つのラウンドに複数のF関数を並列に実行する拡張Feistel構造がある。

[0270] なお、本発明は、このような拡張Feistel構造を適用した暗号処理を実行する暗号処理装置および方法並びに暗号処理を実行するコンピュータ・プログラムと、さらに、上述の拡張Feistel構造を適用した暗号処理を実行するための暗号処理アルゴリズムを構築する情報処理装置、方法並びにコンピュータ・プログラムをも含むものである。

[0271] 暗号処理アルゴリズムを構築する情報処理装置は、例えば一般的なPC等の情報処理装置が適用可能であり、以下の処理ステップを実行可能な制御部を持つ。すな

わち、

データ系列数:dをd≧2の整数とした拡張Feistel構造を適用した暗号処理アルゴリズムの構成において、各ラウンドにおけるF関数において実行する線形変換処理に適用する少なくとも2以上の複数の異なる行列を決定する行列決定ステップと、

行列決定ステップにおいて決定した複数の異なる行列を、拡張Feistel構造の各データ系列に入力するF関数に繰り返し配置する行列設定ステップである。

[0272] 上述の行列決定ステップは、2以上の複数の異なる行列として、拡張Feistel構造の各データ系列に入力するF関数に含まれる線形変換行列に基づくデータ系列対応の最小分岐数中から選択される全データ系列中の最小分岐数が予め定めた値以上となる条件を満足する複数の異なる行列を適用行列として決定する処理を実行するステップとして実行される。

[0273] このような処理アルゴリズムによって設定された拡張Feistel構造を適用した暗号処理においては、拡散行列切り替え機構(DSM:Diffusion Switching Mechanism)が実現され、DSMにより、差分攻撃や線形攻撃に対する耐性を向上させた暗号処理が実現される。

[0274] [9. 暗号処理装置の構成例]

最後に、上述した実施例に従った暗号処理を実行する暗号処理装置としてのICモジュール300の構成例を図20に示す。上述の処理は、例えばPC、ICカード、リーダライタ、その他、様々な情報処理装置において実行可能であり、図20に示すICモジュール300は、これら様々な機器に構成することが可能である。

[0275] 図20に示すCPU(Central processing Unit)301は、暗号処理の開始や、終了、データの送受信の制御、各構成部間のデータ転送制御、その他の各種プログラムを実行するプロセッサである。メモリ302は、CPU301が実行するプログラム、あるいは演算パラメータなどの固定データを格納するROM(Read-Only-Memory)、CPU301の処理において実行されるプログラム、およびプログラム処理において適宜変化するパラメータの格納エリア、ワーク領域として使用されるRAM(Random Access Memory)等からなる。また、メモリ302は暗号処理に必要な鍵データや、暗号処理において適用する変換テーブル(置換表)や変換行列に適用するデータ等の格納領域として

使用可能である。なおデータ格納領域は、耐タンパ構造を持つメモリとして構成されることが好ましい。

[0276] 暗号処理部303は、例えば上述した拡張Feistel型の共通鍵ブロック暗号処理アルゴリズムに従った暗号処理、復号処理を実行する。なお、ここでは、暗号処理手段を個別モジュールとした例を示したが、このような独立した暗号処理モジュールを設けず、例えば暗号処理プログラムをROMに格納し、CPU301がROM格納プログラムを読み出して実行するように構成してもよい。

[0277] 乱数発生器304は、暗号処理に必要となる鍵の生成などにおいて必要となる乱数の発生処理を実行する。

[0278] 送受信部305は、外部とのデータ通信を実行するデータ通信処理部であり、例えばリーダライタ等、ICモジュールとのデータ通信を実行し、ICモジュール内で生成した暗号文の出力、あるいは外部のリーダライタ等の機器からのデータ入力などを実行する。

[0279] このICモジュール300は、例えば、上述した実施例に従って、データ系列数dがd≧2の整数とした拡張Feistel型暗号処理を実行する。拡張Feistel構造におけるF関数の線形変換行列として、上述した実施例に従った態様で、異なる線形変換行列を設定することで、拡散行列切り替え機構(DSM:Diffusion Switching Mechanism)が実現され、差分攻撃や線形攻撃に対する耐性を向上させることが可能となる。

[0280] 以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、特許請求の範囲の欄を参酌すべきである。

[0281] なお、明細書中において説明した一連の処理はハードウェア、またはソフトウェア、あるいは両者の複合構成によって実行することが可能である。ソフトウェアによる処理を実行する場合は、処理シーケンスを記録したプログラムを、専用のハードウェアに組み込まれたコンピュータ内のメモリにインストールして実行させるか、あるいは、各

種処理が実行可能な汎用コンピュータにプログラムをインストールして実行させることが可能である。

[0282] 例えば、プログラムは記録媒体としてのハードディスクやROM(Read Only Memory)に予め記録しておくことができる。あるいは、プログラムはフレキシブルディスク、CD－ROM(Compact Disc Read Only Memory), MO(Magneto optical)ディスク, DVD(Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体に、一時的あるいは永続的に格納(記録)しておくことができる。このようなリムーバブル記録媒体は、いわゆるパッケージソフトウエアとして提供することができる。

[0283] なお、プログラムは、上述したようなリムーバブル記録媒体からコンピュータにインストールする他、ダウンロードサイトから、コンピュータに無線転送したり、LAN(Local Area Network)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを受信し、内蔵するハードディスク等の記録媒体にインストールすることができる。

[0284] なお、明細書に記載された各種の処理は、記載に従って時系列に実行されるのみならず、処理を実行する装置の処理能力あるいは必要に応じて並列的にあるいは個別に実行されてもよい。また、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

産業上の利用可能性

[0285] 上述したように、本発明の一実施例の構成によれば、非線形変換部および線形変換部を有するSPN型のF関数を、複数ラウンド繰り返し実行するFeistel型共通鍵ブロック暗号処理において、2つのデータ系列を持つFeistel構造を拡張したFeistel構造、すなわち、例えば3つ、4つなど、2以上の任意のデータ系列を持つ拡張型のFeistel構造において、複数の異なる線形変換行列を適用したラウンド関数部を設定することで拡散行列切り替え機構(DSM)を実現し、線形解析や差分解析に対する耐性の高い共通鍵ブロック暗号アルゴリズムの構築および暗号処理の実行が可能となる。

[0286] 本発明の一実施例の構成によれば、データ系列数:dをd≧2の整数とした拡張Feistel構造を適用した暗号処理を実行する構成において、各ラウンドにおけるF関数に

おいて実行する線形変換処理に、少なくとも2以上の複数の異なる行列を選択的に適用する構成を有し、2以上の複数の異なる行列として、拡張Feistel構造の各データ系列に入力するF関数に含まれる線形変換行列に基づくデータ系列対応の最小分岐数中から選択される全データ系列中の最小分岐数が予め定めた値以上となる条件を満足する複数の異なる行列として設定することで、拡散行列切り替え機構(DSM)を実現し、線形解析や差分解析に対する耐性の高い共通鍵ブロック暗号アルゴリズムの構築および暗号処理の実行が可能となる。

[0287] さらに、本発明の一実施例の構成によれば、複数の異なる行列による異なる線形変換処理を実行するa(a≧2)種類のF関数を利用したデータ系列数:d=2axの拡張Fesitel構造(x≧1)を適用した暗号処理を実行する構成において、1つのラウンドにおいて、全種類(a種類)のF関数を均等にx個ずつ実行する構成としたので、無駄な回路を設けることのない小型の暗号処理装置が実現される。

[0288] さらに、本発明の一実施例の構成によれば、複数の異なる行列による異なる線形変換処理を実行する複数のF関数実行部を構成して、複数のF関数実行部の利用シーケンスを設定に応じて変更する構成としたことで、

(a)データ系列数d=2としたFeistel構造による暗号処理、または、

(b1)データ系列数d≧2の任意数とした拡張Feistel構造であり、各ラウンドにおいて1つのF関数の実行のみを許容した暗号処理、または、

(b2)データ系列数d≧2の任意数とした拡張Feistel構造であり、各ラウンドにおいて複数のF関数の並列実行を許容した暗号処理、

上記(a),(b1),(b2)のいずれかの暗号処理を選択的に実行することを可能とした暗号処理装置が実現される。

請求の範囲

[1] 暗号処理装置であり、

非線形変換処理および線形変換処理を含むデータ変換処理を実行するSP型F関数を複数ラウンド繰り返すFeistel型共通鍵ブロック暗号処理を実行する暗号処理部を有し、

前記暗号処理部は、

データ系列数:dをd≧2の整数とした拡張Feistel構造を適用した暗号処理を実行する構成であり、各ラウンドにおけるF関数において実行する線形変換処理に、少なくとも2以上の複数の異なる行列を選択的に適用する構成を有し、

前記2以上の複数の異なる行列は、拡張Feistel構造の各データ系列に入力するF関数に含まれる線形変換行列に基づくデータ系列対応の最小分岐数中から選択される全データ系列中の最小分岐数が予め定めた値以上となる条件を満足する複数の異なる行列であり、

前記複数の異なる行列を、拡張Feistel構造の各データ系列に入力するF関数に繰り返し配置した構成を有することを特徴とする暗号処理装置。

[2] 前記暗号処理部において利用される前記複数の異なる行列は、

拡張Feistel構造の各データ系列s(i)に入力する連続するk個(ただし、kは2以上の整数)のF関数に含まれる線形変換行列に基づいて算出されるデータ系列対応の最小分岐数$[B_k^D(s(i))]$中から選択される全データ系列中の最小分岐数$[B_k^D]$が3以上となる条件を満足する複数の異なる行列であることを特徴とする請求項1に記載の暗号処理装置。

[3] 前記暗号処理部において利用される前記複数の異なる行列は、

拡張Feistel構造の各データ系列s(i)に入力する連続する2個のF関数に含まれる線形変換行列に基づいて算出されるデータ系列対応の最小分岐数$[B_2^D(s(i))]$中から選択される全データ系列中の最小分岐数$[B_2^D]$が3以上となる条件を満足する複数の異なる行列であることを特徴とする請求項1に記載の暗号処理装置。

[4] 前記暗号処理部において利用される前記複数の異なる行列は、

拡張Feistel構造の各データ系列s(i)に入力する連続する2個のF関数に含まれる

線形変換行列に基づいて算出されるデータ系列対応の最小分岐数[$B_2^L(s(i))$]中から選択される全データ系列中の最小分岐数[B_2^L]が3以上となる条件を満足する複数の異なる行列であることを特徴とする請求項1に記載の暗号処理装置。

[5] 前記暗号処理部は、

前記複数の異なる行列を、n個（ただし、nは2以上の整数）の異なる行列、

$M_0, M_1, \cdots M_{n-1}$としたとき、

これらの異なる行列$M_0, M_1, \cdots M_{n-1}$を、拡張Feistel構造の各データ系列に入力するF関数に順番に繰り返し配置した構成を有することを特徴とする請求項1に記載の暗号処理装置。

[6] 前記暗号処理部は、

1つのラウンドに1つのF関数のみを実行する拡張Feistel構造を適用した暗号処理を実行する構成であることを特徴とする請求項1～5いずれかに記載の暗号処理装置。

[7] 前記暗号処理部は、

1つのラウンドに複数のF関数を並列に実行する拡張Feistel構造を適用した暗号処理を実行する構成であることを特徴とする請求項1～5いずれかに記載の暗号処理装置。

[8] 前記暗号処理部は、

a≧2の任意の整数、x≧1の任意の整数としたとき、前記複数の異なる行列による異なる線形変換処理を実行するa種類のF関数を利用したデータ系列数：d＝2axの拡張Fesitel構造を適用した暗号処理を実行する構成であり、

1つのラウンドにおいて、全種類（a種類）のF関数を均等にx個ずつ実行する構成であることを特徴とする請求項1～5いずれかに記載の暗号処理装置。

[9] 前記暗号処理部は、

1つのラウンドにおいて並列に実行するax個のF関数を実行するF関数実行部と、

前記F関数実行部に対するデータ入出力制御を実行する制御部とを備えた構成であることを特徴とする請求項8に記載の暗号処理装置。

[10] 前記暗号処理部は、

前記複数の異なる行列による異なる線形変換処理を実行する複数のF関数実行部と、

前記複数のF関数実行部の利用シーケンスを設定に応じて変更する制御部とを備え、

前記制御部は、

(a)データ系列数d＝2としたFeistel構造による暗号処理、または、

(b1)データ系列数d≧2の任意数とした拡張Feistel構造であり、各ラウンドにおいて1つのF関数の実行のみを許容した暗号処理、または、

(b2)データ系列数d≧2の任意数とした拡張Feistel構造であり、各ラウンドにおいて複数のF関数の並列実行を許容した暗号処理、

上記(a)，(b1)，(b2)のいずれかの暗号処理を選択的に実行する構成であることを特徴とする請求項1～5いずれかに記載の暗号処理装置。

[11] 前記制御部は、

暗号化または復号処理の対象となるデータのビット長に応じて、実行する処理形態を選択する構成であることを特徴とする請求項10に記載の暗号処理装置。

[12] 暗号処理装置において、暗号処理を実行する暗号処理方法であり、

暗号処理部において、非線形変換処理および線形変換処理を含むデータ変換処理を実行するSP型F関数を複数ラウンド繰り返すFeistel型共通鍵ブロック暗号処理を実行する暗号処理ステップを有し、

前記暗号処理ステップは、

データ系列数：dをd≧2の整数とした拡張Feistel構造を適用した暗号処理を実行するステップであり、各ラウンドにおけるF関数において実行する線形変換処理に、少なくとも2以上の複数の異なる行列を選択的に適用した演算を実行する演算ステップを有し、

前記演算ステップにおいて適用する複数の異なる行列は、拡張Feistel構造の各データ系列に入力するF関数に含まれる線形変換行列に基づくデータ系列対応の最小分岐数中から選択される全データ系列中の最小分岐数が予め定めた値以上となる条件を満足する複数の異なる行列であり、

前記演算ステップは、

拡張Feistel構造の各データ系列に入力するF関数において、前記複数の異なる行列に基づく線形変換演算を実行するステップであることを特徴とする暗号処理方法。

[13] 前記複数の異なる行列は、

拡張Feistel構造の各データ系列s(i)に入力する連続するk個(ただし、kは2以上の整数)のF関数に含まれる線形変換行列に基づいて算出されるデータ系列対応の最小分岐数$[B_k^D(s(i))]$中から選択される全データ系列中の最小分岐数$[B_k^D]$が3以上となる条件を満足する複数の異なる行列であることを特徴とする請求項12に記載の暗号処理方法。

[14] 前記複数の異なる行列は、

拡張Feistel構造の各データ系列s(i)に入力する連続する2個のF関数に含まれる線形変換行列に基づいて算出されるデータ系列対応の最小分岐数$[B_2^D(s(i))]$中から選択される全データ系列中の最小分岐数$[B_2^D]$が3以上となる条件を満足する複数の異なる行列であることを特徴とする請求項12に記載の暗号処理方法。

[15] 前記複数の異なる行列は、

拡張Feistel構造の各データ系列s(i)に入力する連続する2個のF関数に含まれる線形変換行列に基づいて算出されるデータ系列対応の最小分岐数$[B_2^L(s(i))]$中から選択される全データ系列中の最小分岐数$[B_2^L]$が3以上となる条件を満足する複数の異なる行列であることを特徴とする請求項12に記載の暗号処理方法。

[16] 前記複数の異なる行列を、n個(ただし、nは2以上の整数)の異なる行列、

$M_0, M_1, \cdots M_{n-1}$としたとき、

前記演算ステップは、

拡張Feistel構造の各データ系列に入力するF関数において、これらの異なる行列$M_0, M_1, \cdots M_{n-1}$を順番に繰り返し実行するステップであることを特徴とする請求項12に記載の暗号処理方法。

[17] 前記暗号処理ステップは、

1つのラウンドに1つのF関数のみを実行する拡張Feistel構造を適用した暗号処理

を実行するステップであることを特徴とする請求項12～16いずれかに記載の暗号処理方法。

[18] 前記暗号処理ステップは、

1つのラウンドに複数のF関数を並列に実行する拡張Feistel構造を適用した暗号処理を実行するステップであることを特徴とする請求項12～16いずれかに記載の暗号処理方法。

[19] 前記暗号処理ステップは、

a≧2の任意の整数、x≧1の任意の整数としたとき、前記複数の異なる行列による異なる線形変換処理を実行するa種類のF関数を利用したデータ系列数:d＝2axの拡張Fesitel構造を適用した暗号処理を実行するステップであり、

1つのラウンドにおいて、全種類(a種類)のF関数を均等にx個ずつ実行することを特徴とする請求項12～16いずれかに記載の暗号処理方法。

[20] 前記暗号処理ステップは、

1つのラウンドにおいて並列に実行するax個のF関数を実行するF関数実行部を適用して、前記F関数実行部に対するデータ入出力制御を実行する制御部の制御に従った暗号処理を実行するステップであることを特徴とする請求項19に記載の暗号処理方法。

[21] 前記暗号処理ステップは、

前記複数の異なる行列による異なる線形変換処理を実行する複数のF関数実行部と、

前記複数のF関数実行部の利用シーケンスを設定に応じて変更する制御部とによって暗号処理を実行し、前記制御部の制御によって、

(a)データ系列数d＝2としたFeistel構造による暗号処理、または、

(b1)データ系列数d≧2の任意数とした拡張Feistel構造であり、各ラウンドにおいて1つのF関数の実行のみを許容した暗号処理、または、

(b2)データ系列数d≧2の任意数とした拡張Feistel構造であり、各ラウンドにおいて複数のF関数の並列実行を許容した暗号処理、

上記(a)，(b1)，(b2)のいずれかの暗号処理を選択的に実行することを特徴とす

る請求項12～16いずれかに記載の暗号処理方法。

[22] 前記制御部は、暗号化または復号処理の対象となるデータのビット長に応じて、実行する処理形態を選択することを特徴とする請求項21に記載の暗号処理方法。

[23] 情報処理装置において暗号処理アルゴリズムを構築する暗号処理アルゴリズム構築方法であり、

情報処理装置における制御部が、データ系列数:dをd≧2の整数とした拡張Feistel構造を適用した暗号処理アルゴリズムの構成において、各ラウンドにおけるF関数において実行する線形変換処理に適用する少なくとも2以上の複数の異なる行列を決定する行列決定ステップと、

前記制御部が、前記行列決定ステップにおいて決定した複数の異なる行列を、拡張Feistel構造の各データ系列に入力するF関数に繰り返し配置する行列設定ステップを有し、

前記行列決定ステップは、

前記2以上の複数の異なる行列として、拡張Feistel構造の各データ系列に入力するF関数に含まれる線形変換行列に基づくデータ系列対応の最小分岐数中から選択される全データ系列中の最小分岐数が予め定めた値以上となる条件を満足する複数の異なる行列を適用行列として決定する処理を実行するステップであることを特徴とする暗号処理アルゴリズム構築方法。

[24] 暗号処理装置において、暗号処理を実行させるコンピュータ・プログラムであり、

暗号処理部において、非線形変換処理および線形変換処理を含むデータ変換処理を実行するSP型F関数を複数ラウンド繰り返すFeistel型共通鍵ブロック暗号処理を実行させる暗号処理ステップを有し、

前記暗号処理ステップは、

データ系列数:dをd≧2の整数とした拡張Feistel構造を適用した暗号処理を実行させるステップであり、各ラウンドにおけるF関数において実行する線形変換処理に、少なくとも2以上の複数の異なる行列を選択的に適用した演算を実行する演算ステップを含み、

前記演算ステップにおいて適用する複数の異なる行列は、拡張Feistel構造の各

データ系列に入力するF関数に含まれる線形変換行列に基づくデータ系列対応の最小分岐数中から選択される全データ系列中の最小分岐数が予め定めた値以上となる条件を満足する複数の異なる行列であり、

前記演算ステップは、

拡張Feistel構造の各データ系列に入力するF関数において、前記複数の異なる行列に基づく線形変換演算を実行するステップであることを特徴とするコンピュータ・プログラム。

[25] 情報処理装置において暗号処理アルゴリズムを構築させるコンピュータ・プログラムであり、

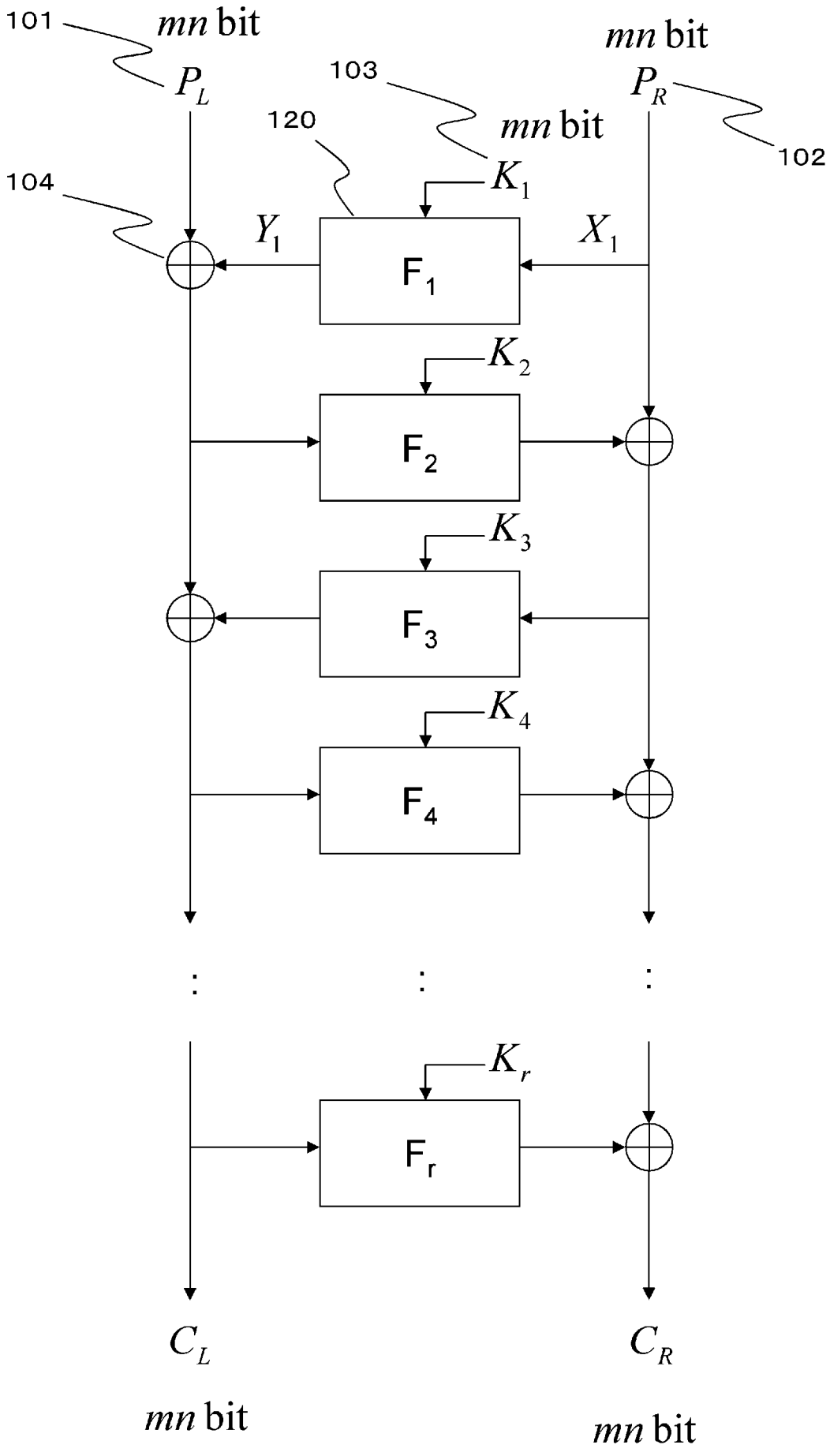
情報処理装置における制御部に、データ系列数:dをd≧2の整数とした拡張Feistel構造を適用した暗号処理アルゴリズムの構成において、各ラウンドにおけるF関数において実行する線形変換処理に適用する少なくとも2以上の複数の異なる行列を決定させる行列決定ステップと、

前記制御部に、前記行列決定ステップにおいて決定した複数の異なる行列を、拡張Feistel構造の各データ系列に入力するF関数に繰り返し配置させる行列設定ステップを有し、

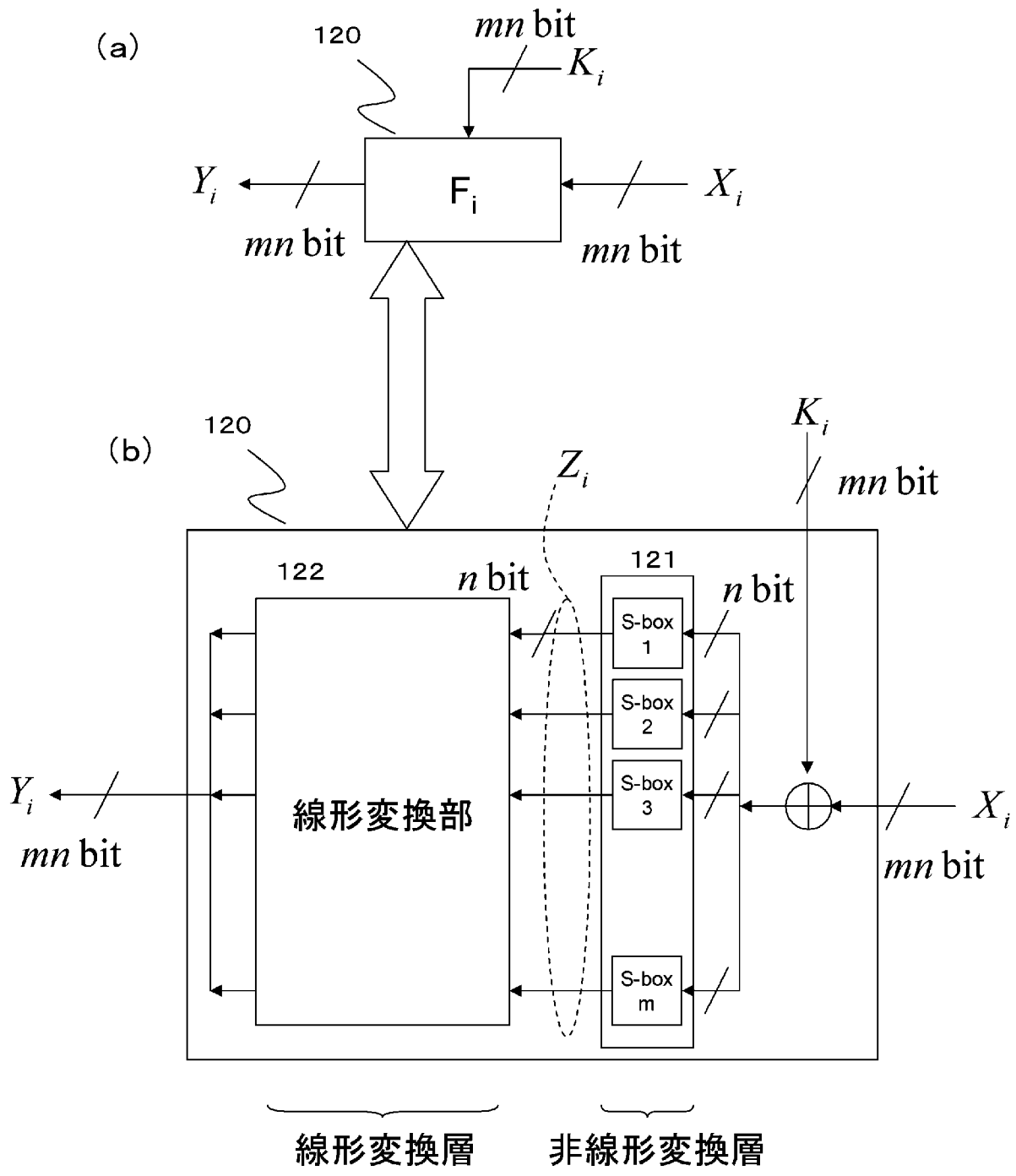
前記行列決定ステップは、

前記2以上の複数の異なる行列として、拡張Feistel構造の各データ系列に入力するF関数に含まれる線形変換行列に基づくデータ系列対応の最小分岐数中から選択される全データ系列中の最小分岐数が予め定めた値以上となる条件を満足する複数の異なる行列を適用行列として決定する処理を実行するステップであることを特徴とするコンピュータ・プログラム。

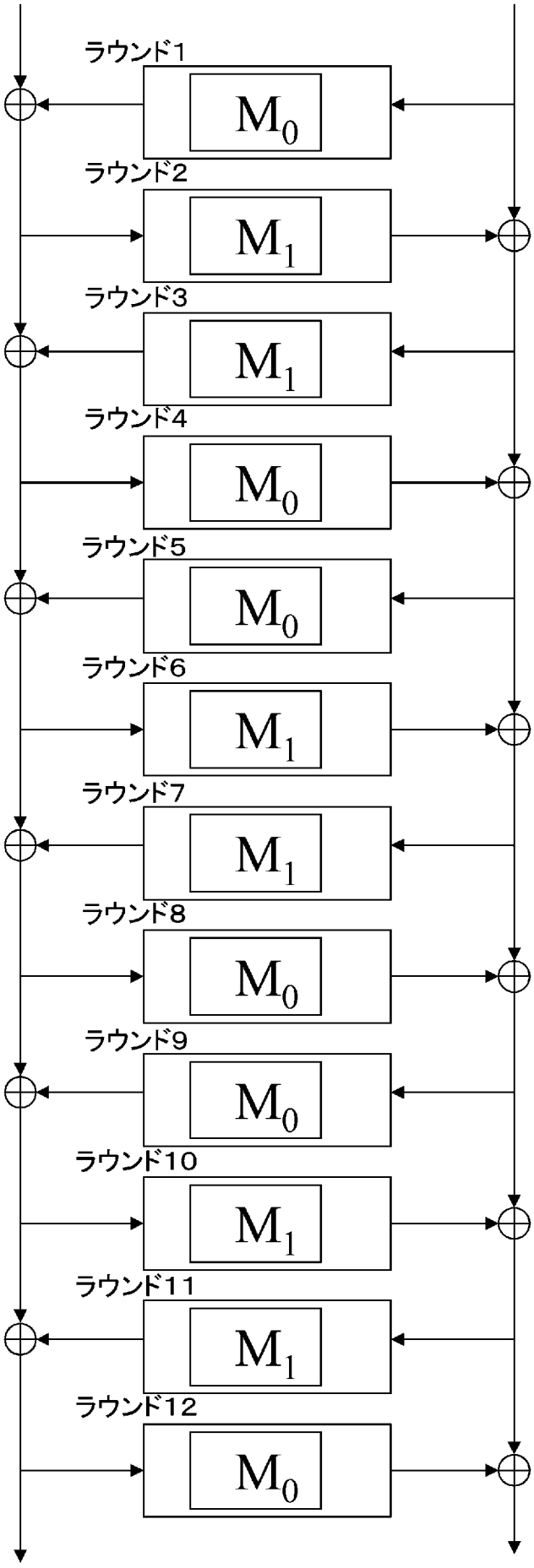
[図1]


101
mn bit
P_L
103
mn bit
P_R
102
120
K_1
104
Y_1
X_1
F_1
K_2
F_2
K_3
F_3
K_4
F_4
K_r
F_r
C_L
C_R
mn bit
mn bit

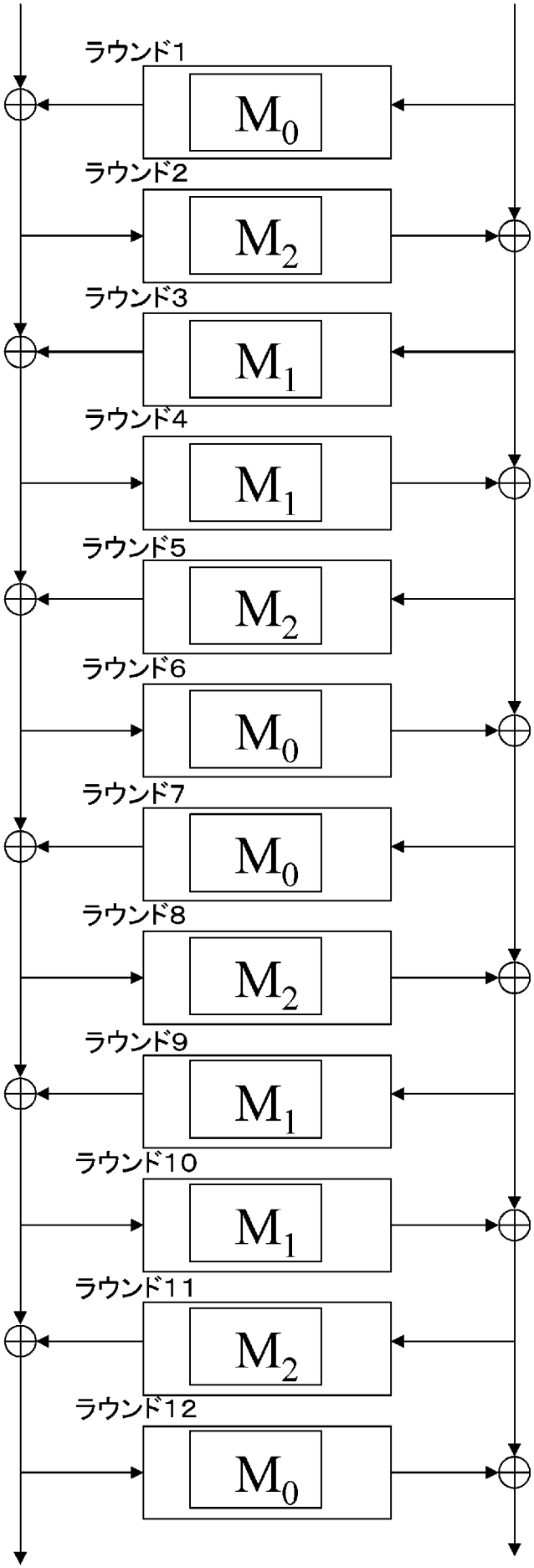
[図2]


(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
Y_i
線形変換部
X_i
mn bit
mn bit
線形変換層
非線形変換層

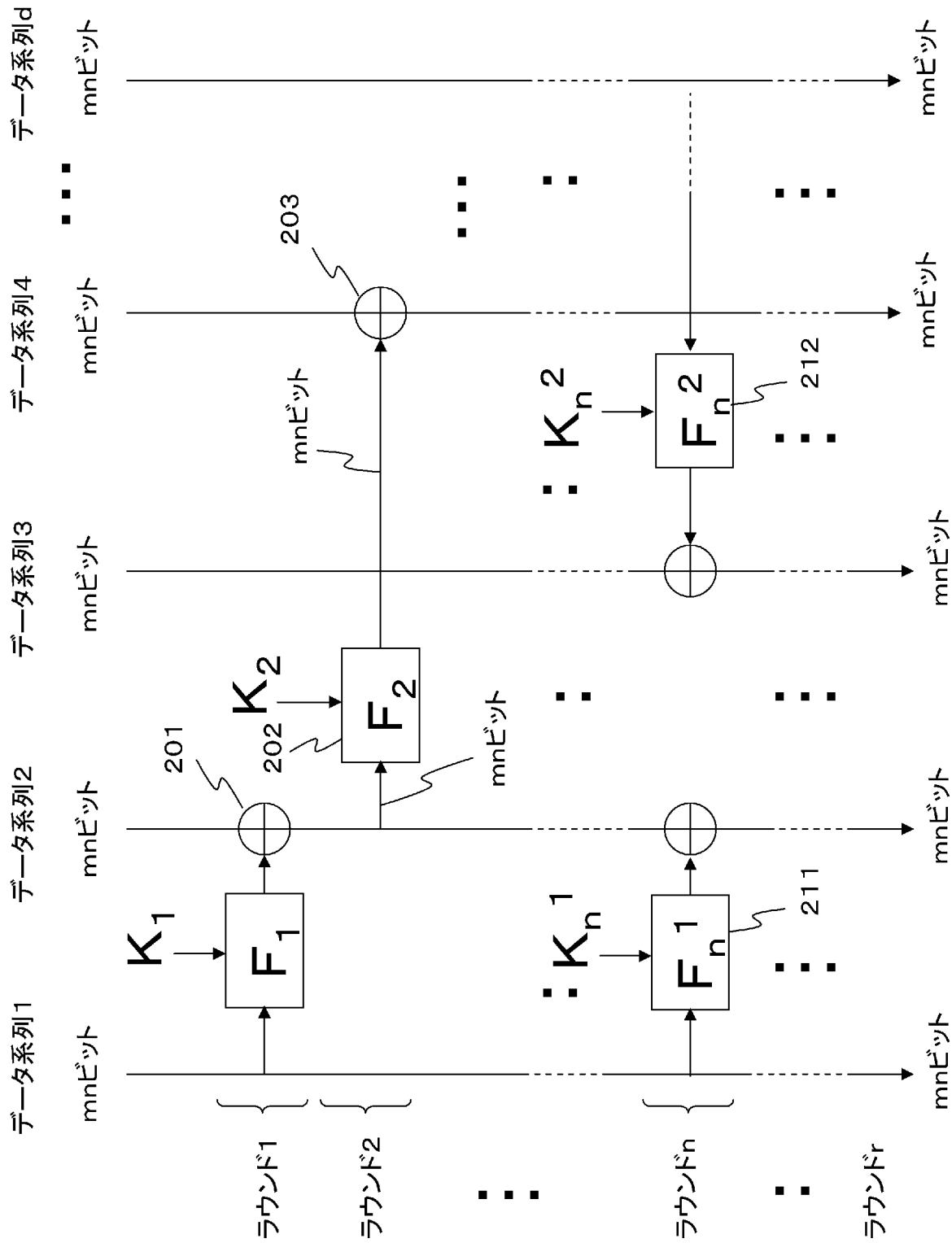
[図3]


ラウンド1
M0
ラウンド2
M1
ラウンド3
M1
ラウンド4
M0
ラウンド5
M0
ラウンド6
M1
ラウンド7
M1
ラウンド8
M0
ラウンド9
M0
ラウンド10
M1
ラウンド11
M1
ラウンド12
M0

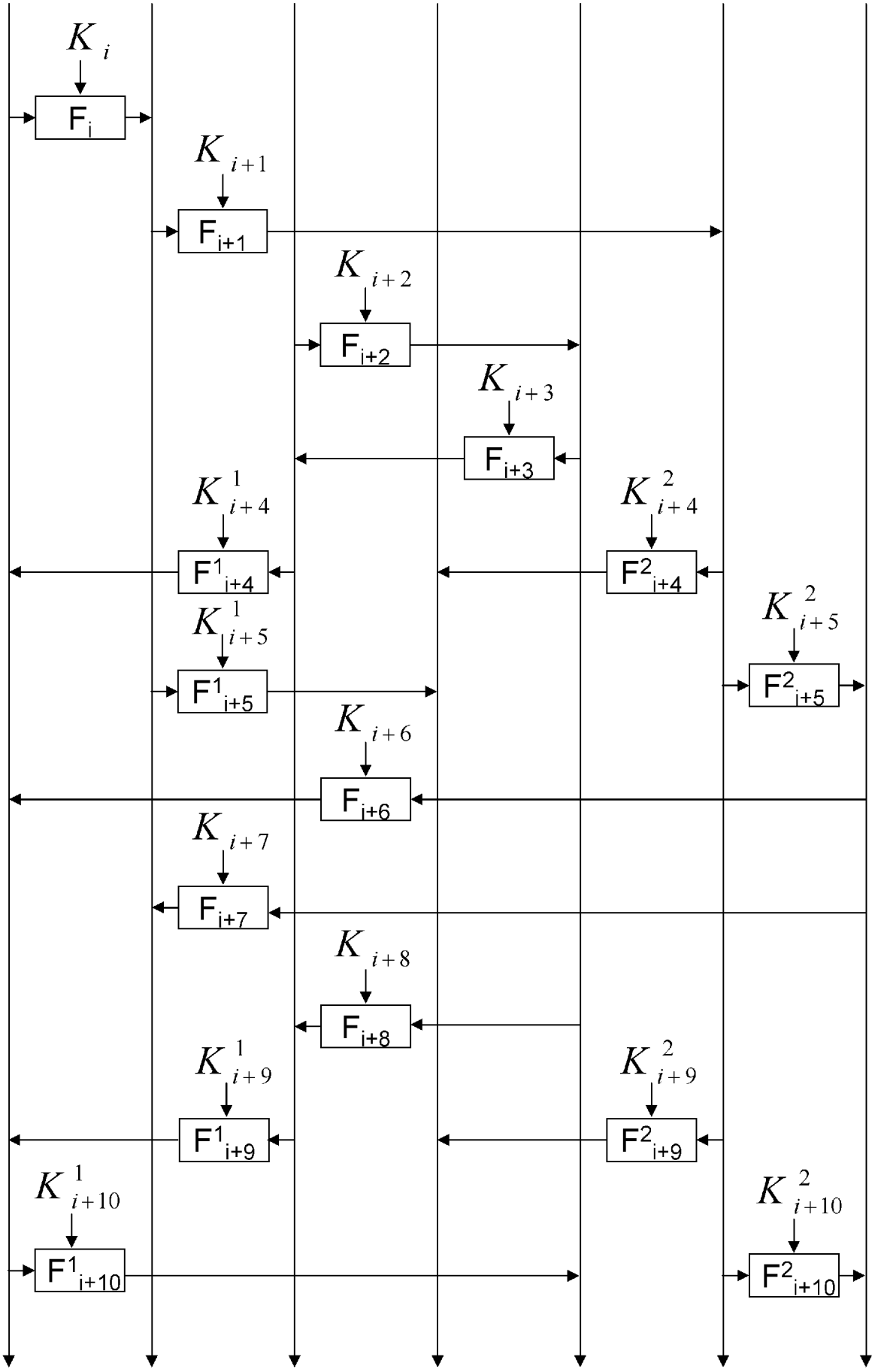
[図4]


ラウンド1
M0
ラウンド2
M2
ラウンド3
M1
ラウンド4
M1
ラウンド5
M2
ラウンド6
M0
ラウンド7
M0
ラウンド8
M2
ラウンド9
M1
ラウンド10
M1
ラウンド11
M2
ラウンド12
M0

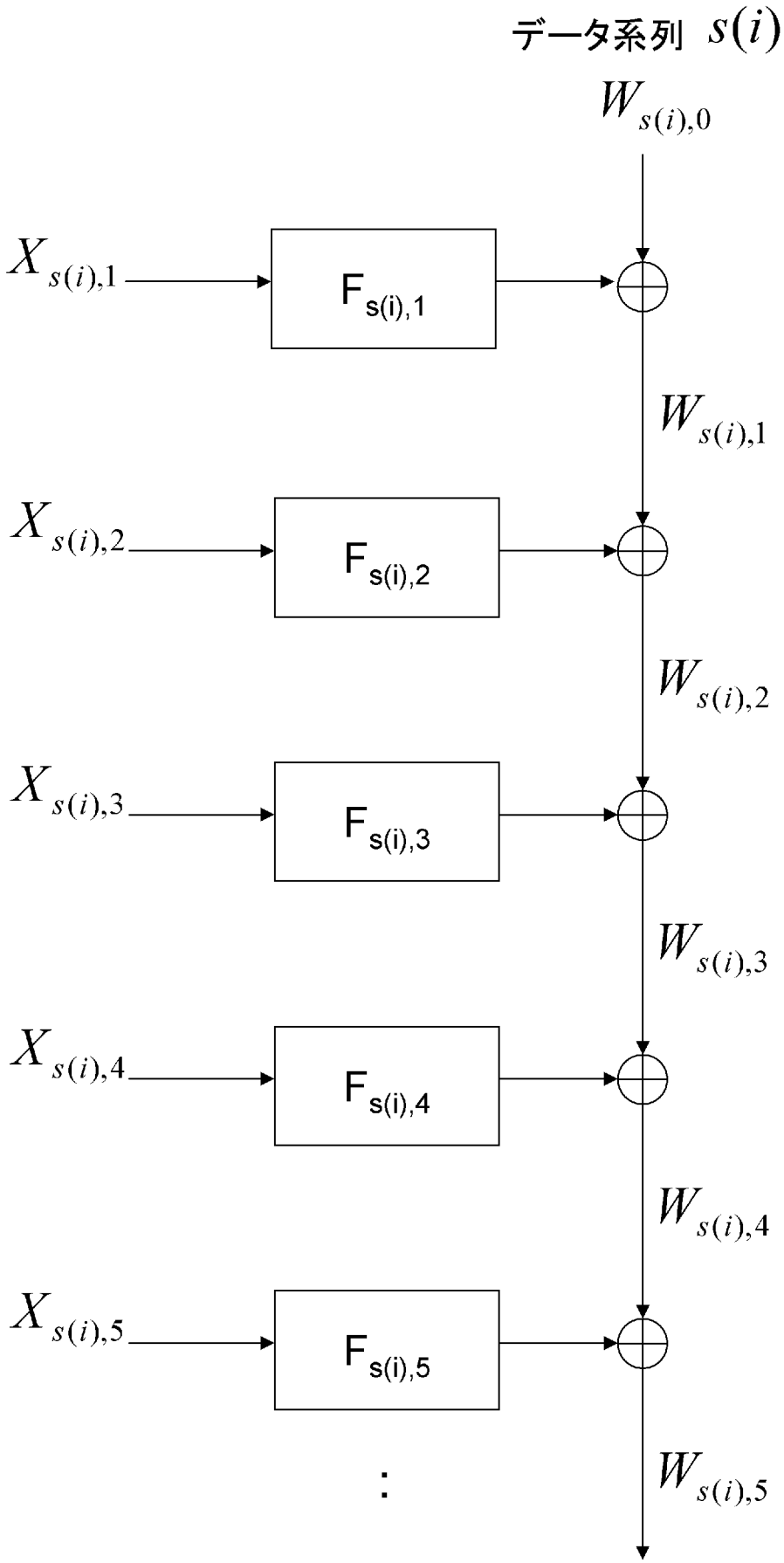
[図5]


データ系列1
データ系列2
データ系列3
データ系列4
データ系列d
mnビット
ラウンド1
ラウンド2
ラウンドn
ラウンドr
K1
F1
K2
F2
Kn1
Fn1
Kn2
Fn2
201
202
203
211
212

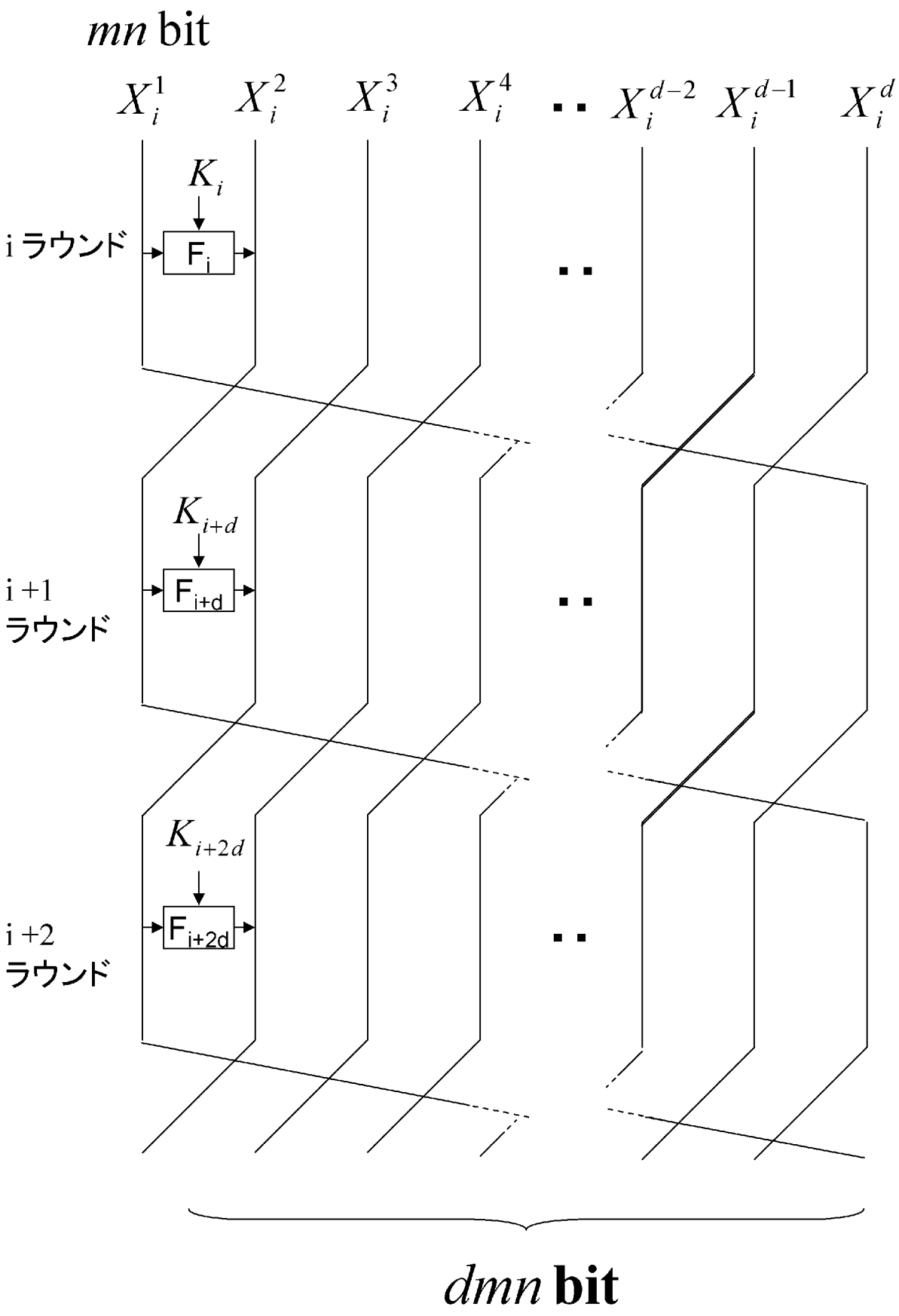
[図6]


K_i
F_i
K_{i+1}
F_{i+1}
K_{i+2}
F_{i+2}
K_{i+3}
F_{i+3}
K^1_{i+4}
F^1_{i+4}
K^2_{i+4}
F^2_{i+4}
K^1_{i+5}
F^1_{i+5}
K^2_{i+5}
F^2_{i+5}
K_{i+6}
F_{i+6}
K_{i+7}
F_{i+7}
K_{i+8}
F_{i+8}
K^1_{i+9}
F^1_{i+9}
K^2_{i+9}
F^2_{i+9}
K^1_{i+10}
F^1_{i+10}
K^2_{i+10}
F^2_{i+10}

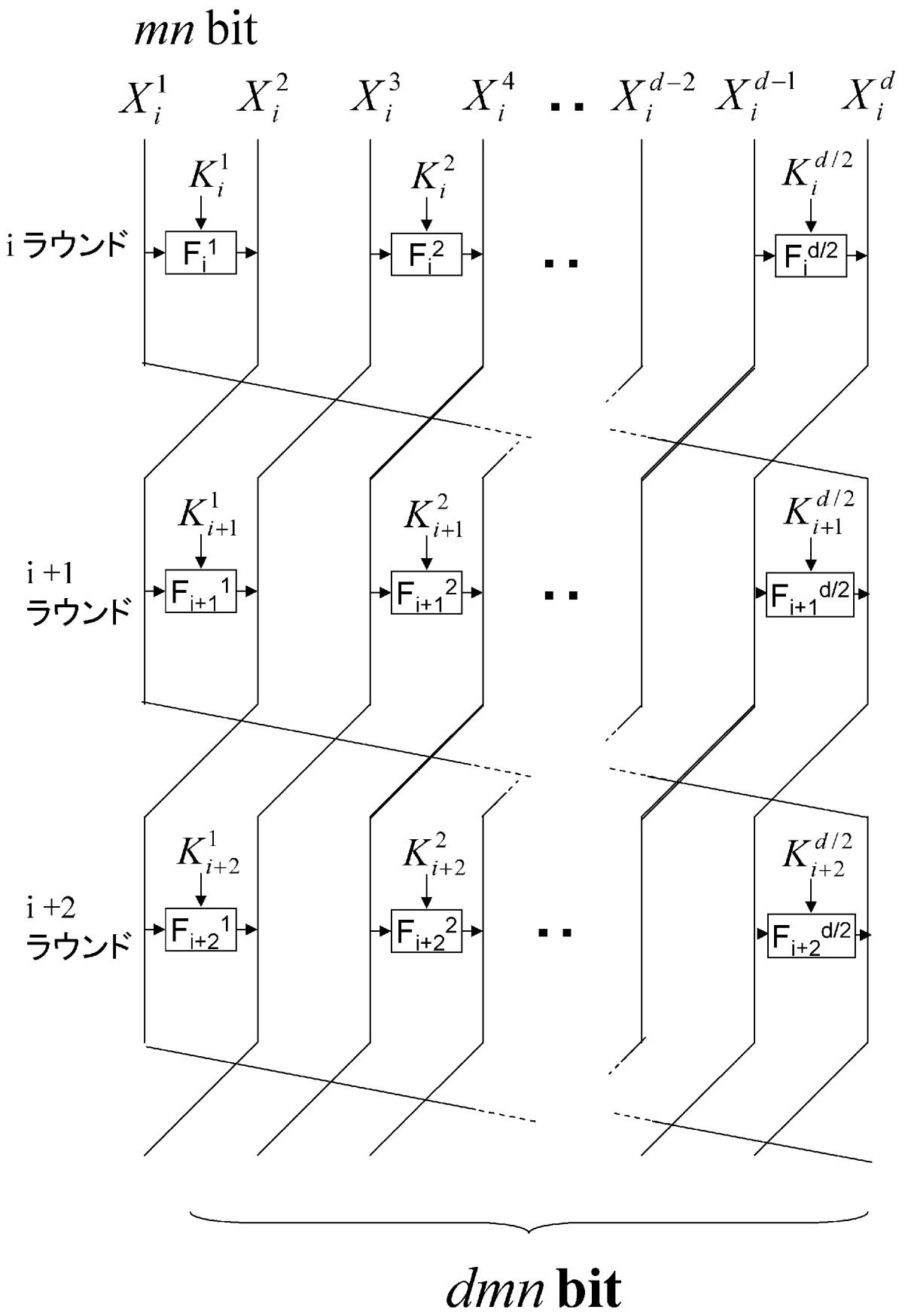
[図7]


データ系列 $s(i)$
$W_{s(i),0}$
$X_{s(i),1}$
$F_{s(i),1}$
$W_{s(i),1}$
$X_{s(i),2}$
$F_{s(i),2}$
$W_{s(i),2}$
$X_{s(i),3}$
$F_{s(i),3}$
$W_{s(i),3}$
$X_{s(i),4}$
$F_{s(i),4}$
$W_{s(i),4}$
$X_{s(i),5}$
$F_{s(i),5}$
:
$W_{s(i),5}$

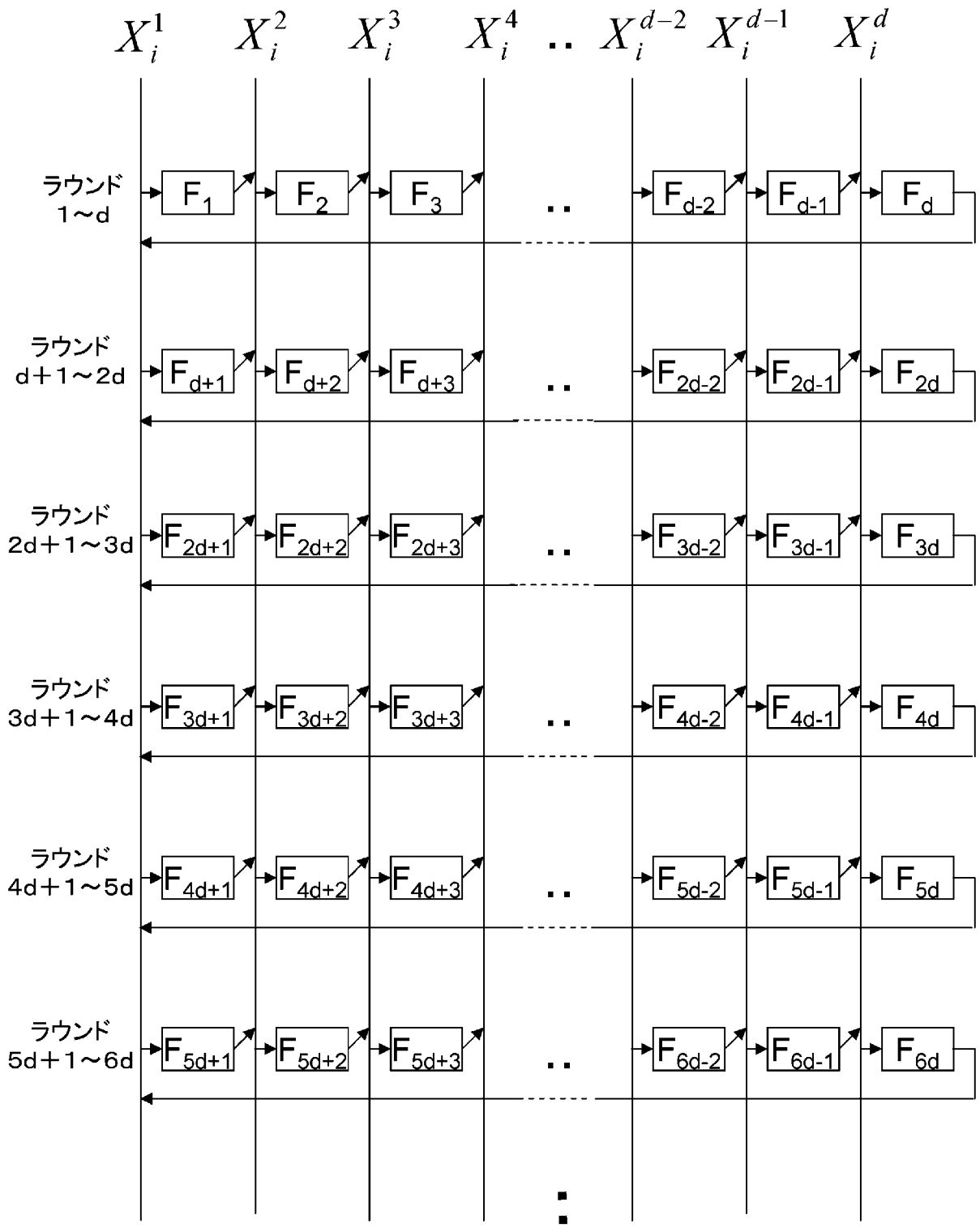
[図8]


mn bit
X_i^1 X_i^2 X_i^3 X_i^4 .. X_i^{d-2} X_i^{d-1} X_i^d
K_i
i ラウンド
F_i
K_{i+d}
i +1
ラウンド
F_{i+d}
K_{i+2d}
i +2
ラウンド
F_{i+2d}
dmn bit

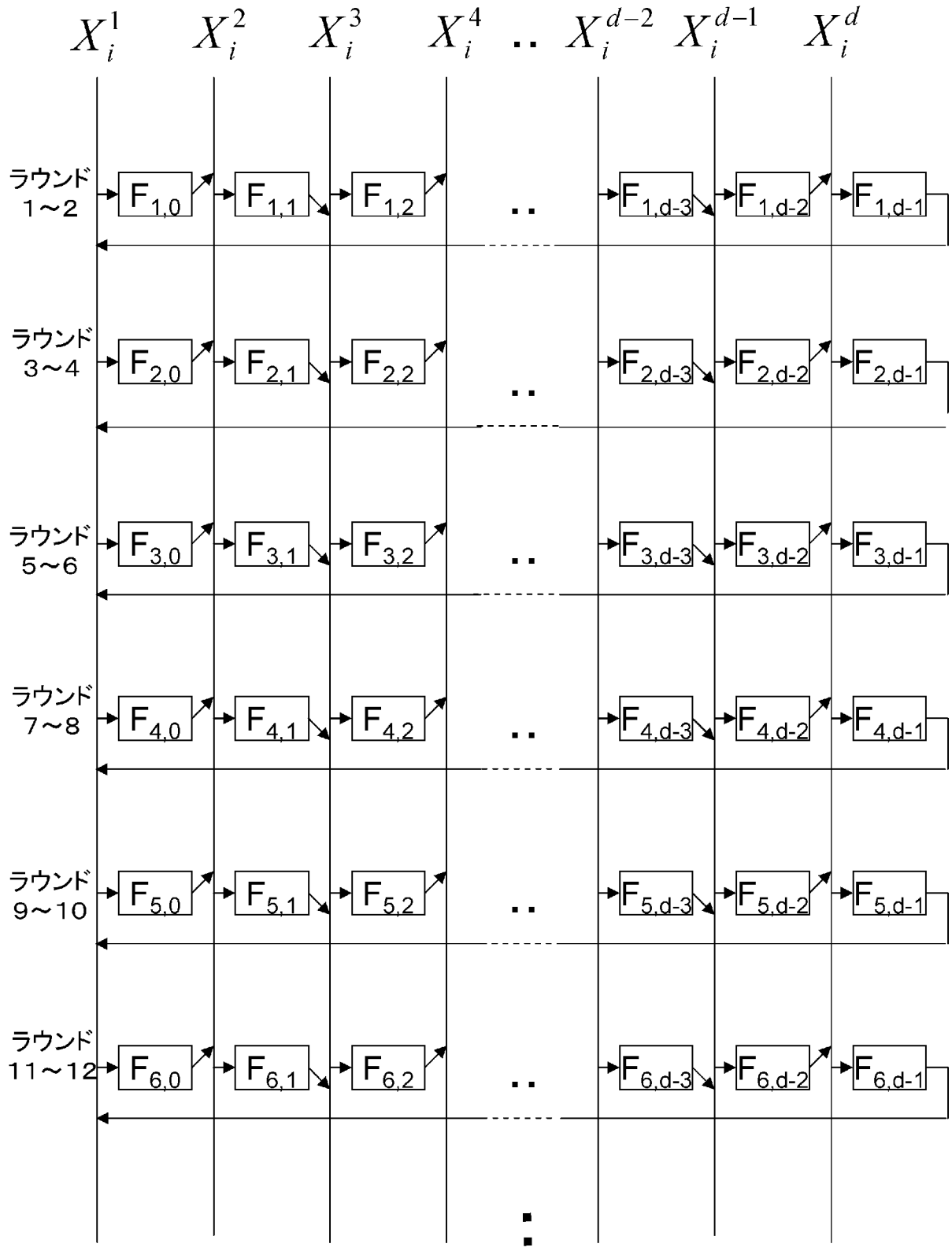
[図9]


mn bit
X_i^1 X_i^2 X_i^3 X_i^4 .. X_i^{d-2} X_i^{d-1} X_i^d
i ラウンド
i +1 ラウンド
i +2 ラウンド
K_i^1 K_i^2 $K_i^{d/2}$
K_{i+1}^1 K_{i+1}^2 $K_{i+1}^{d/2}$
K_{i+2}^1 K_{i+2}^2 $K_{i+2}^{d/2}$
F_i^1 F_i^2 $F_i^{d/2}$
F_{i+1}^1 F_{i+1}^2 $F_{i+1}^{d/2}$
F_{i+2}^1 F_{i+2}^2 $F_{i+2}^{d/2}$
dmn bit

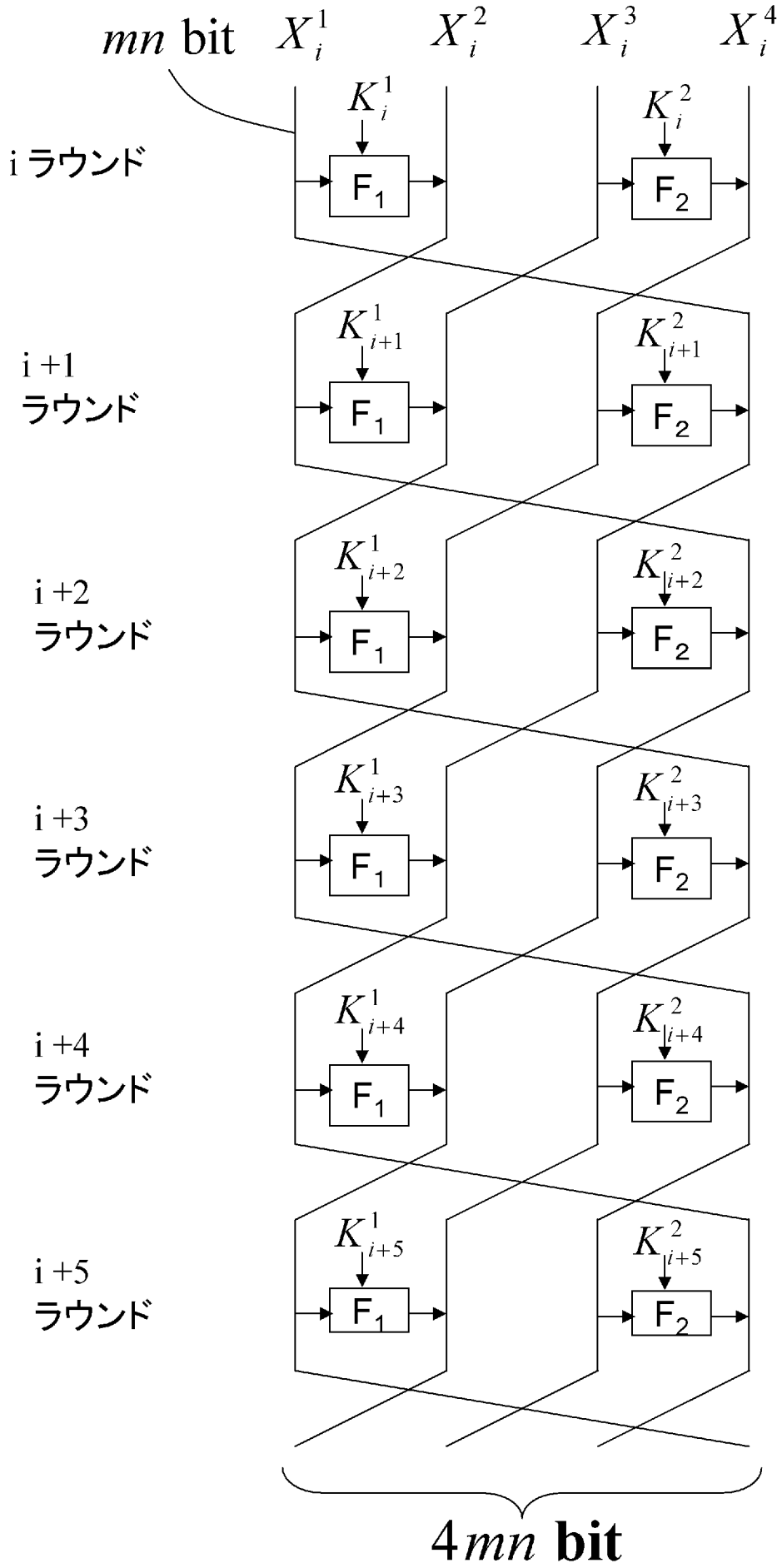
[図10]


X_i^1 X_i^2 X_i^3 X_i^4 .. X_i^{d-2} X_i^{d-1} X_i^d
ラウンド 1～d
F1 F2 F3 .. Fd-2 Fd-1 Fd
ラウンド d＋1～2d
Fd+1 Fd+2 Fd+3 .. F2d-2 F2d-1 F2d
ラウンド 2d＋1～3d
F2d+1 F2d+2 F2d+3 .. F3d-2 F3d-1 F3d
ラウンド 3d＋1～4d
F3d+1 F3d+2 F3d+3 .. F4d-2 F4d-1 F4d
ラウンド 4d＋1～5d
F4d+1 F4d+2 F4d+3 .. F5d-2 F5d-1 F5d
ラウンド 5d＋1～6d
F5d+1 F5d+2 F5d+3 .. F6d-2 F6d-1 F6d

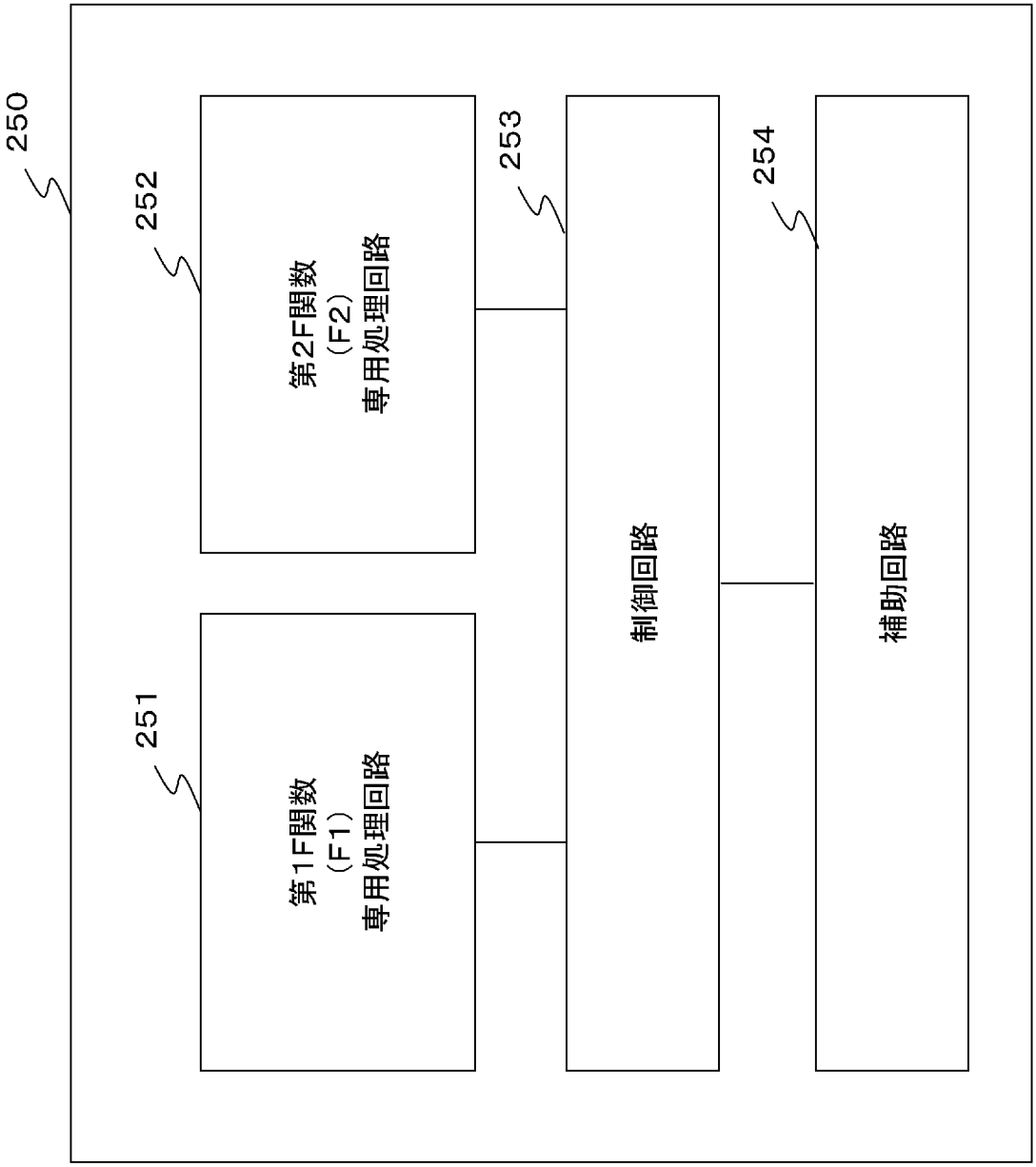
[図11]


X_i^1 X_i^2 X_i^3 X_i^4 .. X_i^{d-2} X_i^{d-1} X_i^d
ラウンド 1～2
ラウンド 3～4
ラウンド 5～6
ラウンド 7～8
ラウンド 9～10
ラウンド 11～12
$F_{1,0}$ $F_{1,1}$ $F_{1,2}$ .. $F_{1,d-3}$ $F_{1,d-2}$ $F_{1,d-1}$
$F_{2,0}$ $F_{2,1}$ $F_{2,2}$ .. $F_{2,d-3}$ $F_{2,d-2}$ $F_{2,d-1}$
$F_{3,0}$ $F_{3,1}$ $F_{3,2}$ .. $F_{3,d-3}$ $F_{3,d-2}$ $F_{3,d-1}$
$F_{4,0}$ $F_{4,1}$ $F_{4,2}$ .. $F_{4,d-3}$ $F_{4,d-2}$ $F_{4,d-1}$
$F_{5,0}$ $F_{5,1}$ $F_{5,2}$ .. $F_{5,d-3}$ $F_{5,d-2}$ $F_{5,d-1}$
$F_{6,0}$ $F_{6,1}$ $F_{6,2}$ .. $F_{6,d-3}$ $F_{6,d-2}$ $F_{6,d-1}$

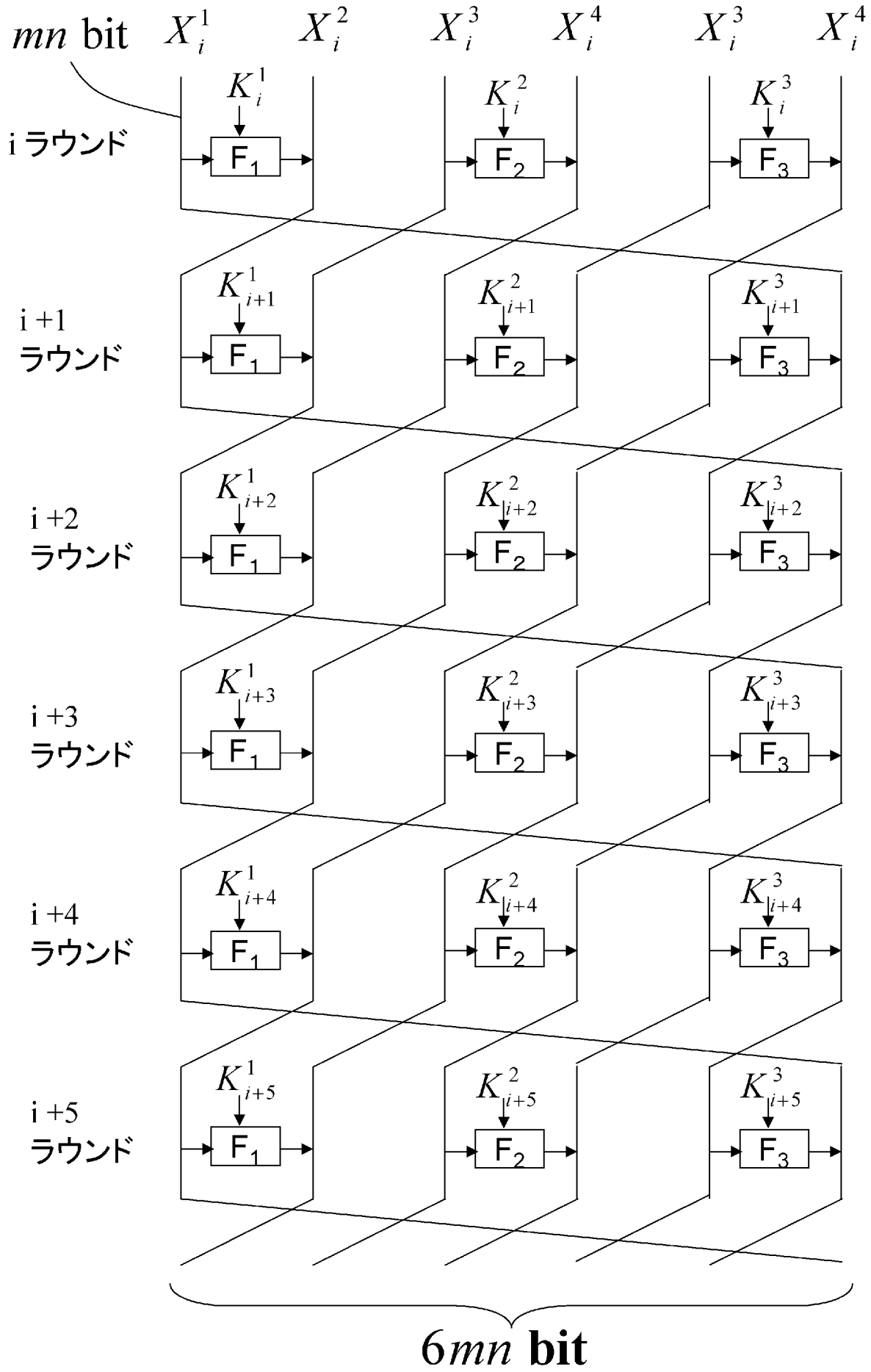
[図12]


mn bit
X_i^1
X_i^2
X_i^3
X_i^4
i ラウンド
i +1 ラウンド
i +2 ラウンド
i +3 ラウンド
i +4 ラウンド
i +5 ラウンド
K_i^1
K_i^2
K_{i+1}^1
K_{i+1}^2
K_{i+2}^1
K_{i+2}^2
K_{i+3}^1
K_{i+3}^2
K_{i+4}^1
K_{i+4}^2
K_{i+5}^1
K_{i+5}^2
F1
F2
4mn bit

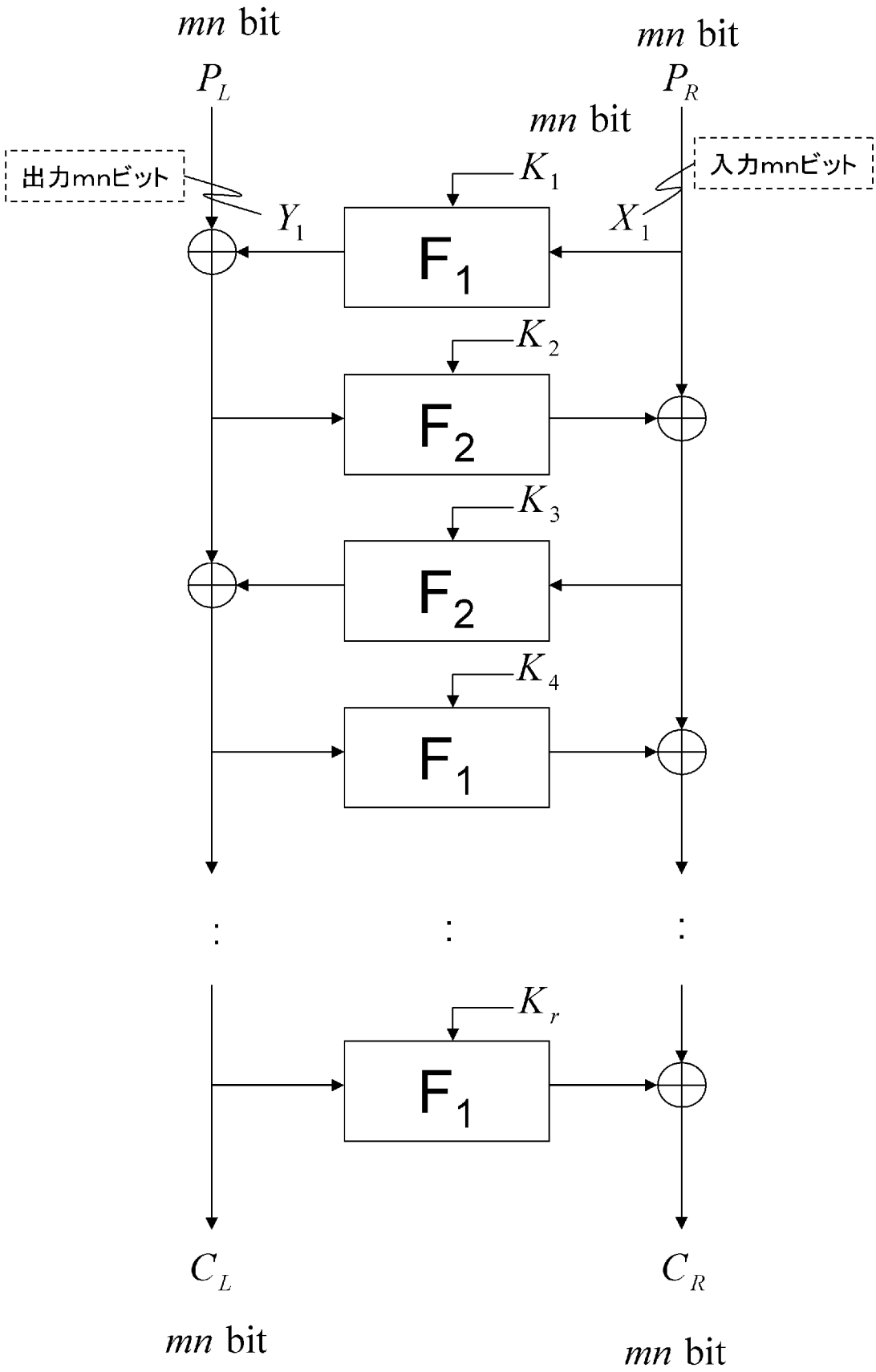
[図13]



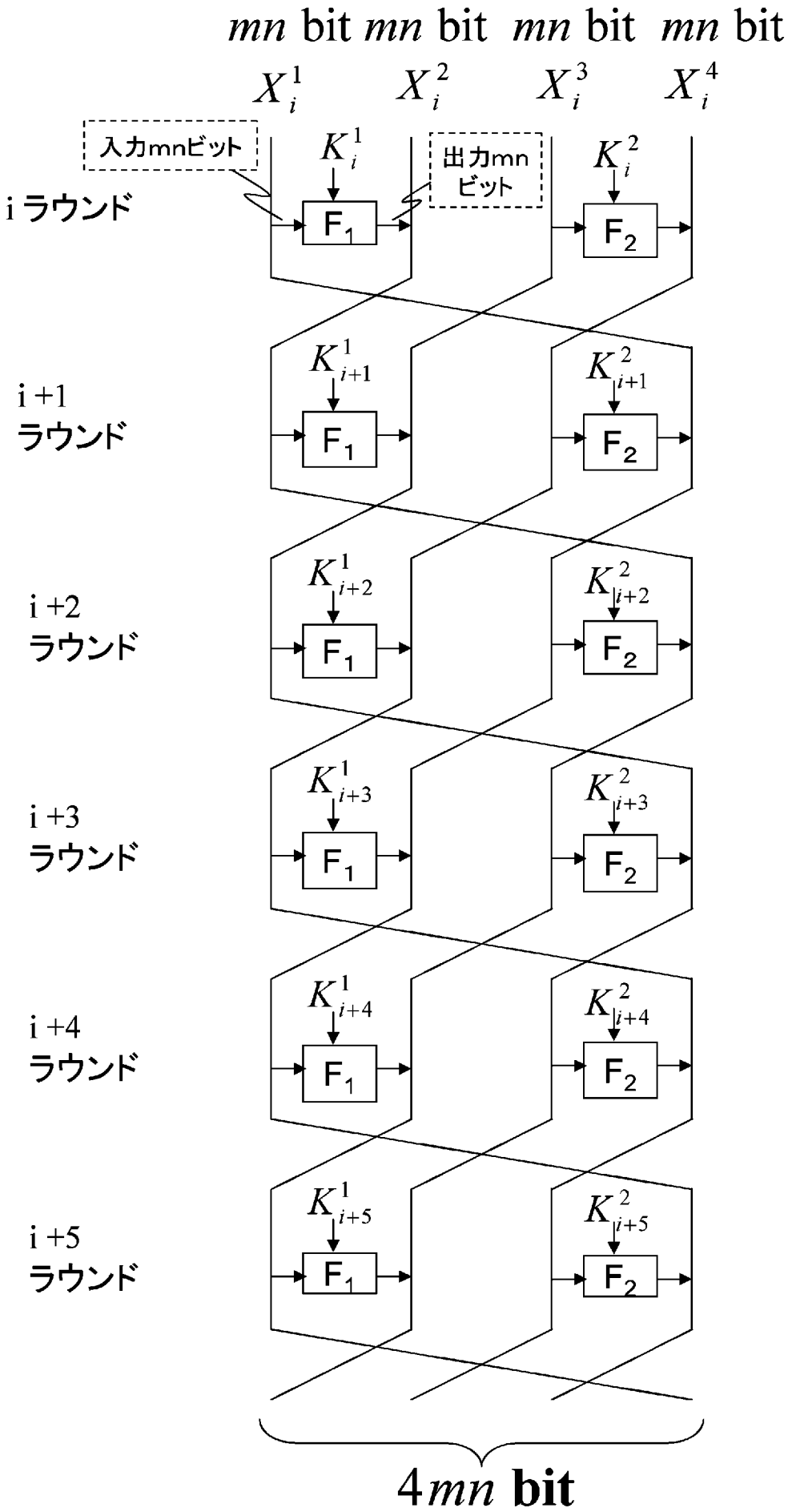
[図14]


mn bit
X_i^1
X_i^2
X_i^3
X_i^4
X_i^3
X_i^4
i ラウンド
i +1 ラウンド
i +2 ラウンド
i +3 ラウンド
i +4 ラウンド
i +5 ラウンド
K_i^1
K_i^2
K_i^3
K_{i+1}^1
K_{i+1}^2
K_{i+1}^3
K_{i+2}^1
K_{i+2}^2
K_{i+2}^3
K_{i+3}^1
K_{i+3}^2
K_{i+3}^3
K_{i+4}^1
K_{i+4}^2
K_{i+4}^3
K_{i+5}^1
K_{i+5}^2
K_{i+5}^3
F1
F2
F3
6mn bit

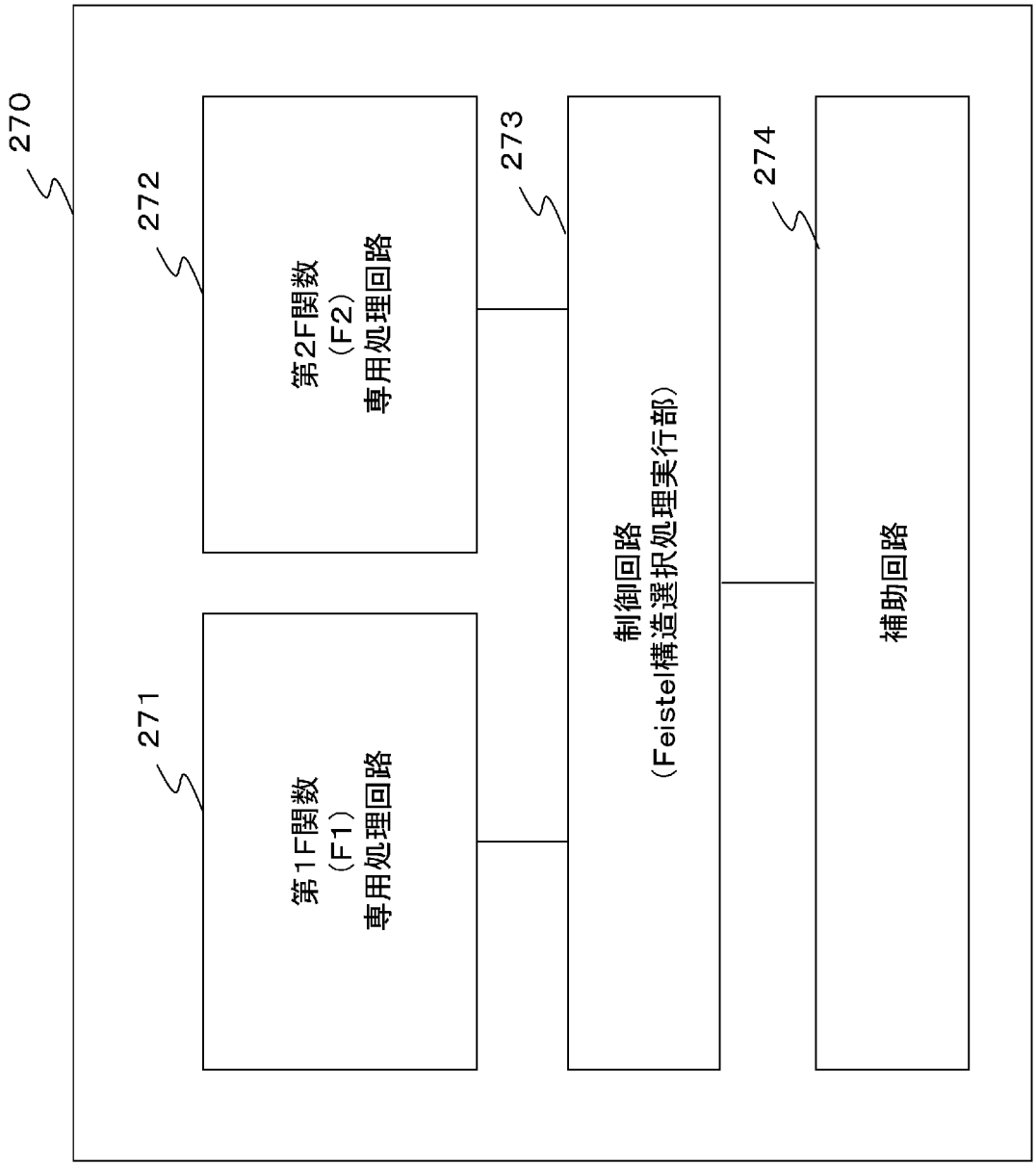
[図15]


mn bit
P_L
mn bit
P_R
mn bit
出力mnビット
入力mnビット
K_1
Y_1
X_1
F_1
K_2
F_2
K_3
F_2
K_4
F_1
K_r
F_1
C_L
C_R
mn bit
mn bit

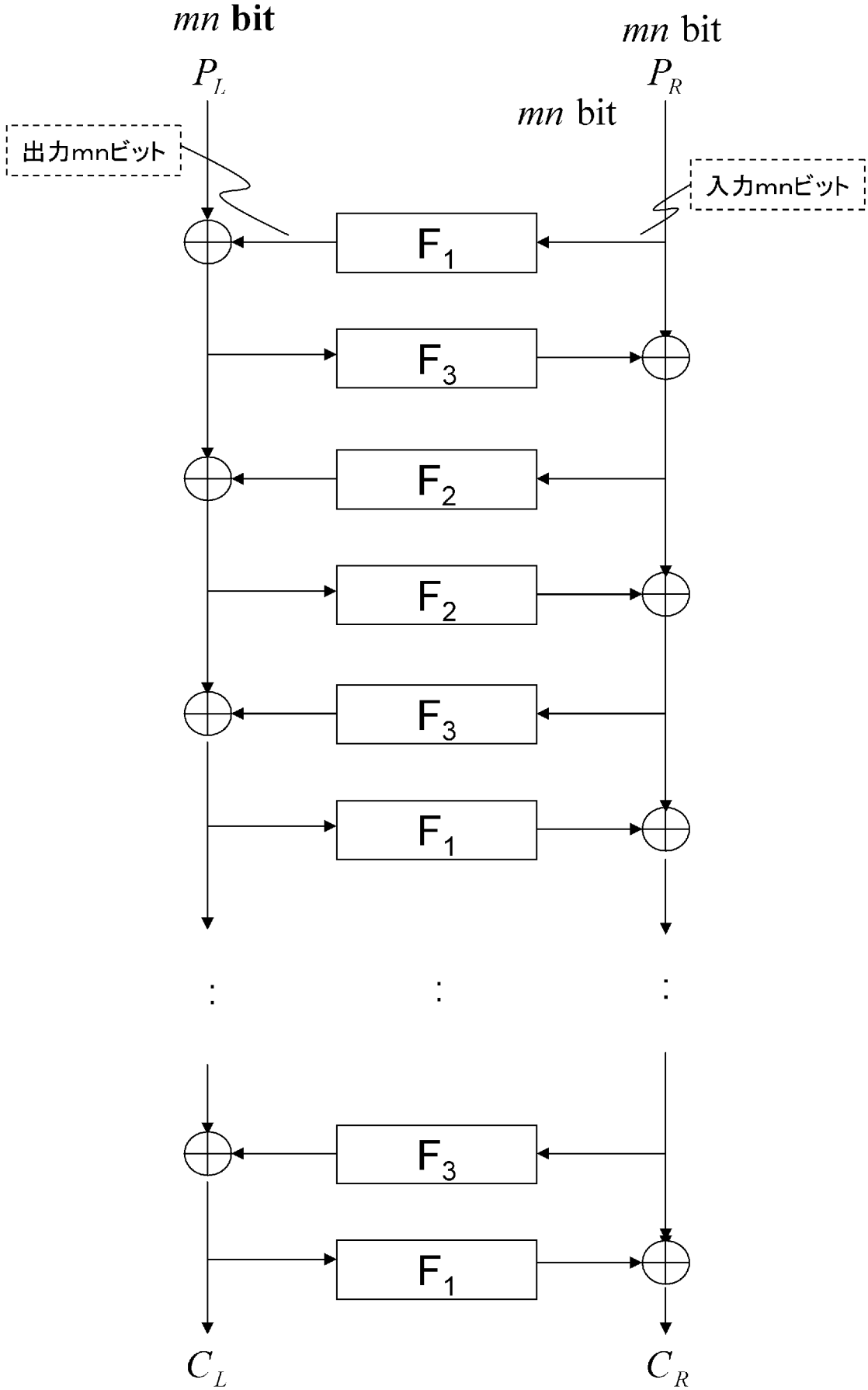
[図16]


mn bit mn bit mn bit mn bit
X_i^1 X_i^2 X_i^3 X_i^4
入力mnビット
出力mnビット
i ラウンド
i +1 ラウンド
i +2 ラウンド
i +3 ラウンド
i +4 ラウンド
i +5 ラウンド
K_i^1 K_i^2
K_{i+1}^1 K_{i+1}^2
K_{i+2}^1 K_{i+2}^2
K_{i+3}^1 K_{i+3}^2
K_{i+4}^1 K_{i+4}^2
K_{i+5}^1 K_{i+5}^2
F1
F2
4mn bit

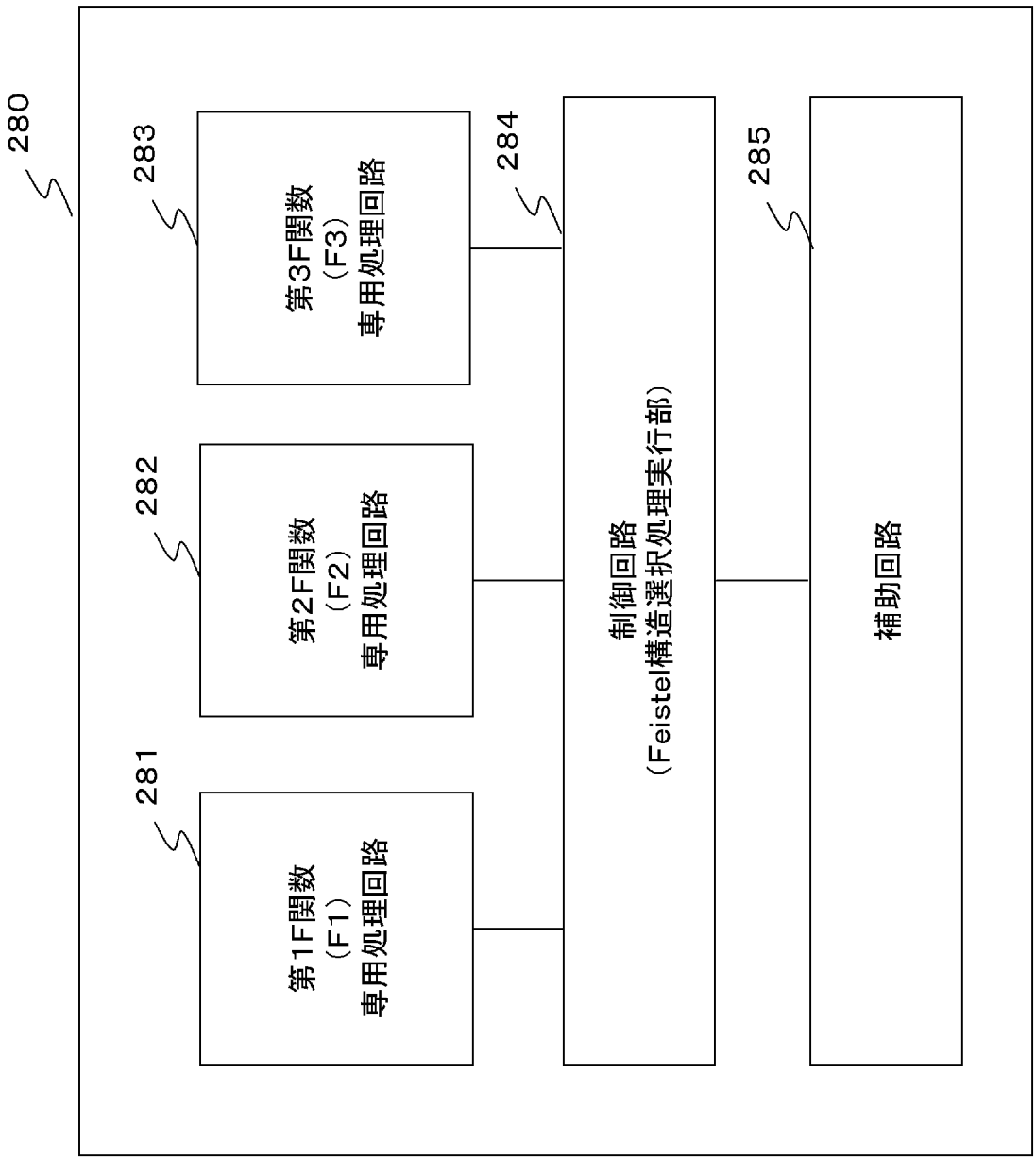
[図17]


270
271
第1F関数
(F1)
専用処理回路
272
第2F関数
(F2)
専用処理回路
273
制御回路
(Feistel構造選択処理実行部)
274
補助回路

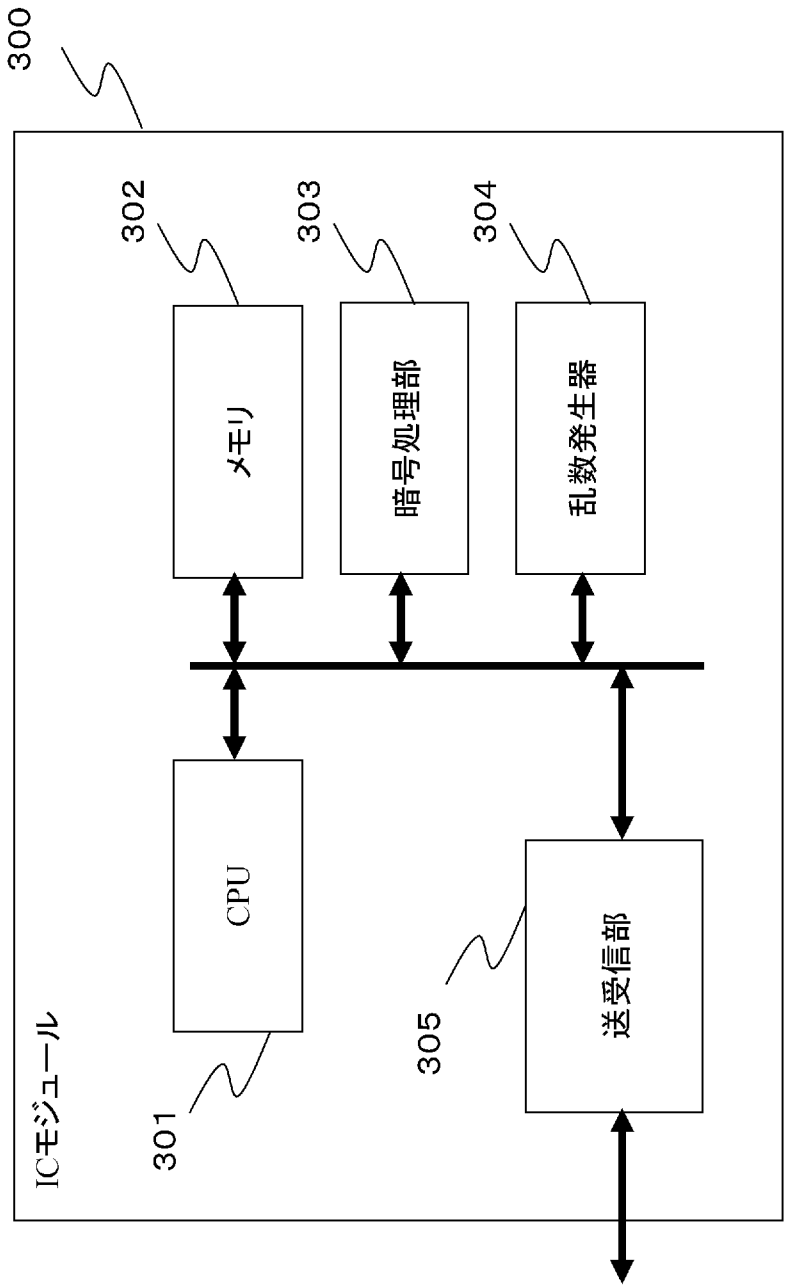
[図18]


mn bit
P_L
mn bit
P_R
mn bit
出力mnビット
入力mnビット
F_1
F_3
F_2
F_2
F_3
F_1
F_3
F_1
C_L
C_R

[図19]


280
283
第3F関数
(F3)
専用処理回路
284
285
282
第2F関数
(F2)
専用処理回路
制御回路
(Feistel構造選択処理実行部)
281
第1F関数
(F1)
専用処理回路
補助回路

[図20]



INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2007/064089

A. CLASSIFICATION OF SUBJECT MATTER
G09C1/00(2006.01)i, *H04L9/06*(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G09C1/00, H04L9/06

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2007
Kokai Jitsuyo Shinan Koho 1971-2007 Toroku Jitsuyo Shinan Koho 1994-2007

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
JSTPlus(JDream2), general, IPPAN (in Japanese), feistel

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	On Feistel Stuctures Using Diffusion Switching Mechanism, Lecture Notes in Computer Science, Vol.4047, p.41-56, 2006.03 especially 4 DSM for General Matrices, 5.4 Feistel Structures Using 2 or 3 Matrices in DSM	1-25
A	A Strategy for Constructing Fast Round Functions with Practical Security Against Differential and Linear Cryptanalysis, Lecture Notes in Computer Science, Vol.1556, p.264-279, 1999 especially 3 Relationship between Matrix Representation and Structure	1-25

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
07 August, 2007 (07.08.07)	21 August, 2007 (21.08.07)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2007/064089

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	"SPN Kozo ni okeru Senkei Henkanso no Ichi Sekkeiho", Transactions of Information Processing Society of Japan, Vol.42, No.8, pages 2087 to 2097, 2001.08. particularly, 3. Senkei Henkanso no Tansaku Shuho	1-25
A	Improving Immunity of Feistel Ciphers against Differential Cryptanalysis by Using Multiple MDS Matrices, Lecture Notes in Computer Science, Vol.3017, p.260-278, 2004 especially 2 Preliminaries, 5 Multiple MDS Feistel Structure Design	1-25
A	On Feistel Structures Using Optimal Diffusion Mappings Across Multiple Rounds, Lecture Notes in Computer Science, Vol.3329, p.1-15, 2004 especially 4 Proofs of Effectiveness of the ODM-MR Design	1-25
A	Provable Security for the Skipjack-like Structure against Differential Cryptanalysis and Linear Cryptanalysis, Lecture Notes in Computer Science, Vol.1976, p.274-288, 2000 especially 4 The Main Result - Provable Security against DC and LC in the Skipjack-like Structure	1-6,10-17, 21-25
A	Differential Cryptanalysis of CAST-256 Reduced to Nine Quad-Rounds, IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences, Vol.E84-A No.4, 2001.04.01 especially 3. Description of CAST-256	1-6,10-17, 21-25
A	JP 5-95350 A (Matsushita Electric Industrial Co., Ltd.), 16 April, 1993 (16.04.93), Particularly, Par. Nos. [0011] to [0033] (Family: none)	1-5,7-17, 19-25
P,A	The 128-bit Blockcipher CLEFIA Design Rationale, Revision 1.0 [online]. 2007.06.01 [retrieved on 2007-08-03]. Retrieved from the Internet: <URL:http://www.sony.net/Products/clefia/technical/index.html> see whole the document	1-25

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００７／０６４０８９

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　G09C1/00(2006.01)i, H04L9/06(2006.01)i

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.　G09C1/00, H04L9/06

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２００７年
日本国実用新案登録公報	１９９６－２００７年
日本国登録実用新案公報	１９９４－２００７年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

JSTPlus(JDream2), general, 一般, feistel

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
A	On Feistel Stuctures Using Diffusion Switching Mechanism, Lecture Notes in Computer Science, Vol.4047, p.41-56, 2006.03　especially 4 DSM for General Matrices, 5.4 Feistel Structures Using 2 or 3 Matrices in DSM	1-25
A	A Strategy for Constructing Fast Round Functions with Practical Security Against Differential and Linear Cryptanalysis, Lecture Notes in Computer Science, Vol.1556, p.264-279, 1999 especially 3 Relationship between Matrix Representation and Structure	1-25

☑　Ｃ欄の続きにも文献が列挙されている。　　☐　パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日 ０７．０８．２００７	国際調査報告の発送日 ２１．０８．２００７
国際調査機関の名称及びあて先 日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員）　５Ｓ　９３６４ 中里　裕正 電話番号　０３－３５８１－１１０１　内線　３５４６

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ａ	SPN 構造における線形変換層の一設計法, 情報処理学会論文誌, Vol.42 No.8, p.2087-2097, 2001.08. 特に ３．線形変換層の探索手法	1-25
Ａ	Improving Immunity of Feistel Ciphers against Differential Cryptanalysis by Using Multiple MDS Matrices, Lecture Notes in Computer Science, Vol.3017, p.260-278, 2004 especially 2 Preliminaries, 5 Multiple MDS Feistel Structure Design	1-25
Ａ	On Feistel Structures Using Optimal Diffusion Mappings Across Multiple Rounds, Lecture Notes in Computer Science, Vol.3329, p.1-15, 2004 especially 4 Proofs of Effectiveness of the ODM-MR Design	1-25
Ａ	Provable Security for the Skipjack-like Structure against Differential Cryptanalysis and Linear Cryptanalysis, Lecture Notes in Computer Science, Vol.1976, p.274-288, 2000 especially 4 The Main Result - Provable Security against DC and LC in the Skipjack-like Structure	1-6,10-17, 21-25
Ａ	Differential Cryptanalysis of CAST-256 Reduced to Nine Quad-Rounds, IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences, Vol.E84-A No.4, 2001.04.01 especially 3. Description of CAST-256	1-6,10-17, 21-25
Ａ	JP 5-95350 A（松下電器産業株式会社）1993.04.16（ファミリなし） 特に第 11-33 段落	1-5,7-17, 19-25
ＰＡ	The 128-bit Blockcipher CLEFIA Design Rationale, Revision 1.0 [online]. 2007.06.01 [retrieved on 2007-08-03]. Retrieved from the Internet: <URL:http://www.sony.net/Products/clefia/technical/index.html> see whole the document	1-25