(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 101496080 B
(45)授权公告日 2010.09.01

(21)申请号 200780028057.0

(22)申请日 2007.07.17

(30)优先权数据
206376/2006 2006.07.28 JP
224674/2006 2006.08.21 JP

(85)PCT申请进入国家阶段日
2009.01.23

(86)PCT申请的申请数据
PCT/JP2007/064089 2007.07.17

(87)PCT申请的公布数据
WO2008/013076 JA 2008.01.31

(73)专利权人 索尼株式会社
地址 日本东京都

(72)发明人 白井太三 涩谷香士

(74)专利代理机构 北京林达刘知识产权代理事务所(普通合伙) 11277
代理人 刘新宇

(51)Int.Cl.
H04L 9/06(2006.01)
G09C 1/00(2006.01)

(56)对比文件
CN 1551559 A,2004.12.01, 全文.
JP 平5-95350 A,1993.04.16, 全文.
CN 1536810 A,2004.10.13, 全文.
KANDA M. ET AL..A Strategy for Constructing Fast Round Functions withPractical Security Against Differential and LinearCryptanalysis.LECTURE NOTES IN COMPUTER SCIENCE1556.1999,1556264-279.
SHIKAI T..On Feistel Ciphers Using Optimal Diffusion Mappings AcrossMultiple Rounds.LECTURE NOTES IN COMPUTER SCIENCE3329.2004,33291-15.
SHIRAI T..On Feistel Structures Using Diffusion Switching Mechanism.LECTURE NOTES IN COMPUTER SCIENCE4047.2006,404741-56.
SUNG J. ET AL..Provable Security for the Skipjack-like StructureagainstDifferential Cryptanalysis and Linear Cryptanalysis.LECTURE NOTES IN COMPUTER SCIENCE1976.2000,1976274-288.
SHIRAI T..Improving Immunity of Feistel Ciphers against DifferentialCryptanalysis by Using Multiple MDS Matrices.LECTURE NOTES IN COMPUTER SCIENCE3017.2004,3017260-278.

审查员 王少伟

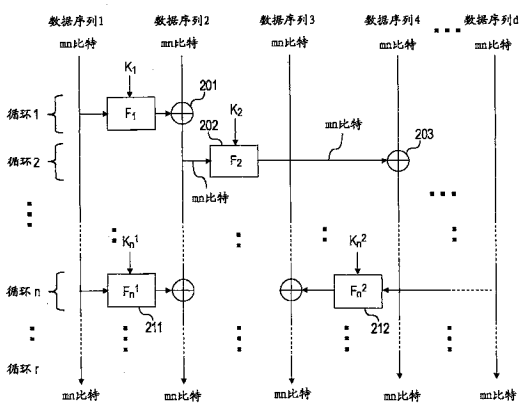
权利要求书 4 页 说明书 41 页 附图 20 页

(54)发明名称

密码处理装置、密码处理算法构建方法和密码处理方法

(57)摘要

实现应用了扩散矩阵切换机构(DSM)的扩展Feistel型共用密钥块密码处理结构。在应用了将数据序列数:d设为d≥2的整数的扩展Feistel结构的密码处理结构中,在F函数部的线性变换处理中选择性地应用多个不同的多个矩阵。作为矩阵,选择满足从基于线性变换矩阵的与数据序列对应的最小分支数中选择的全部数据序列中的最小分支数为预先决定的值以上的条件的多个不同的矩阵,其中上述线性变换矩阵包含在输入到扩展Feistel结构的各数据序列的F函数中。根据本发明,实现对基于DSM的线性分析、差分分析的抵抗性较高的共用密钥块密码。



CN 101496080 B

1. 一种密码处理装置，其特征在于，

具有密码处理部，该密码处理部执行将 SP 型 F 函数反复多次循环的 Feistel 型共用密钥块密码处理，其中，上述 SP 型 F 函数执行包括非线性变换处理和线性变换处理的数据变换处理，

上述密码处理部是执行应用了将数据序列数 :d 设为 d ≥ 2 的整数的扩展 Feistel 结构的密码处理的结构，具有在各循环的 F 函数中执行的线性变换处理中选择性地应用至少两个以上的多个不同的矩阵的结构，

其中，上述两个以上的多个不同的矩阵是满足以下条件的多个不同的矩阵 :从基于线性变换矩阵的与数据序列对应的最小分支数中选择的全部数据序列中的最小分支数为预先决定的值以上，其中，上述线性变换矩阵包含在对扩展 Feistel 结构的各数据序列进行输入的 F 函数中，

具有在对扩展 Feistel 结构的各数据序列进行输入的 F 函数中反复配置上述多个不同的矩阵的结构。

2. 根据权利要求 1 所述的密码处理装置，其特征在于，

在上述密码处理部中利用的上述多个不同的矩阵是满足以下条件的多个不同的矩阵 :从根据线性变换矩阵而算出的与数据序列对应的最小分支数 $[B_k^D(s(i))]$ 中选择的全部数据序列中的最小分支数 $[B_k^D]$ 为 3 以上，其中，上述线性变换矩阵包含在对扩展 Feistel 结构的各数据序列 s(i) 进行输入的连续的 k 个 F 函数中，其中，k 为 2 以上的整数。

3. 根据权利要求 1 所述的密码处理装置，其特征在于，

在上述密码处理部中利用的上述多个不同的矩阵是满足以下条件的多个不同的矩阵 :从根据线性变换矩阵而算出的与数据序列对应的最小分支数 $[B_2^D(s(i))]$ 中选择的全部数据序列中的最小分支数 $[B_2^D]$ 为 3 以上，其中，上述线性变换矩阵包含在对扩展 Feistel 结构的各数据序列 s(i) 进行输入的连续的两个 F 函数中。

4. 根据权利要求 1 所述的密码处理装置，其特征在于，

在上述密码处理部中利用的上述多个不同的矩阵是满足以下条件的多个不同的矩阵 :从根据线性变换矩阵而算出的与数据序列对应的最小分支数 $[B_2^L(s(i))]$ 中选择的全部数据序列中的最小分支数 $[B_2^L]$ 为 3 以上，其中，上述线性变换矩阵包含在对扩展 Feistel 结构的各数据序列 s(i) 进行输入的连续的两个 F 函数中。

5. 根据权利要求 1 所述的密码处理装置，其特征在于，

上述密码处理部具有如下结构 :

当将上述多个不同的矩阵设为 n 个不同的矩阵 M_0、M_1、..M_{n-1} 时，

在对扩展 Feistel 结构的各数据序列进行输入的 F 函数中依次反复配置这些不同的矩阵 M_0、M_1、..M_{n-1}，其中，n 为 2 以上的整数。

6. 根据权利要求 1 ～ 5 中的任一项所述的密码处理装置，其特征在于，

上述密码处理部是执行应用了在一个循环中仅执行一个 F 函数的扩展 Feistel 结构的密码处理的结构。

7. 根据权利要求 1 ～ 5 中的任一项所述的密码处理装置，其特征在于，

上述密码处理部是执行应用了在一个循环中并行地执行多个 F 函数的扩展 Feistel 结构的密码处理的结构。

8. 根据权利要求 1 ～ 5 中的任一项所述的密码处理装置，其特征在于，

上述密码处理部是如下结构 ：

在设为 a ≥ 2 的任意的整数、x ≥ 1 的任意的整数时，执行应用了数据序列数 ：d ＝ 2ax 的扩展 Feistel 结构的密码处理，其中，所述扩展 Feistel 结构利用了由上述多个不同的矩阵执行不同的线性变换处理的 a 种 F 函数，

在一个循环中均等地执行所有种类即 a 种类的 F 函数各 x 个。

9. 根据权利要求 8 所述的密码处理装置，其特征在于，

上述密码处理部具备 ：

F 函数执行部，其执行在一个循环中并行地执行的 ax 个 F 函数 ；以及

控制部，其执行对上述 F 函数执行部的数据输入输出控制。

10. 根据权利要求 1 ～ 5 中的任一项所述的密码处理装置，其特征在于，

上述密码处理部具备 ：

多个 F 函数执行部，其利用上述多个不同的矩阵执行不同的线性变换处理 ；以及

控制部，其根据设定而变更上述多个 F 函数执行部的利用顺序，

其中，上述控制部是选择性地执行 (a)、(b1)、(b2) 中的任一个的密码处理的结构，其中，上述 (a)、(b1)、(b2) 为

(a) 通过设为数据序列数 d ＝ 2 的 Feistel 结构进行的密码处理、或者

(b1) 是设为数据序列数 d ≥ 2 的任意数的扩展 Feistel 结构，在各循环中仅允许执行一个 F 函数的密码处理、或者

(b2) 是设为数据序列数 d ≥ 2 的任意数的扩展 Feistel 结构，在各循环中允许并行执行多个 F 函数的密码处理。

11. 根据权利要求 10 所述的密码处理装置，其特征在于，

上述控制部是根据成为加密或解密处理的对象的数据的比特长度来选择要执行的处理方式的结构。

12. 一种密码处理方法，在密码处理装置中执行密码处理，其特征在于，

具有密码处理步骤，在密码处理部中执行将 SP 型 F 函数反复多次循环的 Feistel 型共用密钥块密码处理，其中，上述 SP 型 F 函数执行包括非线性变换处理和线性变换处理的数据变换处理，

上述密码处理步骤是执行应用了将数据序列数 ：d 设为 d ≥ 2 的整数的扩展 Feistel 结构的密码处理的步骤，具有运算步骤，在该运算步骤中，执行在各循环的 F 函数中执行的线性变换处理中选择性地应用了至少两个以上的多个不同的矩阵的运算，

在上述运算步骤中应用的多个不同的矩阵是满足以下条件的多个不同的矩阵 ：从基于线性变换矩阵的与数据序列对应的最小分支数中选择的全部数据序列中的最小分支数为预先决定的值以上，其中，上述线性变换矩阵包含在对扩展 Feistel 结构的各数据序列进行输入的 F 函数中，

上述运算步骤是在对扩展 Feistel 结构的各数据序列进行输入的 F 函数中执行基于上述多个不同的矩阵的线性变换运算的步骤。

13. 根据权利要求 12 所述的密码处理方法，其特征在于，

上述多个不同的矩阵是满足以下条件的多个不同的矩阵 ：从根据线性变换矩阵而算出

的与数据序列对应的最小分支数 $[B_k^D(s(i))]$ 中选择的全部数据序列中的最小分支数 $[B_k^D]$ 为 3 以上，其中，上述线性变换矩阵包含在对扩展 Feistel 结构的各数据序列 s(i) 进行输入的连续的 k 个 F 函数中，其中，k 为 2 以上的整数。

14. 根据权利要求 12 所述的密码处理方法，其特征在于，

上述多个不同的矩阵是满足以下条件的多个不同的矩阵：从根据线性变换矩阵而算出的与数据序列对应的最小分支数 $[B_2^D(s(i))]$ 中选择的全部数据序列中的最小分支数 $[B_2^D]$ 为 3 以上，其中，上述线性变换矩阵包含在对扩展 Feistel 结构的各数据序列 s(i) 进行输入的连续的两个 F 函数中。

15. 根据权利要求 12 所述的密码处理方法，其特征在于，

上述多个不同的矩阵是满足以下条件的多个不同的矩阵：从根据线性变换矩阵而算出的与数据序列对应的最小分支数 $[B_2^L(s(i))]$ 中选择的全部数据序列中的最小分支数 $[B_2^L]$ 为 3 以上，其中，上述线性变换矩阵包含在对扩展 Feistel 结构的各数据序列 s(i) 进行输入的连续的两个 F 函数中。

16. 根据权利要求 12 所述的密码处理方法，其特征在于，

在将上述多个不同的矩阵设为 n 个不同的矩阵 M_0、M_1、..M_{n-1} 时，

上述运算步骤是在对扩展 Feistel 结构的各数据序列进行输入的 F 函数中依次反复执行这些不同的矩阵 M_0、M_1、..M_{n-1} 的步骤，其中，n 为 2 以上的整数。

17. 根据权利要求 12 ～ 16 中的任一项所述的密码处理方法，其特征在于，

上述密码处理步骤是执行应用了在一个循环中仅执行一个 F 函数的扩展 Feistel 结构的密码处理的步骤。

18. 根据权利要求 12 ～ 16 中的任一项所述的密码处理方法，其特征在于，

上述密码处理步骤是执行应用了在一个循环中并行地执行多个 F 函数的扩展 Feistel 结构的密码处理的步骤。

19. 根据权利要求 12 ～ 16 中的任一项所述的密码处理方法，其特征在于，

上述密码处理步骤是如下的步骤：

在设为 $a \geqslant 2$ 的任意的整数、$x \geqslant 1$ 的任意的整数时，执行应用了数据序列数：$d = 2ax$ 的扩展 Feistel 结构的密码处理，其中所述扩展 Feistel 结构利用了由上述多个不同的矩阵执行不同的线性变换处理的 a 种 F 函数

在一个循环中均等地执行所有种类即 a 种类的 F 函数各 x 个。

20. 根据权利要求 19 所述的密码处理方法，其特征在于，

上述密码处理步骤是应用 F 函数执行部，按照控制部的控制来执行密码处理的步骤，其中，上述 F 函数执行部执行在一个循环中并行地执行的 ax 个 F 函数，上述控制部执行对上述 F 函数执行部的数据输入输出控制。

21. 根据权利要求 12 ～ 16 中的任一项所述的密码处理方法，其特征在于，

在上述密码处理步骤中，

利用由上述多个不同的矩阵执行不同的线性变换处理的多个 F 函数执行部和根据设定而变更上述多个 F 函数执行部的利用顺序的控制部来执行密码处理，通过上述控制部的控制，选择性地执行 (a)、(b1)、(b2) 中的任一个的密码处理，其中，上述 (a)、(b1)、(b2) 为

(a) 通过设为数据序列数 d = 2 的 Feistel 结构进行的密码处理、或者

(b1) 是设为数据序列数 d ≥ 2 的任意数的扩展 Feistel 结构，在各循环中仅允许执行一个 F 函数的密码处理、或者

(b2) 是设为数据序列数 d ≥ 2 的任意数的扩展 Feistel 结构，在各循环中允许并行执行多个 F 函数的密码处理。

22. 根据权利要求 21 所述的密码处理方法，其特征在于，

上述控制部根据成为加密或解密处理的对象的数据的比特长度来选择要执行的处理方式。

23. 一种密码处理算法构建方法，在信息处理装置中构建密码处理算法，其特征在于，具有以下步骤：

矩阵决定步骤，在应用了将数据序列数 :d 设为 d ≥ 2 的整数的扩展 Feistel 结构的密码处理算法的结构中，信息处理装置中的控制部决定在各循环的 F 函数中执行的线性变换处理中应用的至少两个以上的多个不同的矩阵；以及

矩阵设定步骤，上述控制部在对扩展 Feistel 结构的各数据序列进行输入的 F 函数中反复配置在上述矩阵决定步骤中决定的多个不同的矩阵，

其中，上述矩阵决定步骤是执行以下处理的步骤：作为上述两个以上的多个不同的矩阵，将满足从基于线性变换矩阵的与数据序列对应的最小分支数中选择的全部数据序列中的最小分支数为预先决定的值以上的条件的多个不同的矩阵决定为应用矩阵，其中，上述线性变换矩阵包含在对扩展 Feistel 结构的各数据序列进行输入的 F 函数中。

密码处理装置、密码处理算法构建方法和密码处理方法

技术领域

[0001] 本发明涉及一种密码处理装置、密码处理算法构建方法和密码处理方法、以及计算机程序。更详细地说，涉及一种执行 Feistel 型共用密钥块密码处理的密码处理装置、密码处理算法构建方法和密码处理方法、以及计算机程序。

背景技术

[0002] 最近，随着网络通信、电子商务的发展，确保通信中的安全成为重要的问题。确保安全的方法之一是密码技术，现在实际进行着使用了各种加密方法的通信。

[0003] 例如实际应用有如下的系统：在 IC 卡等小型装置中嵌入密码处理模块，在 IC 卡与作为数据读取写入装置的读写器之间进行数据的发送接收，进行认证处理或者发送接收数据的加密、解密。

[0004] 在密码处理算法中存在各种算法，大致分类为公开密钥密码方式和共用密钥密码方式，其中，上述公开密钥密码方式将加密密钥和解密密钥设定为不同的密钥、例如公开密钥和私人密钥，上述共用密钥密码方式将加密密钥和解密密钥设定为共用的密钥。

[0005] 在共用密钥密码方式中也存在各种算法，其中之一是如下的方式：以共用密钥为基础生成多个密钥，使用所生成的多个密钥来反复执行块单位 (64 比特、128 比特等) 的数据变换处理。应用了这种密钥生成方式和数据变换处理的算法的代表方式是共用密钥块密码方式。

[0006] 作为代表的共用密钥块密码的算法，例如存在作为美国标准密码的 DES(Data Encryption Standard：数据加密标准) 算法，在各种领域中广泛使用。

[0007] 以 DES 为代表的共用密钥块密码的算法主要可分为循环函数部和密钥调度部，其中，上述循环函数部执行输入数据的变换，上述密钥调度部生成在循环函数 (F 函数) 部的各循环中应用的密钥。根据一个主密钥 (Master key)，将其输入到密钥调度部来生成在循环函数部的各循环中应用的，在各循环函数部中应用该循环密钥 (副密钥)。

[0008] 作为执行应用了这种循环函数的算法的具体结构，已知有 Feistel 结构。Feistel 结构具有如下结构：通过简单的反复被称为循环函数的变换函数，将明文变换为密文。作为记载有应用了 Feistel 结构的密码处理的文献，例如存在非专利文献 1、非专利文献 2。

[0009] 但是，例如在应用 Feistel 结构的共用密钥密码处理中，由密码分析引起的密钥的泄漏成为问题。作为密码分析或者攻击方法的代表方法，已知有差分分析 (也称为差分解读法或者差分攻击)、线性分析 (也称为线性解读法或者线性攻击)，其中，上述差分分析通过多次分析具有某个差分的输入数据 (明文) 及其输出数据 (密文) 来分析各循环函数中的应用密钥，上述线性分析根据明文和对应的密文进行分析。

[0010] 利用密码分析容易分析密钥是指其密码处理的安全性较低。在现有的密码算法中，在循环函数 (F 函数) 部的线性变换部中应用的处理 (变换矩阵) 在各级的循环中相同，因此容易进行分析，其结果导致容易分析密钥。

[0011] 作为应对这种问题的结构，提出在 Feistel 结构的循环函数 (F 函数) 部的线性变

换部中配置两个以上不同的矩阵的结构。该技术被称为扩散矩阵切换机构(DSM:Diffusion SwitchingMechanism,下面为DSM)。通过该DSM能够提高对差分攻击、线性攻击的抵抗性。

[0012] 该扩散矩阵切换机构(DSM)被表示为对于通常的具有两个数据序列的Feistel结构的应用结构。另一方面,与这种一般的具有两个数据序列的Feistel结构不同,存在具有三个以上数据序列的扩展型Feistel结构。但是,并没有公开在这种具有三个以上数据序列的扩展型Feistel结构中应用上述扩散矩阵切换机构(DSM)来提高对差分攻击、线性攻击的抵抗性的结构。

[0013] 非专利文献1:K.Nyberg,"Generalized Feistel networks",ASIACRYPT'96,Springer Verlag,1996,pp.91～104.

[0014] 非专利文献2:Yuliang Zheng,Tsutomu Matsumoto,HidekiImai:On the Construction of Block Ciphers Provably Secure andNot Relying on Any Unproved Hypotheses.CRYPTO 1989:461-480

发明内容

[0015] 发明要解决的问题

[0016] 本发明是鉴于上述问题点而完成的,其目的在于提供一种实现对线性分析、差分分析的抵抗性较高的共用密钥块密码算法的密码处理装置、密码处理算法构建方法和密码处理方法、以及计算机程序。

[0017] 更具体地说,本发明的目的在于提供如下的密码处理装置、密码处理算法构建方法和密码处理方法、以及计算机程序:在扩展具有两个数据序列的Feistel结构得到的Feistel结构、即例如具有三个、四个等两个以上的任意数据序列的扩展型Feistel结构中,设定应用了多个不同的线性变换矩阵的循环函数部,实现对线性分析、差分分析的抵抗性较高的共用密钥块密码算法。

[0018] 用于解决问题的方案

[0019] 本发明的第一侧面在于,一种密码处理装置,其特征在于,具有密码处理部,该密码处理部执行将SP型F函数反复多次循环的Feistel型共用密钥块密码处理,其中,上述SP型F函数执行包括非线性变换处理和线性变换处理的数据变换处理,上述密码处理部是执行应用了将数据序列数:d设为d≥2的整数的扩展Feistel结构的密码处理的结构,具有在各循环的F函数中执行的线性变换处理中选择性地应用至少两个以上的多个不同的矩阵的结构,上述两个以上的多个不同的矩阵是满足以下条件的多个不同的矩阵:从基于线性变换矩阵的与数据序列对应的最小分支数中选择的全部数据序列中的最小分支数为预先决定的值以上,其中,上述线性变换矩阵包含在对扩展Feistel结构的各数据序列进行输入的F函数中,具有在对扩展Feistel结构的各数据序列进行输入的F函数中反复配置上述多个不同的矩阵的结构。

[0020] 并且,在本发明的密码处理装置的一个实施方式中,其特征在于,在上述密码处理部中利用的上述多个不同的矩阵是满足以下条件的多个不同的矩阵:从根据线性变换矩阵而算出的与数据序列对应的最小分支数[B_k^D(s(i))]中选择的全部数据序列中的最小分支数[B_k^D]为3以上,其中,上述线性变换矩阵包含在对扩展Feistel结构的各数据序列s(i)进行输入的连续的k个(其中,k为2以上的整数)F函数中。

[0021] 并且，在本发明的密码处理装置的一个实施方式中，其特征在于，在上述密码处理部中利用的上述多个不同的矩阵是满足以下条件的多个不同的矩阵：从根据线性变换矩阵而算出的与数据序列对应的最小分支数 $[B_2^D(s(i))]$ 中选择的全部数据序列中的最小分支数 $[B_2^D]$ 为 3 以上，其中，上述线性变换矩阵包含在对扩展 Feistel 结构的各数据序列 s(i) 进行输入的连续的两个 F 函数中。

[0022] 并且，在本发明的密码处理装置的一个实施方式中，其特征在于，在上述密码处理部中利用的上述多个不同的矩阵是满足以下条件的多个不同的矩阵：从根据线性变换矩阵而算出的与数据序列对应的最小分支数 $[B_2^L(s(i))]$ 中选择的全部数据序列中的最小分支数 $[B_2^L]$ 为 3 以上，其中，上述线性变换矩阵包含在对扩展 Feistel 结构的各数据序列 s(i) 进行输入的连续的两个 F 函数中。

[0023] 并且，在本发明的密码处理装置的一个实施方式中，其特征在于，上述密码处理部具有如下结构：在将上述多个不同的矩阵设为 n 个（其中，n 为 2 以上的整数）不同的矩阵 M_0、M_1、・・M_{n-1} 时，在对扩展 Feistel 结构的各数据序列进行输入的 F 函数中依次反复配置这些不同的矩阵 M_0、M_1、・・M_{n-1}。

[0024] 并且，在本发明的密码处理装置的一个实施方式中，其特征在于，上述密码处理部是执行应用了在一个循环中仅执行一个 F 函数的扩展 Feistel 结构的密码处理的结构。

[0025] 并且，在本发明的密码处理装置的一个实施方式中，其特征在于，上述密码处理部是执行应用了在一个循环中并行地执行多个 F 函数的扩展 Feistel 结构的密码处理的结构。

[0026] 并且，在本发明的密码处理装置的一个实施方式中，其特征在于，上述密码处理部是如下结构：在设为 $a \geq 2$ 的任意的整数、$x \geq 1$ 的任意的整数时，执行应用了数据序列数：$d = 2ax$ 的扩展 Feistel 结构的密码处理，所述扩展 Feistel 结构利用了由上述多个不同的矩阵执行不同的线性变换处理的 a 种 F 函数，在一个循环中均等地执行所有种类（a 种类）的 F 函数各 x 个。

[0027] 并且，在本发明的密码处理装置的一个实施方式中，其特征在于，上述密码处理部具备：F 函数执行部，其执行在一个循环中并行地执行的 ax 个 F 函数；以及控制部，其执行对上述 F 函数执行部的数据输入输出控制。

[0028] 并且，在本发明的密码处理装置的一个实施方式中，其特征在于，上述密码处理部具备：多个 F 函数执行部，其利用上述多个不同的矩阵执行不同的线性变换处理；以及控制部，其根据设定而变更上述多个 F 函数执行部的利用顺序，其中，上述控制部是选择性地执行 (a)、(b1)、(b2) 中的任一个的密码处理的结构，其中，上述 (a)、(b1)、(b2) 为

[0029] (a) 通过设为数据序列数 $d = 2$ 的 Feistel 结构进行的密码处理、或者

[0030] (b1) 是设为数据序列数 $d \geq 2$ 的任意数的扩展 Feistel 结构，在各循环中仅允许执行一个 F 函数的密码处理、或者

[0031] (b2) 是设为数据序列数 $d \geq 2$ 的任意数的扩展 Feistel 结构，在各循环中允许并行执行多个 F 函数的密码处理。

[0032] 并且，在本发明的密码处理装置的一个实施方式中，其特征在于，上述控制部是根据成为加密或解密处理的对象的数据的比特长度来选择要执行的处理方式的结构。

[0033] 并且，本发明的第二侧面在于，一种密码处理方法，在密码处理装置中执行密码处

理，其特征在于，具有密码处理步骤，在密码处理部中执行将 SP 型 F 函数反复多次循环的 Feistel 型共用密钥块密码处理，其中，上述 SP 型 F 函数执行包括非线性变换处理和线性变换处理的数据变换处理，上述密码处理步骤是执行应用了将数据序列数 :d 设为 d ≥ 2 的整数的扩展 Feistel 结构的密码处理的步骤，具有运算步骤，在该运算步骤中，执行在各循环的 F 函数中执行的线性变换处理中选择性地应用了至少两个以上的多个不同的矩阵的运算，在上述运算步骤中应用的多个不同的矩阵是满足以下条件的多个不同的矩阵 :从基于线性变换矩阵的与数据序列对应的最小分支数中选择的全部数据序列中的最小分支数为预先决定的值以上，其中，上述线性变换矩阵包含在对扩展 Feistel 结构的各数据序列进行输入的 F 函数中，上述运算步骤是在对扩展 Feistel 结构的各数据序列进行输入的 F 函数中执行基于上述多个不同的矩阵的线性变换运算的步骤。

[0034] 并且，在本发明的密码处理方法的一个实施方式中，其特征在于，上述多个不同的矩阵是满足以下条件的多个不同的矩阵 :从根据线性变换矩阵而算出的与数据序列对应的最小分支数 $[B_k^D(s(i))]$ 中选择的全部数据序列中的最小分支数 $[B_k^D]$ 为 3 以上，其中，上述线性变换矩阵包含在对扩展 Feistel 结构的各数据序列 s(i) 进行输入的连续的 k 个（其中，k 为 2 以上的整数）F 函数中。

[0035] 并且，在本发明的密码处理方法的一个实施方式中，其特征在于，上述多个不同的矩阵是满足以下条件的多个不同的矩阵 :从根据线性变换矩阵而算出的与数据序列对应的最小分支数 $[B_2^D(s(i))]$ 中选择的全部数据序列中的最小分支数 $[B_2^D]$ 为 3 以上，其中，上述线性变换矩阵包含在对扩展 Feistel 结构的各数据序列 s(i) 进行输入的连续的两个 F 函数中。

[0036] 并且，在本发明的密码处理方法的一个实施方式中，其特征在于，上述多个不同的矩阵是满足以下条件的多个不同的矩阵 :从根据线性变换矩阵而算出的与数据序列对应的最小分支数 $[B_2^L(s(i))]$ 中选择的全部数据序列中的最小分支数 $[B_2^L]$ 为 3 以上，其中，上述线性变换矩阵包含在对扩展 Feistel 结构的各数据序列 s(i) 进行输入的连续的两个 F 函数中。

[0037] 并且，在本发明的密码处理方法的一个实施方式中，其特征在于，在将上述多个不同的矩阵设为 n 个（其中，n 为 2 以上的整数）不同的矩阵 M_0、M_1、・・M_{n-1} 时，上述运算步骤是在对扩展 Feistel 结构的各数据序列进行输入的 F 函数中依次反复执行这些不同的矩阵 M_0、M_1、・・M_{n-1} 的步骤。

[0038] 并且，在本发明的密码处理方法的一个实施方式中，其特征在于，上述密码处理步骤是执行应用了在一个循环中仅执行一个 F 函数的扩展 Feistel 结构的密码处理的步骤。

[0039] 并且，在本发明的密码处理方法的一个实施方式中，其特征在于，上述密码处理步骤是执行应用了在一个循环中并行地执行多个 F 函数的扩展 Feistel 结构的密码处理的步骤。

[0040] 并且，在本发明的密码处理方法的一个实施方式中，其特征在于，上述密码处理步骤是如下的步骤 :在设为 a ≥ 2 的任意的整数、x ≥ 1 的任意的整数时，执行应用了数据序列数 :d = 2ax 的扩展 Feistel 结构的密码处理，所述扩展 Feistel 结构利用了由上述多个不同的矩阵执行不同的线性变换处理的 a 种 F 函数，在一个循环中均等地执行所有种类 (a 种类）的 F 函数各 x 个。

[0041] 并且，在本发明的密码处理方法的一个实施方式中，其特征在于，上述密码处理步骤是应用 F 函数执行部，按照控制部的控制来执行密码处理的步骤，其中，上述 F 函数执行部执行在一个循环中并行地执行的 ax 个 F 函数，上述控制部执行对上述 F 函数执行部的数据输入输出控制。

[0042] 并且，在本发明的密码处理方法的一个实施方式中，其特征在于，在上述密码处理步骤中，利用由上述多个不同的矩阵执行不同的线性变换处理的多个 F 函数执行部和根据设定而变更上述多个 F 函数执行部的利用顺序的控制部来执行密码处理，通过上述控制部的控制，选择性地执行 (a)、(b1)、(b2) 中的任一个的密码处理，其中，上述 (a)、(b1)、(b2) 为

[0043] (a) 通过设为数据序列数 d ＝ 2 的 Feistel 结构进行的密码处理、或者

[0044] (b1) 是设为数据序列数 d ≥ 2 的任意数的扩展 Feistel 结构，在各循环中仅允许执行一个 F 函数的密码处理、或者

[0045] (b2) 是设为数据序列数 d ≥ 2 的任意数的扩展 Feistel 结构，在各循环中允许并行执行多个 F 函数的密码处理。

[0046] 并且，在本发明的密码处理方法的一个实施方式中，其特征在于，上述控制部根据成为加密或解密处理的对象的数据的比特长度来选择要执行的处理方式。

[0047] 并且，本发明的第三侧面在于，一种密码处理算法构建方法，在信息处理装置中构建密码处理算法，其特征在于，具有以下步骤 :矩阵决定步骤，在应用了将数据序列数 :d 设为 d ≥ 2 的整数的扩展 Feistel 结构的密码处理算法的结构中，信息处理装置中的控制部决定在各循环的 F 函数中执行的线性变换处理中应用的至少两个以上的多个不同的矩阵 ；以及矩阵设定步骤，上述控制部在对扩展 Feistel 结构的各数据序列进行输入的 F 函数中反复配置在上述矩阵决定步骤中决定的多个不同的矩阵，其中，上述矩阵决定步骤是执行以下处理的步骤 :作为上述两个以上的多个不同的矩阵，将满足从基于线性变换矩阵的与数据序列对应的最小分支数中选择的全部数据序列中的最小分支数为预先决定的值以上的条件的多个不同的矩阵决定为应用矩阵，其中，上述线性变换矩阵包含在对扩展 Feistel 结构的各数据序列进行输入的 F 函数中。

[0048] 并且，本发明的第四侧面在于，一种计算机程序，使密码处理装置执行密码处理，其特征在于，具有密码处理步骤，使密码处理部执行将 SP 型 F 函数反复多次循环的 Feistel 型共用密钥块密码处理，其中，上述 SP 型 F 函数执行包括非线性变换处理和线性变换处理的数据变换处理，上述密码处理步骤是执行应用了将数据序列数 :d 设为 d ≥ 2 的整数的扩展 Feistel 结构的密码处理的步骤，包括运算步骤，在该运算步骤中，执行在各循环的 F 函数中执行的线性变换处理中选择性地应用了至少两个以上的多个不同的矩阵的运算，在上述运算步骤中应用的多个不同的矩阵是满足以下条件的多个不同的矩阵 :从基于线性变换矩阵的与数据序列对应的最小分支数中选择的全部数据序列中的最小分支数为预先决定的值以上，其中，上述线性变换矩阵包含在对扩展 Feistel 结构的各数据序列进行输入的 F 函数中，上述运算步骤是在对扩展 Feistel 结构的各数据序列进行输入的 F 函数中执行基于上述多个不同的矩阵的线性变换运算的步骤。

[0049] 并且，本发明的第五侧面在于，一种计算机程序，在信息处理装置中构建密码处理算法，其特征在于，具有以下步骤 :矩阵决定步骤，在应用了将数据序列数 :d 设为 d ≥ 2 的

整数的扩展 Feistel 结构的密码处理算法的结构中，使信息处理装置中的控制部决定在各循环的 F 函数中执行的线性变换处理中应用的至少两个以上的多个不同的矩阵；以及矩阵设定步骤，使上述控制部在对扩展 Feistel 结构的各数据序列进行输入的 F 函数中反复配置在上述矩阵决定步骤中决定的多个不同的矩阵，其中，上述矩阵决定步骤是执行以下处理的步骤：作为上述两个以上的多个不同的矩阵，将满足从基于线性变换矩阵的与数据序列对应的最小分支数中选择的全部数据序列中的最小分支数为预先决定的值以上的条件的多个不同的矩阵决定为应用矩阵，其中，上述线性变换矩阵包含在对扩展 Feistel 结构的各数据序列进行输入的 F 函数中。

[0050] 此外，本发明的计算机程序例如是以计算机可读形式提供的能够通过存储介质、通信介质、例如 CD、FD、MO 等记录介质、或网络等通信介质来对可执行各种程序代码的计算机系统提供的计算机程序。通过以计算机可读形式提供这种程序，在计算机系统上实现与程序相应的处理。

[0051] 通过基于后述的本发明的实施例、附图的更详细的说明，本发明的进一步的其它目的、特征、优点会更清楚。此外，在本说明书中的系统是多个装置的逻辑集合结构，并不限于各结构的装置在同一壳体内。

[0052] 发明的效果

[0053] 根据本发明的一个实施例的结构，在将具有非线性变换部和线性变换部的 SP 型 F 函数反复执行多个循环的 Feistel 型共用密钥块密码处理中，在将具有两个数据序列的 Feistel 结构扩展得到的 Feistel 结构、即具有例如三个、四个等两个以上的任意的数据序列的扩展型 Feistel 结构中，通过设定应用了多个不同的线性变换矩阵的循环函数部来实现扩散矩阵切换机构 (DSM)，能够构建对线性分析、差分分析的抵抗性较高的共用密钥块密码算法以及执行密码处理。

[0054] 根据本发明的一个实施例的结构，在执行应用了将数据序列数 :d 设为 d ≥ 2 的整数的扩展 Feistel 结构的密码处理的结构中，具有在各循环的 F 函数中执行的线性变换处理中选择性地应用至少两个以上的多个不同的矩阵的结构，作为两个以上多个不同的矩阵设定为满足从基于线性变换矩阵的与数据序列对应的最小分支数中选择的全部数据序列中的最小分支数为预先决定的值以上的条件的多个不同的矩阵，由此实现扩散矩阵切换机构 (DSM)，能够构建对线性分析、差分分析的抵抗性较高的共用密钥块密码算法以及执行密码处理，其中，上述线性变换矩阵包含在对扩展 Feistel 结构的各数据序列进行输入的 F 函数中。

[0055] 并且，根据本发明的一个实施例的结构，在利用由多个不同的矩阵执行不同的线性变换处理的 a(a ≥ 2) 种 F 函数执行应用了数据序列数 :d = 2ax 的扩展 Feistel 结构 (x ≥ 1) 的密码处理的结构中，设为在一个循环中均等地执行所有种类 (a 种类) 的 F 函数各 x 个的结构，因此实现没有设置多余的电路的小型密码处理装置。

[0056] 并且，根据本发明的一个实施例的结构，设为构成由多个不同的矩阵执行不同的线性变换处理的多个 F 函数执行部、并根据设定来变更多个 F 函数执行部的利用顺序的结构，由此实现能够选择性地执行 (a)、(b1)、(b2) 中的任一个的密码处理的密码处理装置，其中，上述 (a)、(b1)、(b2) 为

[0057] (a) 通过设为数据序列数为 d = 2 的 Feistel 结构进行的密码处理、或者

[0058] (b1) 是设为数据序列数为 d ≥ 2 的任意数的扩展 Feistel 结构，在各循环中仅允许执行一个 F 函数的密码处理、或者

[0059] (b2) 是设为数据序列数为 d ≥ 2 的任意数的扩展 Feistel 结构，在各循环中允许并行执行多个 F 函数的密码处理。

附图说明

[0060] 图 1 是表示具有 Feistel 结构的代表性的共用密钥块密码的结构的图。

[0061] 图 2 是说明作为循环函数部设定的 F 函数的结构的图。

[0062] 图 3 是说明利用了两个不同的线性变换矩阵的 Feistel 型密码算法的图。

[0063] 图 4 是说明利用了三个不同的线性变换矩阵的 Feistel 型密码算法的图。

[0064] 图 5 是说明扩展 Feistel 结构的定义的图。

[0065] 图 6 是表示具有 7 个数据序列 (d = 7) 的扩展 Feistel 结构例的图。

[0066] 图 7 是说明扩展 Feistel 结构的各结构部以及各结构部的输入输出数据的定义的图。

[0067] 图 8 是说明对于扩展 Feistel 结构的类型 1 的 DSM 应用的图。

[0068] 图 9 是说明对于扩展 Feistel 结构的类型 2 的 DSM 应用的图。

[0069] 图 10 是说明对于扩展 Feistel 结构的类型 1 的 DSM 应用的图。

[0070] 图 11 是说明对于扩展 Feistel 结构的类型 2 的 DSM 应用的图。

[0071] 图 12 是说明提高了扩展 Feistel 结构的安装效率的结构的图。

[0072] 图 13 是说明提高了扩展 Feistel 结构的安装效率的硬件结构例的图。

[0073] 图 14 是说明用于有效安装三种 F 函数的配置例的图。

[0074] 图 15 是表示设为数据序列 d = 2 的 Feistel 结构的 2mn 比特的块密码结构的图。

[0075] 图 16 是表示满足扩散矩阵切换机构 (DSM) 的数据序列数 d = 4 的扩展 Feistel 结构的图。

[0076] 图 17 是说明能够执行不同比特数的块密码的电路共用结构的图。

[0077] 图 18 是说明应用了三种 F 函数 F1、F2、F3 的 F 函数的数据序列 d = 2 的 Feistel 结构的图。

[0078] 图 19 是说明执行三种 F 函数 F1、F2、F3 的密码处理装置的结构例的图。

[0079] 图 20 是表示作为本发明所涉及的执行密码处理的密码处理装置的 IC 模块的结构例的图。

具体实施方式

[0080] 下面，详细说明本发明的密码处理装置和密码处理方法、以及计算机程序。按照以下项目进行说明。

[0081] 1. 具有 SP 型 F 函数的 Feistel 结构

[0082] 2. 分支数运算函数和抵抗性评价函数

[0083] 2-1. 分支数运算函数 :Branch()

[0084] 2-2. 对差分攻击的抵抗性评价指标

[0085] 2-3. 对线性攻击的抵抗性评价指标

[0086] 3. 对于具有两个数据序列的 Feistel 结构的 DSM 的设定方法

[0087] 4. 扩展 Feistel 结构中的 DSM 的设定

[0088] 4-1. 关于扩展 Feistel 结构

[0089] 4-2. 在扩展 Feistel 结构中用于提高对差分攻击的抵抗性的结构

[0090] 4-2-1. 使最小分支数 B_2^D 的值为 3 以上的 F 函数中的矩阵选择结构

[0091] 4-2-2. 使最小分支数 B_k^D 的值为 3 以上的 F 函数中的矩阵选择结构

[0092] 4-3. 在扩展 Feistel 结构中用于提高对线性攻击的抵抗性的结构

[0093] 4-3-1. 使最小分支数 B_2^L 的值为 3 以上的 F 函数中的矩阵选择结构

[0094] 5. 对于具有特定形式的扩展 Feistel 结构的 DSM 的利用结构

[0095] 5-1. 对于扩展 Feistel 结构的类型 1 的 DSM 的应用

[0096] 5-2. 对于扩展 Feistel 结构的类型 2 的 DSM 的应用

[0097] 6. 扩展 Feistel 结构的各类型的有效 S-box 数与基于 F 函数中的线性变换矩阵的最小分支数之间的关系式的证明

[0098] 6-1. 扩展 Feistel 结构的类型 1 的有效 S-box 数与基于 F 函数中的线性变换矩阵的最小分支数之间的关系式的证明

[0099] 6-2. 扩展 Feistel 结构的类型 2 的有效 S-box 数与基于 F 函数中的线性变换矩阵的最小分支数之间的关系式的证明

[0100] 7. 基于 F 函数的设定以及利用处理的方法的安装中的改进结构

[0101] 7-1. 扩展 Feistel 的类型 2 的有效的 F 函数配置方法

[0102] 7-2. Feistel 结构与扩展 Feistel 结构中的部件的共用化

[0103] 8. 本发明的密码处理以及密码算法构建处理的归纳

[0104] 9. 密码处理装置的结构例

[0105] 首先，说明具有 SP 型 F 函数的 Feistel 结构。作为共用密钥块密码的设计，已知有 Feistel 结构。Feistel 结构具有如下结构：通过被称为循环函数的基本处理单位的重复，将明文变换为密文。

[0106] 参照图 1 说明 Feistel 结构的基本结构。在图 1 中示出具有 r 个循环的循环数＝r 的具有两个数据序列的 Feistel 结构的例子。此外，循环数 r 是在设计阶段决定的参数，例如是能够根据所输入的密钥的长度而改变的值。

[0107] 在图 1 所示的 Feistel 结构中，将作为加密对象而输入的明文的长度设为 2mn 比特。其中，m、n 都是整数。首先，将 2mn 比特的明文分割为 mn 比特的两个输入数据 P_L(Plain-Left：左明文)101、P_R(Plain-Right：右明文)102，并将其设为输入值。

[0108] 以被称为循环函数的基本处理单位的重复来表现 Feistel 结构，各循环中所包含的数据变换函数被称为 F 函数 120。在图 1 的结构中，示出有 F 函数（循环函数）120 重复了 r 级的结构例。

[0109] 例如在第一个循环中，将 mn 比特的输入数据 X 和从密钥生成部（未图示）输入的 mn 比特的循环密钥 $K_1$103 输入到 F 函数 120，在 F 函数 120 中进行数据变换处理之后输出 mn 比特的数据 Y。在异或部 104 中对输出与来自另一方前级的输入数据（第 1 级的情况下是输入数据 P_L）进行异或运算，并向下一个循环函数输出 mn 比特的运算结果。应用该处理、即仅反复应用 F 函数决定的循环数 (r) 来完成加密处理，输出密文的分割数据 C_L(Cipher-Left：

左密码）、C_R(Cipher-Right :右密码）。通过以上结构得出 Feistel 结构的解密处理只要使插入循环密钥的顺序反转即可、不需要构成反函数。

[0110] 参照图 2 说明设定为各循环的函数的 F 函数 120 的结构。图 2 的 (a) 是表示对一个循环中的 F 函数 120 的输入以及输出的图，图 2 的 (b) 是表示 F 函数 120 的详细结构的图。如图 2 的 (b) 所示，F 函数 120 具有连接了非线性变换层 (S 层）和线性变换层 (P 层）的所谓的 SP 型结构。

[0111] 图 2 所示的 F 函数 120 是输入输出比特长度具有 m×n(m、n 为整数）比特的设定的函数。在 SP 型 F 函数内部中，首先执行密钥数据 K_i 与数据 X_i 之间的异或，然后应用非线性变换层 (S 层），接着应用线性变换层 (P 层）。

[0112] 具体地说，在非线性变换层 (S 层）中排列了 m 个被称为 S 盒 (S-box)121 的 n 比特输入 n 比特输出的非线性变换表，将 mn 比特的数据以每 n 比特进行分割、并分别输入到对应的 S 盒 (S-box)121 来变换数据。在各 S 盒中例如执行应用了变换表的非线性变换处理。

[0113] 线性变换层 (P 层）由线性变换部 122 构成，对线性变换部 122 输入来自 S 盒 121 的作为输出数据的 mn 比特的输出值 Z，线性变换部 122 对该输入实施线性变换而输出 mn 比特的结果。线性变换部 122 执行输入比特位置的替换处理等线性变换处理，输出 mn 比特的输出值 Y。该输出值 Y 与来自前级的输入数据进行异或，被设为下一个循环的 F 函数的输入值。

[0114] 此外，在下面说明的本实施例的结构中，将在作为线性变换层 (P 层）的线性变换部 122 中执行的线性变换定义为应用在 GF(2) 上定义的 mn×mn 矩阵而进行的线性变换，另外，将包含在第 i 个循环中的矩阵称为 M_i。此外，将在本发明中说明的结构中的作为非线性变换部的 S 盒和线性变换都设为双射。

[0115] 接着，说明为了理解本发明而需要的分支数运算函数和抵抗性评价函数。

[0116] (2-1. 分支数运算函数 :Branch())

[0117] 将作为在线性变换部 122 中执行的线性变换的例子的最优扩散变换 (Optimal Diffusion Mappings) 的分支数运算函数 :Branch() 定义为如下，其中，上述线性变换部 122 作为上述 F 函数内的线性变换层 (P 层）。

[0118] 对于进行从 n×a 比特数据向 n×b 比特数据的线性变换的映射，

[0119] $\theta : \{0,1\}^{na} \rightarrow \{0,1\}^{nb}$

[0120] 将分支数 :$Branch_n(\theta)$ 定义为如下。

[0121] $Branch_n(\theta) = \min_{\alpha \neq 0}\{hw_n(\alpha)+hw_n(\theta(\alpha))\}$

[0122] 其中，将 $\min_{\alpha \neq 0}\{X_\alpha\}$ 设为表示满足 $\alpha \neq 0$ 的所有 X_α 中的最小值的 X_α，将 $hw_n(Y)$ 设为在将比特列 Y 按每 n 比特进行分割来表示时 n 比特的数据都返回不是 0 的（非零）元素的数的函数。

[0123] 此外，此时，将 $Branch_n(\theta)$ 为 b+1 那样的映射 θ 定义为最优扩散变换。

[0124] (2-2. 对差分攻击的抵抗性评价指标）

[0125] 在应用 Feistel 结构的共用密钥密码处理中，由密码分析引起的密钥的泄漏成为问题。作为密码分析或者攻击方法的代表方法，已知有差分分析（也称为差分解读法或者差分攻击）、线性分析（也称为线性解读法或者线性攻击），其中，上述差分分析通过多次分

析具有某个差分（ΔX）的输入数据（明文）及其输出数据（密文）来分析各循环函数中的应用密钥，上述线性分析根据明文与对应的密文进行分析。

[0126] 作为实现对差分攻击的抵抗性的指标，能够应用包含在表现差分的连接关系的差分路径中的差分有效 S 盒的最小数。

[0127] 差分路径是对除了加密函数中的密钥数据以外的所有数据部分指定特定的差分值而得到的。差分值并不是自由决定的，而是变换处理前后的差分值互相关联。在线性变换处理的前后，一对一地决定输入差分与输出差分之间的关系。在非线性变换的前后，不是一对一地决定输入差分与输出差分之间的关系，而是导入概率的概念。设为能够事先计算对于某个输入差分和输出差分的概率。将对于所有输出的概率全部相加为 1。

[0128] 在具有 SP 型 F 函数的 Feistel 结构中，非线性变换仅为由 S 盒进行处理的部分。因而，在这种情况下，具有 0 以外的概率的差分路径是从对明文（输入）的差分值开始直到密文（输出）的差分值为止的差分数据的集合，在所有的 S 盒前后提供的差分值具有 0 以外的概率。设为将具有 0 以外的概率的某个差分路径的输入到 S 盒的差分值不是 0 的 S 盒称为差分有效 S 盒。已知将具有 0 以外的概率的所有差分路径的有效 S 盒数之中最小的数称为最小差分有效 S 盒数，该数值作为对差分攻击的安全性指标。此外，所有差分值为 0 那样的差分路径概率为 1，作为攻击没有意义，因此以后不予考虑。

[0129] 在本发明的一个实施例中，具有通过保证该最小差分有效 S 盒数较大来提高对差分攻击的安全性的结构。

[0130] (2-3. 对线性攻击的抵抗性评价指标）

[0131] 并且，作为实现对线性攻击的抵抗性的指标，能够应用包含在表现线性掩模的连接关系的线性路径（多被称为线性近似，但是为了与差分对应，在此使用称为“路径”的词语）中的线性有效 S 盒的最小数。

[0132] 线性路径是对除了加密函数中的密钥数据以外的所有数据部分指定特定的线性掩模值而得到的。线性掩模值并不是自由决定的，而是变换处理前后的线性值互相关联。在线性变换处理的前后，一对一地决定输入线性掩模值与输出线性掩模值之间的关系。在非线性变换的前后，不是一对一地决定输入线性掩模值与输出线性掩模值之间的关系，而是导入概率的概念。对于输入线性掩模值，存在能够输出的一个以上的线性掩模值的集合，能够事先计算各线性掩模值被输出的概率。对所有输出的概率全部相加为 1。

[0133] 在具有 SP 型 F 函数的 Feistel 结构中，非线性变换仅为由 S 盒进行处理的部分。因而，在这种情况下，具有 0 以外的概率的线性路径是从对明文（输入）的线性值开始直到密文（输出）的线性值为止的线性掩模值数据的集合，在所有的 S 盒前后提供的线性值是具有 0 以外的概率的线性值。设为将具有 0 以外的概率的某个线性路径的输入到 S 盒的线性值不是 0 的 S 盒称为线性有效 S 盒。将具有 0 以外的概率的所有线性路径的有效 S 盒数之中最小的数称为最小线性有效 S 盒数，已知该数值作为对线性攻击的安全性指标。此外，所有线性掩模值为 0 那样的线性路径概率为 1，作为攻击没有意义，因此以后不予考虑。

[0134] 在本发明的一个实施例中，通过保证该最小线性有效 S 盒数较大来提高对线性攻击的安全性。

[0135] 如之前所说明的那样，在应用了 Feistel 结构的密码处理中，作为提高对上述的差分攻击、线性攻击的抵抗性的结构，提出应用扩散矩阵切换机构 (DSM :Diffusion

Switching Mechanism，下面是DSM）的结构。DSM是在Feistel结构的循环函数（F函数）部的线性变换部中配置两个以上不同的矩阵的结构。通过该DSM能够保证最小线性有效S盒数较大，能够提高对差分攻击、线性攻击的抵抗性。

[0136] 关于该DSM，说明其概要。在Feistel结构中，在应用了扩散矩阵切换机构（DSM）的情况下，在构成Feistel结构的循环函数（F函数）部的线性变换部（P层）中应用的矩阵为多个不同的矩阵。例如，如图1所示的r个循环的Feistel结构的各循环中的应用矩阵不是设定为全部相同的线性变换矩阵，而是按照特定的规则排列至少两种以上的矩阵。

[0137] 例如，图3示出通过两个线性变换矩阵M_0、M_1来实现扩散矩阵切换机构（DSM）的Feistel结构例，图4示出通过三个线性变换矩阵M_0、M_1、M_2来实现扩散矩阵切换机构（DSM）的Feistel结构例。

[0138] 在图3所示的Feistel结构例中，两个线性变换矩阵M_0、M_1由不同的矩阵构成。另外，在图4所示的Feistel结构例中，三个线性变换矩阵M_0、M_1、M_2由不同的矩阵构成。

[0139] 为了实现扩散矩阵切换机构（DSM），所应用的矩阵需要满足规定的条件。该条件之一是与上述分支数（Branch）有关的限制。下面，说明该限制。

[0140] 在Feistel结构中的循环函数部的线性变换所应用的多个不同的矩阵M_0～M_n各自的分支数中，

[0141] 将应用矩阵中的分支数的最小值：B_1^D、

[0142] 与所应用的多个矩阵的关联矩阵对应的分支数的最小值：B_2^D、B_3^D、B_2^L定义为如下。

[0143] [数1]

[0144] $$B_1^D = \min_i(Branch_n(M_i))$$

[0145] $$B_2^D = \min_i(Branch_n([M_i \mid M_{i+2}]))$$

[0146] $$B_3^D = \min_i(Branch_n([M_i \mid M_{i+2} \mid M_{i+4}]))$$

[0147] $$B_2^L = \min_i(Branch_n([{}^tM_i^{-1} \mid {}^tM_{i+2}^{-1}]))$$

[0148] 在上式中，

[0149] M_i表示在Feistel结构中的第i个循环的线性变换处理中应用的线性变换矩阵，

[0150] $[M_i|M_{i+2}|\cdot\cdot]$表示通过$M_i|M_{i+2}|\cdot\cdot$各矩阵关联得到的关联矩阵，

[0151] ${}^tM$表示矩阵M的转置矩阵，M-1表示矩阵M的逆矩阵。

[0152] 在上式中，：B_2^D、B_3^D、B_2^L具体表示将在Feistel结构中的一个数据序列中连续的两个循环或者三个循环的F函数所包含的矩阵关联得到的矩阵的分支数的最小值。

[0153] 可知例如通过设定各矩阵使得上述各分支数满足以下条件、即

[0154] $B_2^D \geqslant 3$、$B_3^D \geqslant 3$、$B_2^L \geqslant 3$

[0155] 在Feistel结构中能够提高对差分攻击、线性攻击的抵抗性。

[0156] 此外，B_1^D、B_2^D、B_3^D、B_2^L中的各上下标具有下面的意思。

[0157] B_n^D的n表示所关联的矩阵数，B_n^D的D表示用于具有对差分攻击（Differential Attack）的抵抗性的条件，B_n^L中的L表示用于具有对线性攻击（Linear Attack）的抵抗性的条件。

[0158] 在本发明中，提出对具有例如三个序列、四个序列等两个以上的任意的数据序

列的 Feistel 结构实现扩散矩阵切换机构 (DSM) 的结构，而不是对具有两个数据序列的 Feistel 结构实现扩散矩阵切换机构 (DSM) 的结构。下面，详细说明该结构。

[0159] 在本发明中要处理的 Feistel 结构在使用 SP 型 F 函数这点上与上述具有两个数据序列的 Feistel 结构相同，但是以将数据序列数的分割数一般化为 d 的扩展 Feistel 结构为对象。其中，d 是 2 以上的整数。

[0160] 如上所述，提出了对于限定为数据序列数＝ 2 的 Feistel 结构的 DSM 的应用结构，但是并不知道对于具有将数据序列数 d 设为 d ≥ 2 的任意数的 d 的扩展 Feistel 结构应用 DSM 来提高抵抗性的方法。本发明实现对具有设为 d ≥ 2 的任意数的数据序列数 d 的扩展 Feistel 结构应用扩散矩阵切换机构 (DSM) 来提高对差分攻击、线性攻击的抵抗性的结构。

[0161] 下面，说明本发明的具体结构以及处理例。

[0162] (4-1. 关于扩展 Feistel 结构)

[0163] 下面，参照图 5 说明扩展 Feistel 结构的定义。在本说明书中将扩展 Feistel 结构定义为如下。

[0164] 1. 具有 d 个 (d 是 2 以上) 数据序列，各数据序列的大小是 mn 比特。

[0165] 2.F 函数的输入输出大小是 mn 比特。

[0166] 3. 具有称为循环的处理单位，在循环内对一个或多个数据序列实施由 F 函数进行的变换处理，在其它的数据序列中对其结果进行异或。其中，设为在一个循环内包含两个以上 F 函数的情况下，在所有的成为 F 函数的输入输出的数据序列中不存在重复的序列。

[0167] 参照图 5 说明由上述定义构建的扩展 Feistel 结构的例子。

[0168] 上述定义 1. 具有 d 个 (d 是 2 以上) 数据序列，各数据序列的大小是 mn 比特。

[0169] 参照图 5 说明该定义。在图 5 中，意味着数据序列 1 ～ d 的各数据序列的输入输出大小是 mn 比特，输入输出的总比特数是 dmn 比特。

[0170] 上述定义 2.F 函数的输入输出大小是 mn 比特。

[0171] 参照图 5 说明该定义。例如从数据序列 2 的上一级的异或 (XOR) 运算部 201 对 F 函数 202 输入作为运算结果的 mn 比特，并且输入循环密钥 K 来执行运算处理。该运算处理是参照图 2 的 (b) 所说明的处理，包括 S 盒中的非线性变换和线性变换部中的应用线性变换矩阵 M_i 的线性变换处理。F 函数 202 的输出是 mn 比特，被输入到数据序列 4 的异或 (XOR) 运算部 203。

[0172] 上述定义 3. 具有称为循环的处理单位，在循环内对一个或多个数据序列实施由 F 函数进行的变换处理，在其它的数据序列中对其结果进行异或。其中，设为在一个循环内包含两个以上的 F 函数的情况下，在所有成为 F 函数的输入输出的数据序列中不存在重复的序列。

[0173] 参照图 5 说明该定义。图 5 示出具有 r 个循环的结构的扩展 Feistel 结构。在各循环中包含一个以上的 F 函数，在其它的数据序列中对其结果进行异或。图 5 所示的循环 n，在一个循环内包含多个 F 函数。是图 5 所示的 F 函数 211 和 F 函数 212。

[0174] 这样，在一个循环中包含多个 F 函数的情况下，各 F 函数的输入输出序列分别是不同的数据序列，设定为重复的数据序列不作为输入输出序列来应用。

[0175] 图 5 所示的 F 函数 211 的输入数据序列是数据序列 1，输出数据序列是数据序列 2，

[0176] F函数212的输入数据序列是数据序列5以上的任一个，输出数据序列是数据序列3，

[0177] 设定为任意的输入输出数据序列都不重复。

[0178] 此外，也如图5所示，在本说明书中，F函数表示为[F]，循环密钥表示为[K]。对这些各标识符F、K设定的上下标具有下面的意思。

[0179] F_i^n、K_i^n的i表示循环，n表示同一循环中的F函数或者循环密钥的识别编号。

[0180] 此外，虽然没有图示，但是在以下的说明中，在各循环的F函数的线性变换部中应用的线性变换矩阵表示为[M]，对M设定的上下标也与上述同样地，

[0181] 设M_i^n的i表示循环，n表示与设定在同一循环中的多个F函数分别对应的线性变换矩阵的识别编号。

[0182] 图6表示满足上述定义的具有7个数据序列(d＝7)的扩展Feistel结构例。此外，在图6中，省略各F函数的输出与各数据序列之间的异或运算(XOR)部的标记，但是是如下的结构：各F函数的输出与各数据序列在各交叉点上利用各自的输入执行异或运算(XOR)，向同一数据序列的下方向输出该异或运算(XOR)结果。在图6所示的例子中，循环i+4、循环i+5、循环i+9、循环i+10是在一个循环中包含两个以上F函数的循环，在这些循环中示出的F函数[F]和循环密钥[K]的右上方显示表示同一循环中的F函数或循环密钥的识别编号的编号。

[0183] 当根据上述定义1～3构建将序列数d设为d＝2的Feistel结构时，成为由两个数据序列构成的Feistel结构、即之前参照图1所说明的Feistel结构。即，成为F函数交替往来于两个数据序列间那样的结线结构，但是在具有三个以上的数据序列的扩展Feistel结构的情况下，由于存在多个被选为F函数的输入和输出的数据序列，因此无法唯一地确定结线结构。也就是说，在扩展Feistel结构中，d越大F函数的设置位置的自由度呈指数函数增大。

[0184] 在本发明中，提出在这种扩展Feistel结构中实现提高对差分攻击、线性攻击的抵抗性的扩散矩阵切换机构(DSM:Diffusion Switching Mechanism)的结构。

[0185] 在将序列数d设为d＝2的Feistel结构中，例如如图3、图4所示，通过将在构成Feistel结构的循环函数(F函数)部的线性变换部(P层)中应用的矩阵设为两个不同的线性变换矩阵M_0、M_1、或者三个不同的线性变换矩阵M_0、M_1、M_2等来实现DSM。其中，为了实现DSM，需要所应用的矩阵满足规定的条件。该条件之一是与上述分支数(Branch)有关的限制。

[0186] 在说明在将数据序列数d设为

[0187] d:d≥2的任意的整数

[0188] 的扩展Feistel结构中实现DSM的结构之前，参照图7说明在下面的说明中使用的扩展Feistel结构的各结构部以及各结构部的输入输出数据的定义。

[0189] 图7是仅提取表示例如构成如图6所示的扩展Feistel结构的一个数据序列的图。如图7所示，可知对某一个数据序列的输入数据与一次以上的F函数的输出进行异或(XOR)而输出。该处理适用于扩展Feistel结构所包含的任意的数据序列。

[0190] 在图7中，表示对一个数据序列[s(i)]通过异或运算(XOR)将多个F函数[$F_{s(i),1}$、$F_{s(i),2}$、…]的输出相加的情形。

[0191] 此外，将扩展 Feistel 结构中具有 d 个的数据序列分别设为 s(i)(1 ≤ i ≤ d)，将对数据序列 s(i) 进行输入的 F 函数从靠近数据序列 s(i) 的输入起依次命名为 $F_{s(i),1}$、$F_{s(i),2}$、…。

[0192] 另外，将数据序列 s(i) 的输入数据设为 $W_{s(i),0}$，

[0193] 将对 F 函数 $F_{s(i),j}$ 的输出进行异或之后的数据设为 $W_{s(i),j}$。

[0194] 另外，将对 F 函数 $F_{s(i),j}$ 的输入数据设为 $X_{s(i),j}$。

[0195] 各 $X_{s(i),j}$ 是属于数据序列 s(i) 以外的其它的序列的数据，在此设为不追究其属于哪个序列。

[0196] 此时，能够认为扩展 Feistel 结构是将这种数据序列 d 个相互连接而构成的结构。

[0197] 在扩展 Feistel 结构中用于实现 DSM 的结构

[0198] 下面，说明在设为 d：d ≥ 2 的任意的整数的扩展 Feistel 结构中用于实现 DSM 的结构。针对

[0199] (4-2) 在扩展 Feistel 结构中用于提高对差分攻击的抵抗性的结构

[0200] (4-3) 在扩展 Feistel 结构中用于提高对线性攻击的抵抗性的结构

[0201] 这些各个结构依次进行说明。

[0202] (4-2. 在扩展 Feistel 结构中用于提高对差分攻击的抵抗性的结构）

[0203] 首先，说明在扩展 Feistel 结构中用于提高对差分攻击的抵抗性的结构。

[0204] 如上所述，差分攻击是通过多次分析具有某个差分（ΔX）的输入数据（明文）及其输出数据（密文）来分析各循环函数中的应用密钥的攻击，作为实现对差分攻击的抵抗性的指标，应用包含在表现差分的连接关系的差分路径中的差分有效 S 盒的最小数。差分路径是除了加密函数中的密钥数据之外的数据部分的差分值。在线性变换处理的前后，一对一地决定输入差分与输出差分之间的关系，在非线性变换处理的前后，不是一对一地决定，而是算出对某个输入差分的输出差分的出现概率。将对于所有输出的概率全部相加为 1。

[0205] 在具有 SP 型 F 函数的 Feistel 结构中，非线性变换仅是 S 盒。在这种情况下，具有 0 以外的概率的差分路径是从对明文（输入）的差分值开始直到密文（输出）的差分值为止的差分数据的集合，在所有的 S 盒前后提供的差分值具有 0 以外的概率。将具有 0 以外的概率的某个差分路径的输入到 S 盒的差分值不是 0 的 S 盒称为差分有效 S 盒。将具有 0 以外的概率的所有差分路径的有效 S 盒数之中最小的数称为最小差分有效 S 盒数，使用该数值作为对差分攻击的安全性指标。

[0206] 使最小差分有效 S 盒数变大来提高对差分攻击的抵抗性。下面说明在将数据序列数 d 设为 d ≥ 2 的任意整数的扩展 Feistel 结构中构建使最小差分有效 S 盒数的数量变大的 DSM 结构的方法。

[0207] 将扩展 Feistel 结构所包含的 F 函数 $[F_{s(i),x}]$ 中使用的线性变换矩阵设为 $[M_{s(i),x}]$。此时，将应用了分支数运算函数：Branch() 的分支数算出式 $B_2^D(s(i))$ 定义为如下。

[0208] $$B_2^D(s(i)) = \min_j(Branch_n([M_{s(i),j} \mid M_{s(i),j+1}]))$$

[0209] 上式是求出在对构成扩展 Feistel 结构的任意的数据序列 s(i) 进行输入的两个相邻的 F 函数 $[F_{s(i),j}、F_{s(i),j+1}]$ 中使用的两个线性变换矩阵 $[M_{s(i),j}、M_{s(i),j+1}]$ 的关联矩阵

$[M_{s(i),j}|M_{s(i),j+1}]$ 中的分支数的最小值的式子。

[0210] 在构成扩展Feistel结构的任意的数据序列s(i)中，将与从上一级输入到数据序列s(i)的F函数的个数相当的[j]设为任意的j，考虑数据序列s(i)上的数据$[W_{s(i),j}]$。

[0211] 针对夹着对数据序列s(i)进行输入的两个F函数$[F_{s(i),j+1}]$、$[F_{s(i),j+2}]$的对数据序列s(i)的输入部的数据序列s(i)上的输入输出数据$[W_{s(i),j}]$和$[W_{s(i),j+2}]$，考虑

[0212] $W_{s(i),j}=0$、

[0213] $W_{s(i),j+2}=0$的情况。

[0214] 此时，

[0215] 在向对数据序列s(i)进行输入的F函数中相邻的F函数$[F_{s(i),j+1}]$和$[F_{s(i),j+2}]$输入的各输入差分值$[\Delta X_{s(i),j+1}]$和$[\Delta X_{s(i),j+2}]$之间，

[0216] $$hw_n(\Delta X_{s(i),j+1})+hw_n(\Delta X_{s(i),j+2})\geq B_2^D(s(i))$$

[0217] 的关系式成立。

[0218] 此外，在上式中，hw是汉明重量，上式的左边表示F函数的输入差分数据中的非零的要素数、即有效S盒数之和。保证该数为较大的值是能够期望提高对差分攻击的抵抗性的条件。因而，如果其以外的条件相同，则得出优选为选择构成扩展Feistel结构的各F函数内的矩阵使得$B_2^D(s(i))$尽可能变大。

[0219] 在目前为止的扩展Feistel型密码中一般为在所有F函数内的线性变换部中利用一个线性变换矩阵的结构。

[0220] 然而，当对数据序列s(i)进行输入的两个相邻的F函数$[F_{s(i),j}$、$F_{s(i),j+1}]$中使用的两个线性变换矩阵$[M_{s(i),j}]$和$[M_{s(i),j+1}]$是相同的矩阵时，导致应用了上述分支数运算函数:Branch()的分支数的算出式、即

[0221] $B_2^D(s(i))$

[0222] 一定是最低的值、即2。因此，无法期望得到抵抗性提高的效果。

[0223] 另外，即使在使用不同的矩阵的情况下，当随意选择两个矩阵时，也存在$B_2^D(s(i))$为2的情况。

[0224] 将由上述分支数算出式定义的$B_2^D(s(i))$设为更大的分支数能够保证局部的最小差分有效S盒数较大，从而提高对差分攻击的抵抗性。因而，例如通过选择矩阵使得$B_2^D(s(i))$为3以上，能够提高对差分攻击的抵抗性。

[0225] 对扩展Feistel结构的所有数据序列计算$B_2^D(s(i))$，将它们之中最小值的$B_2^D(s(i))$设为B_2^D。下面说明选择F函数中的矩阵使得该B_2^D为3以上的方法。

[0226] (4-2-1.使最小分支数B_2^D的值为3以上的F函数中的矩阵选择结构)

[0227] 首先，下面说明只要存在最少两种矩阵就能够实现使扩展Feistel结构的所有数据序列的最小分支数$[B_2^D(s(i))]$中最小的分支数$[B_2^D]$为3以上的情形。

[0228] 首先，准备两个不同的矩阵$[A_0]$和$[A_1]$的关联矩阵$[A_0|A_1]$的分支数为3以上、即满足

[0229] $Branch_n([A_0|A_1])\geq 3$

[0230] 的两个不同的矩阵$[A_0]$和$[A_1]$。

[0231] 接着，将对扩展Feistel结构的数据序列s(i)进行输入的多个F函数的线性变换

部的线性变换矩阵设定为如下。

[0232] 设定在最初的 F 函数 $F_{s(i),1}$ 的线性变换部中的线性变换矩阵为 A_0、

[0233] 设定在第二个 F 函数 $F_{s(i),2}$ 的线性变换部中的线性变换矩阵为 A_1、

[0234] 设定在第三个 F 函数 $F_{s(i),3}$ 的线性变换部中的线性变换矩阵为 A_0、

[0235] ：

[0236] 如上那样，对向数据序列 s(i) 进行输入的多个 F 函数从上开始依次交替地配置两个不同的矩阵 $[A_0]$ 和 $[A_1]$。

[0237] 在这样设定线性变换矩阵的情况下，求出对任意的数据序列 s(i) 进行输入的两个相邻的 F 函数 $[F_{s(i),j}、F_{s(i),j+1}]$ 中使用的两个线性变换矩阵 $[M_{s(i),j}、M_{s(i),j+1}]$ 的关联矩阵 $[M_{s(i),j}|M_{s(i),j+1}]$ 中的分支数的最小值的上式是

[0238] $$B_2^D(s(i)) = \min_j(Branch_n([M_{s(i),j} \mid M_{s(i),j+1}])) \geq 3$$ 。

[0239] 即，保证最小分支数为 3 以上。

[0240] 当然，即使轮换矩阵 $[A_0]$ 和 $[A_1]$，效果也相同。另外，如果对扩展 Feistel 结构的所有数据序列 s(i) 同样地设定矩阵，则仅使用两个矩阵就能够使 B_2^D 的值为 3 以上。

[0241] 这样，准备满足 $Branch_n([A_0|A_1]) \geq 3$ 的两个不同的矩阵 $[A_0]$ 和 $[A_1]$，通过设定为在对扩展 Feistel 结构的各数据序列 s(i) 进行输入的 F 函数中交替地配置这些各个矩阵，能够使最小分支数 B_2^D 的值为 3 以上，从而实现利用扩散矩阵切换机构 (DSM) 提高对差分攻击的抵抗性。

[0242] 上述的说明是应用两个不同的矩阵 $[A_0]$ 和 $[A_1]$ 的例子。

[0243] 接着，下面说明将不同的矩阵一般化为 2 以上的任意数 [k] 的例子。

[0244] 将在扩展 Feistel 结构所包含的 F 函数 $[F_{s(i),j}]$ 中使用的线性变换矩阵设为 $[M_{s(i),j}]$。此时，将应用了分支数运算函数 :Branch() 的分支数的算出式 $B_2^D(s(i))$ 定义为如下。

[0245] $$B_k^D(s(i)) = \min_j(Branch_n([M_{s(i),j} \mid M_{s(i),j+1} \mid M_{s(i),j+2} \mid \cdots \mid M_{s(i),j+k-1}]))$$

[0246] 上式是求出在对构成扩展 Feistel 结构的任意数据序列 s(i) 进行输入的 k 个相邻的 F 函数 $[F_{s(i),j}、F_{s(i),j+1}、\cdots、F_{s(i),j+k-1}]$ 中使用的 k 个线性变换矩阵 $[M_{s(i),j}、M_{s(i),j+1}、\cdots、M_{s(i),j+k-1}]$ 的关联矩阵 $[M_{s(i),j}|M_{s(i),j+1}|\cdots|M_{s(i),j+k-1}]$ 中的分支数的最小值的式子。

[0247] 在构成扩展 Feistel 结构的任意数据序列 s(i) 中，将与从上一级输入到数据序列 s(i) 的 F 函数的个数相当的 [j] 设为任意的 j，考虑数据序列 s(i) 上的数据 $[W_{s(i),j}]$。

[0248] 对夹着对数据序列 s(i) 进行输入的 k 个 F 函数 $[F_{s(i),j+1}]\cdots[F_{s(i),j+k}]$ 的对数据序列 s(i) 的输入部的数据序列 s(i) 上的输入输出数据 $[W_{s(i),j}]$ 和 $[W_{s(i),j+k}]$，考虑

[0249] $W_{s(i),j} = 0$、

[0250] $W_{s(i),j+k} = 0$ 的情况。

[0251] 此时，

[0252] 在向对数据序列 s(i) 进行输入的 F 函数中相邻的 k 个 F 函数 $[F_{s(i),j+1}]\cdots[F_{s(i),j+k}]$ 输入的各输入差分值 $[\Delta X_{s(i),j+1}]\cdots[\Delta X_{s(i),j+k}]$ 之间，得到

[0253] $$\sum_{l=j+1}^{j+k} hw_n(\Delta X_{s(i),l}) \geq B_k^D(s(i))$$

[0254] 的关系式。

[0255] 此外，在上式中，hw 是汉明重量，上式的左边表示 F 函数的输入差分数据中的非零要素数、即有效 S 盒数之和。保证该数为较大的值是能够期望提高对差分攻击的抵抗性的条件。因而，如果其以外的条件相同，则得出优选为选择构成扩展 Feistel 结构的各 F 函数内的矩阵使得 $B_k^D(s(i))$ 尽可能大。

[0256] 然而，即使在向数据序列 s(i) 进行输入的 k 个相邻的 F 函数 $[F_{s(i),j}]\cdots[F_{s(i),j+k-1}]$ 中使用的 k 个线性变换矩阵 $[M_{s(i),j}]\cdots[M_{s(i),j+k-1}]$ 中存在一个相同的矩阵，也会导致应用了上述分支数运算函数 :Branch() 的分支数的算出式、即

[0257] $B_k^D(s(i))$

[0258] 一定是最低的值、即 2。因此，无法期望得到抵抗性提高的效果。

[0259] 另外，即使在 k 个线性变换矩阵 $[M_{s(i),j}]\cdots[M_{s(i),j+k-1}]$ 中使用不同的矩阵的情况下，当随意选择矩阵时，也存在 $B_k^D(s(i))$ 为 2 的情况。

[0260] 将由上述分支数算出式定义的 $B_k^D(s(i))$ 设为更大的分支数能够保证局部的最小线性有效 S 盒数变大，从而提高对差分攻击的抵抗性。因而，例如通过选择矩阵使得 $B_k^D(s(i))$ 为 3 以上，能够提高对差分攻击的抵抗性。

[0261] 对扩展 Feistel 结构的所有数据序列计算 $B_k^D(s(i))$，将它们之中最小值的 $B_k^D(s(i))$ 设为 B_k^D。下面说明选择 F 函数中的矩阵使得该 B_k^D 为 3 以上的方法。

[0262] (4-2-2. 使最小分支数 B_k^D 的值为 3 以上的 F 函数中的矩阵选择结构)

[0263] 下面说明只要存在至少 k 种矩阵就能够实现使扩展 Feistel 结构的所有数据序列的最小分支数 $[B_k^D(s(i))]$ 中最小的分支数 $[B_k^D]$ 为 3 以上的情形。

[0264] 首先，准备 k 个不同的矩阵 $[A_0]$、$[A_1]$、$[A_2]$、…$[A_{k-1}]$ 的关联矩阵 $[A_0|A_1|\cdots|A_{k-1}]$ 的分支数为 3 以上、即满足

[0265] $Branch_n([A_0|A_1|\cdots|A_{k-1}]) \geq 3$

[0266] 的 k 个不同的矩阵 $[A_0]$、$[A_1]$、$[A_2]$、…$[A_{k-1}]$。

[0267] 接着，将对扩展 Feistel 结构的数据序列 s(i) 进行输入的多个 F 函数的线性变换部的线性变换矩阵设定为如下。

[0268] 设定在最初的 F 函数 $F_{s(i),1}$ 的线性变换部中的线性变换矩阵为 A_0、

[0269] 设定在第二个 F 函数 $F_{s(i),2}$ 的线性变换部中的线性变换矩阵为 A_1、

[0270] 设定在第三个 F 函数 $F_{s(i),3}$ 的线性变换部中的线性变换矩阵为 A_2、

[0271] :

[0272] 设定在第 k 个 F 函数 $F_{s(i),k}$ 的线性变换部中的线性变换矩阵为 A_{k-1}、

[0273] 设定在第 k+1 个 F 函数 $F_{s(i),k+1}$ 的线性变换部中的线性变换矩阵为 A_0、

[0274] 设定在第 k+2 个 F 函数 $F_{s(i),k+2}$ 的线性变换部中的线性变换矩阵为 A_1、

[0275] :

[0276] 如上那样，对向数据序列 s(i) 进行输入的多个 F 函数从上开始依次重复配置 k 个不同的矩阵 $[A_0]$、$[A_1]$、$[A_2]$、…$[A_{k-1}]$。

[0277] 在这样设定线性变换矩阵 $[A_0]$、$[A_1]$、$[A_2]$、…$[A_{k-1}]$ 的情况下，求出对任意数据序列 s(i) 进行输入的 k 个相邻的 F 函数 $[F_{s(i),j}、F_{s(i),j+1}\cdots F_{s(i),j+k-1}]$ 中使用的 k 个线性变换矩阵 $[M_{s(i),j}、M_{s(i),j+1}\cdots M_{s(i),j+k-1}]$ 的关联矩阵 $[M_{s(i),j}|M_{s(i),j+1}|\cdots M_{s(i),j+k-1}]$ 中的分支数的最

小值的式子是

[0278] [数 7]

[0279]

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

。

[0280] 即，保证最小分支数为 3 以上。

[0281] 当然，即使轮换矩阵 $[A_0]$、$[A_1]$、$[A_2]$、…$[A_{k-1}]$，效果也相同。另外，如果对扩展 Feistel 结构的所有数据序列 s(i) 同样地设定矩阵，则仅使用 k 个矩阵就能够使 B_k^D 的值为 3 以上。

[0282] 这样，准备满足

[0283] $Branch_n([A_0|A_1|\cdots|A_{k-1}]) \geq 3$

[0284] 的 k 个不同的矩阵 $[A_0]$、$[A_1]$、$[A_2]$、…$[A_{k-1}]$，通过设定为在对扩展 Feistel 结构的各数据序列 s(i) 进行输入的 F 函数中依次反复配置这些各矩阵，能够使最小分支数 B_k^D 的值为 3 以上，从而实现利用扩散矩阵切换机构 (DSM) 提高对差分攻击的抵抗性。

[0285] 此外，关于 k 的值的选择，只要 k 至少为 2 以上就能够期望得到上述效果。k 越大，被保证的范围越大，因此能够进一步期望抵抗性的提高。但是，另一方面，由于所需的矩阵种类的最小数变大，因此有可能不适于有效安装。因此，k 的值应该是在设计阶段根据状况而选择的值。

[0286] (4-3. 在扩展 Feistel 结构中用于提高对线性攻击的抵抗性的结构）

[0287] 接着，说明在扩展 Feistel 结构中提高对线性攻击的抵抗性的结构。

[0288] 首先，如所说明的那样，作为实现对线性攻击的抵抗性的指标，能够应用表现线性掩模的连接关系的线性路径（多被称为线性近似，但是为了与差分对应，在此使用称为“路径”的词语）所包含的线性有效 S 盒的最小数。线性路径是对除了加密函数中的密钥数据以外的所有数据部分指定特定的线性掩模值而得到的。在线性变换处理的前后，一对一地决定输入线性掩模值与输出线性掩模值之间的关系，在非线性变换处理的前后，不是一对一地决定，而是算出对某输入线性掩模的输出线性掩模的出现概率。对所有输出的概率全部相加为 1。

[0289] 在具有 SP 型 F 函数的 Feistel 结构中，非线性变换仅为由 S 盒进行处理的部分。因而，在这种情况下，具有 0 以外的概率的线性路径是从对明文（输入）的线性值开始直到密文（输出）的线性值为止的线性掩模值数据的集合，在所有 S 盒前后提供的线性值具有 0 以外的概率。将具有 0 以外的概率的某线性路径的输入到 S 盒的线性值不是 0 的 S 盒称为线性有效 S 盒。将具有 0 以外的概率的所有线性路径的有效 S 盒数之中最小的数称为最小线性有效 S 盒数，使用该数值作为对线性攻击的安全性指标。

[0290] 使最小线性有效 S 盒数变大来提高对线性攻击的抵抗性。下面说明在将数据序列数 d 设为 $d \geq 2$ 的任意整数的扩展 Feistel 结构中构建使最小线性有效 S 盒数的数量变大的 DSM 结构的方法。

[0291] 将在扩展 Feistel 结构所包含的 F 函数 $[F_{s(i),x}]$ 中使用的线性变换矩阵设为 $[M_{s(i),x}]$。此时，将应用了分支数运算函数 :Branch() 的分支数的算出式 $B_2^L(s(i))$ 定义为如下。

[0292] $$B_2^{I'}(s(i)) = \min_j(Branch_n([{}^tM^{-1}_{s(i),j} | {}^tM^{-1}_{s(i),j+1}]))$$

[0293] 上式是求出在对构成扩展 Feistel 结构的任意数据序列 s(i) 进行输入的两个相邻的 F 函数 $[F_{s(i),j}、F_{s(i),j+1}]$ 中使用的两个线性变换矩阵 $[M_{s(i),j}]$、$[M_{s(i),j+1}]$ 各自的逆矩阵的转置矩阵 $[{}^tM^{-1}{}_{s(i),j}]$、$[{}^tM^{-1}{}_{s(i),j+1}]$ 的关联矩阵 $[{}^tM^{-1}{}_{s(i),j} | {}^tM^{-1}{}_{s(i),j+1}]$ 中的分支数的最小值的式子。

[0294] 在构成扩展Feistel结构的任意数据序列s(i)中，将与从上一级对数据序列s(i)进行输入的F函数的个数相当的[j]设为任意的j，对于某j，

[0295] 对第 j 个 F 函数的输入：$X_{s(i),j}$、

[0296] 第 j 个 F 函数的输出与数据序列 s(i) 上的数据之间的异或 (XOR) 结果：$W_{s(i),j}$、

[0297] 对第 j+1 个 F 函数的输入：$X_{s(i),j+1}$，

[0298] 当将这些各数据的线性掩模分别设为

[0299] $\Gamma X_{s(i),j}$、

[0300] $\Gamma W_{s(i),j}$、

[0301] $\Gamma X_{s(i),j+1}$

[0302] 时，如果它们之中任一个都不为 0，则满足下式。

[0303] 即，

[0304] $$hw_n(\Gamma X_{s(i),j}) + hw(\Gamma W_{s(i),j}) + hw(\Gamma X_{s(i),j+1}) \geq B_2^{I'}(s(i))$$

[0305] 满足上式。意味着上式左边的值越大，局部的线性有效 S 盒数越大。因而，可以说优选为选择矩阵以使 $B_2^L(s(i))$ 变大。

[0306] 然而，当在对数据序列 s(i) 进行输入的两个相邻的 F 函数 $[F_{s(i),j}、F_{s(i),j+1}]$ 中使用的两个线性变换矩阵 $[M_{s(i),j}]$、$[M_{s(i),j+1}]$ 是相同的矩阵时，上述的分支数算出式、即

[0307] $B_2^L(s(i))$

[0308] 一定是最低的值、即 2。因此无法期望得到抵抗性提高的效果。将 $B_2^L(s(i))$ 设为更大的分支数能够保证最小线性有效 S 盒数变大，从而提高对线性攻击的抵抗性。因而，例如通过选择矩阵使得 $B_2^L(s(i))$ 为 3 以上，能够提高对线性攻击的抵抗性。

[0309] 对扩展 Feistel 结构的所有数据序列计算 $B_2^L(s(i))$，将它们之中最小值的 $B_2^L(s(i))$ 设为 B_2^L。下面说明选择 F 函数中的矩阵使得该 B_2^L 为 3 以上的方法。

[0310] (4-3-1. 使最小分支数 B_2^L 的值为 3 以上的 F 函数中的矩阵选择结构)

[0311] 下面说明只要存在至少两种矩阵就能够实现使扩展 Feistel 结构的所有数据序列的最小分支数 $[B_2^L(s(i))]$ 中最小的分支数 $[B_2^L]$ 为 3 以上的情形。

[0312] 首先，准备两个不同的矩阵 $[A_0]$ 和 $[A_1]$ 的关联矩阵 $[{}^tA_0^{-1} | {}^tA_1^{-1}]$ 的分支数为 3 以上、即满足

[0313] $Branch_n([{}^tA_0^{-1} | {}^tA_1^{-1}]) \geq 3$

[0314] 的两个不同的矩阵 $[A_0]$ 和 $[A_1]$。

[0315] 接着，将对扩展 Feistel 结构的数据序列 s(i) 进行输入的多个 F 函数的线性变换部的线性变换矩阵设定为如下。

[0316] 设定在最初的 F 函数 $F_{s(i),1}$ 的线性变换部中的线性变换矩阵为 A_0、

[0317] 设定在第二个 F 函数 $F_{s(i),2}$ 的线性变换部中的线性变换矩阵为 A_1、

[0318] 设定在第三个 F 函数 $F_{s(i),3}$ 的线性变换部中的线性变换矩阵为 A_0、

[0319] ：

[0320] 如上那样，对向数据序列 s(i) 进行输入的多个 F 函数从上开始依次交替地配置两个不同的矩阵 $[A_0]$ 和 $[A_1]$。

[0321] 在这样设定线性变换矩阵的情况下，求出在对任意数据序列 s(i) 进行输入的两个相邻的 F 函数 $[F_{s(i),j}、F_{s(i),j+1}]$ 中使用的两个线性变换矩阵 $[M_{s(i),j}]$、$[M_{s(i),j+1}]$ 各自的逆矩阵的转置矩阵 $[{}^tM^{-1}{}_{s(i),j}]$、$[{}^tM^{-1}{}_{s(i),j+1}]$ 的关联矩阵 $[{}^tM^{-1}{}_{s(i),j}|{}^tM^{-1}{}_{s(i),j+1}]$ 中的分支数的最小值的上式成为

[0322] $$B_2^L(s(i)) = \min_j(Branch_n([{}^tM^{-1}_{s(i),j}|{}^tM^{-1}_{s(i),j+1}])) \geq 3$$ 。

[0323] 即，保证最小分支数为 3 以上。

[0324] 当然，即使轮换矩阵 $[A_0]$ 和 $[A_1]$，效果也相同。另外，如果对扩展 Feistel 结构的所有数据序列 s(i) 同样地设定矩阵，则仅使用两个矩阵就能够使 $B_2{}^L$ 的值为 3 以上。

[0325] 这样，准备满足 $Branch_n([{}^tA_0{}^{-1}|{}^tA_1{}^{-1}]) \geq 3$ 的两个不同的矩阵 $[A_0]$ 和 $[A_1]$，通过设定为在对扩展 Feistel 结构的各数据序列 s(i) 进行输入的 F 函数中交替地配置这些各矩阵，能够使最小分支数 $B_2{}^L$ 的值为 3 以上，从而实现利用扩散矩阵切换机构 (DSM) 提高对线性攻击的抵抗性。

[0326] 如上所述，通过在将数据序列数 d 设为 $d \geq 2$ 的任意整数的扩展 Feistel 结构中应用 DSM 技术，能够提高对差分攻击、线性攻击的抵抗性。下面，说明能够以较高的水平保证对差分攻击、线性攻击的安全性指标的具体的扩展 Feistel 结构。

[0327] 如之前参照图 5、图 6 所说明的那样，将数据序列数 d 设为 $d \geq 2$ 的任意整数的扩展 Feistel 结构是能够进行从其它各种数据序列对一个数据序列的输入、并且能够在一个循环中并行地执行多个 F 函数等的各种结构。下面，将扩展 Feistel 结构大致分类为两个类型（类型 1、类型 2），按每各个类型说明能够以较高的水平保证对差分攻击、线性攻击的安全性指标的具体的扩展 Feistel 结构。

[0328] (5-1. 对于扩展 Feistel 结构的类型 1 的 DSM 的应用）

[0329] 首先，参照图 8 说明对于扩展 Feistel 结构的类型 1 的 DSM 的应用。

[0330] 设扩展 Feistel 结构的类型 1 具有以下参数。

[0331] 参数

[0332] (a) 数据分割数 :d(d 为 3 以上）

[0333] (b) 输入输出数据长度 :dmn 比特

[0334] (c) 分割数据长度 :mn 比特

[0335] (d) 每一个循环的 F 函数的数量 :1

[0336] 如图 8 所示，在各循环内，对图 8 所示的左端的数据序列上的 mn 比特数据应用 F 函数，将 F 函数的处理结果输出到紧邻的数据序列并进行异或。此外，在图 8 中省略异或的运算标记。

[0337] 如图 8 所示，采用如下结构 :在各循环中对 F 函数进行数据输入的左端的数据序列

在下一个循环中移动到右端，其以外的数据序列逐一向左移动。

[0338] 说明这样在各循环的每一个循环中执行一个 F 函数的扩展 Feistel 结构中应用 DSM 来提高对差分攻击和线性攻击的抵抗性的结构。

[0339] 在之前所说明的 (4-2. 在扩展 Feistel 结构中用于提高对差分攻击的抵抗性的结构）中，说明了以下情形 :对扩展 Feistel 结构的所有数据序列计算 $B_2^D(s(i))$，将它们之中最小值的 $B_2^D(s(i))$ 设为 B_2^D，选择 F 函数中的矩阵使得该 B_2^D 为 3 以上，由此提高对差分攻击的抵抗性。

[0340] 并且，在之前所说明的 (4-3. 在扩展 Feistel 结构中用于提高对线性攻击的抵抗性的结构）中，说明了以下情形 :对扩展 Feistel 结构的所有数据序列计算 $B_2^L(s(i))$，将它们之中最小值的 $B_2^L(s(i))$ 设为 B_2^L，选择 F 函数中的矩阵使得该 B_2^L 为 3 以上，由此提高对线性攻击的抵抗性。

[0341] 除了该 B_2^D 和 B_2^L，还将 B_1^D 设为包含在如图 8 所示的类型 1 的扩展 Feistel 结构中的 F 函数中的线性变换矩阵的分支数中的最小的分支数。

[0342] 此时，当将包含在如图 8 所示的类型 1 的扩展 Feistel 结构中的连续 p 个循环中的差分有效 S 盒数记载为 ActD(p)、将线性有效 S 盒数记载为 ActL(p) 时，存在下面的关系式。

[0343] $ActD(3d) \geqslant B_1^D + B_2^D$

[0344] $ActL(3d) \geqslant 2B_2^L$

[0345] 在上式中，

[0346] ActD(3d) 表示包含在连续的 3d 个循环中的差分有效 S 盒数，

[0347] ActL(3d) 表示包含在连续的 3d 个循环中的线性有效 S 盒数。

[0348] 稍后记述这些关系式成立的证明。

[0349] 根据该内容，通过利用使 B_1^D、B_2^D、B_2^L 变大那样的矩阵，能够确保有效 S 盒数变大，其结果，能够提高对差分攻击和线性攻击的抵抗性。

[0350] 此外，已知这些 B_1^D、B_2^D、B_2^L 的逻辑上的最大值为 m+1。

[0351] 在上述的式子、即

[0352] $ActD(3d) \geqslant B_1^D + B_2^D$

[0353] $ActL(3d) \geqslant 2B_2^L$

[0354] 这些式子的右边包含之前所说明的最小分支数 B_2^D 或 B_2^L，使这些最小分支数的值变大有助于确保有效 S 盒数变大，对提高对差分攻击和线性攻击的抵抗性是有效的。因而，在如图 8 所示的扩展 Feistel 结构的类型 1 的结构中，之前所说明的使最小分支数 B_2^D 或 B_2^L 为 3 以上的结构是有效的，通过设为该结构能够保证对差分攻击和线性攻击的抵抗性比以往更高。

[0355] (5-2. 对于扩展 Feistel 结构的类型 2 的 DSM 的应用）

[0356] 接着，参照图 9 说明对于扩展 Feistel 结构的类型 2 的 DSM 的应用。

[0357] 设扩展 Feistel 结构的类型 2 具有以下参数。

[0358] 参数

[0359] (a) 数据分割数 :d（其中，d 为 4 以上的偶数）

[0360] (b) 输入输出数据长度 :dmn 比特

[0361] (c) 分割数据长度 :mn 比特

[0362] (d) 每一个循环的 F 函数的数量 :d/2

[0363] 如图 9 所示，在各循环内，对从左端起处于第奇数个的 mn 比特的数据序列应用 F 函数，将 F 函数的处理结果输出到紧邻的数据序列并进行异或。此外，在图 9 中省略异或的运算标记。

[0364] 如图 9 所示，采用如下结构 :在各循环中，对 F 函数进行数据输入的左端的数据序列在下一个循环中移动到右端，其以外的数据序列逐一向左移动。

[0365] 说明这样在各循环的每一个循环中执行 d/2 个 F 函数的扩展 Feistel 结构中应用 DSM 来提高对差分攻击和线性攻击的抵抗性的结构。

[0366] 在之前所说明的 (4-2. 在扩展 Feistel 结构中用于提高对差分攻击的抵抗性的结构) 中，说明了以下情形 :对扩展 Feistel 结构的所有数据序列计算 $B_2^D(s(i))$，将它们之中最小值的 $B_2^D(s(i))$ 设为 B_2^D，选择 F 函数中的矩阵使得该 B_2^D 为 3 以上，由此提高对差分攻击的抵抗性。

[0367] 并且，在之前所说明的 (4-3. 在扩展 Feistel 结构中用于提高对线性攻击的抵抗性的结构) 中，说明了以下情形 :对扩展 Feistel 结构的所有数据序列计算 $B_2^L(s(i))$，将它们之中最小值的 $B_2^L(s(i))$ 设为 B_2^L，选择 F 函数中的矩阵使得该 B_2^L 为 3 以上，由此提高对线性攻击的抵抗性。

[0368] 除了该 B_2^D 和 B_2^L，还将 B_1^D 设为如图 9 所示的类型 2 的扩展 Feistel 结构中包含的 F 函数中的线性变换矩阵的分支数中的最小的分支数。

[0369] 此时，当将包含在如图 9 所示的类型 2 的扩展 Feistel 结构中的连续 p 个循环中的差分有效 S 盒数记载为 ActD(p)、将线性有效 S 盒数记载为 ActL(p) 时，存在下面的关系式。

[0370] $ActD(6) \geq B_1^D+B_2^D$

[0371] $ActL(6) \geq 2B_2^L$

[0372] 在上式中，

[0373] ActD(6) 表示包含在连续的 6 个循环中的差分有效 S 盒数，

[0374] ActL(6) 表示包含在连续的 6 个循环中的线性有效 S 盒数。

[0375] 稍后记述这些关系式成立的证明。

[0376] 根据该内容，通过利用使 B_1^D、B_2^D、B_2^L 变大那样的矩阵，能够确保有效 S 盒数变大，其结果，能够提高对差分攻击和线性攻击的抵抗性。

[0377] 此外，已知这些 B_1^D、B_2^D、B_2^L 的逻辑上的最大值为 m+1。

[0378] 在上述的式子、即

[0379] $ActD(6) \geq B_1^D+B_2^D$

[0380] $ActL(6) \geq 2B_2^L$

[0381] 这些式子的右边包含之前所说明的最小分支数 B_2^D 或 B_2^L，使这些最小分支数的值变大有助于确保有效 S 盒数变大，对提高对差分攻击和线性攻击的抵抗性是有效的。因而，在如图 9 所示的扩展 Feistel 结构的类型 2 的结构中，之前所说明的使最小分支数 B_2^D 或 B_2^L 为 3 以上的结构是有效的，通过设为该结构能够保证对差分攻击和线性攻击的抵抗性比以往更高。

[0382] 接着，说明在上述的

[0383] (5-1. 对于扩展 Feistel 结构的类型 1 的 DSM 的应用)

[0384] (5-2. 对于扩展 Feistel 结构的类型 2 的 DSM 的应用)

[0385] 中所说明的有效 S 盒数与基于 F 函数中的线性变换矩阵的最小分支数之间的关系式的证明。

[0386] (6-1. 扩展 Feistel 结构的类型 1 的有效 S 盒数与基于 F 函数中的线性变换矩阵的最小分支数之间的关系式的证明)

[0387] 首先，说明之前参照图 8 所说明的扩展 Feistel 结构的类型 1 的有效 S 盒数与基于 F 函数中的线性变换矩阵的最小分支数之间的关系式的证明。

[0388] 即，证明将包含在类型 1 的扩展 Feistel 结构中的连续的 p 个循环中的差分有效 S 盒数记载为 ActD(p)、将线性有效 S 盒数记载为 ActL(p) 的情况下的关系式、

[0389] $ActD(3d) \geq B_1^D + B_2^D$

[0390] $ActL(3d) \geq 2B_2^L$

[0391] 该关系式成立。

[0392] 能够如图 10 那样以其它的形式表示之前参照图 8 所说明的扩展 Feistel 结构的类型 1 的结构。在图 8 中在每个循环中轮换表示各数据序列的排列使得对 F 函数进行输入的数据序列位于左端，但是图 10 不进行数据序列在每个循环中的轮换，而以一条直线表示。在图 10 中示出循环 1 ～ 6d。将 d 个的循环 (循环 1 ～ d、d+1 ～ 2d、…、5d+1 ～ 6d) 排列在一条横线上来表示，但是它们并不是被并行地执行，而是依次执行各循环、例如循环 1 ～ d。

[0393] 另外，图中省略了在 F 函数的输出与各数据序列的交点的异或 (XOR) 运算标记，但是在 F 函数的输出与各数据序列的交点上执行异或 (XOR) 运算，其结果成为下一个循环的 F 函数的输入。

[0394] 证明在该扩展 Feistel 结构的类型 1 的结构中之前在 (5-1. 对于扩展 Feistel 结构的类型 1 的 DSM 的应用) 中所说明的关系式、

[0395] $ActD(3d) \geq B_1^D + B_2^D$

[0396] $ActL(3d) \geq 2B_2^L$

[0397] 成立。

[0398] 在上式中，

[0399] ActD(3d)、ActL(3d) 意味着包含在图 8 或图 10 所示的类型 1 的扩展 Feistel 结构中的连续的 3d 个循环中的差分有效 S 盒数和线性有效 S 盒数。

[0400] B_1^D 是包含在类型 1 的扩展 Feistel 结构中的 F 函数中的线性变换矩阵的分支数中的最小的分支数，

[0401] B_2^D、B_2^L 是在之前在 (4-2)、(4-3) 中所说明的对扩展 Feistel 结构中包含的一个数据序列进行输入的连续的 F 函数中的线性变换矩阵的关联矩阵的最小分支数、以及逆矩阵的转置矩阵的关联矩阵的最小分支数。

[0402] 将 B_1^D、B_2^D、B_2^L 定义为如下。

[0403] $$B_1^D = \min_i (Branch_n(M_i))$$

[0404] $$B_2^D = \min_i(Branch_n([M_i \mid M_{i+d}]))$$

[0405] $$B_2^L = \min_i(Branch_n([{}^tM_i^{-1} \mid {}^tM_{i+d}^{-1}]))$$

[0406] 此外，在上述定义中，

[0407] $B_1^D \geq B_2^D$

[0408] 的关系成立。

[0409] 另外，设为用 D_k 表示包含在图 8 或图 10 所示的类型 1 的扩展 Feistel 结构中的第 k 个 F 函数中的差分有效 S 盒数，用 L_k 表示线性有效 S 盒数。

[0410] （证明 1. $ActD(3d) \geq B_1^D+B_2^D$ 的证明）

[0411] 首先证明 $ActD(3d) \geq B_1^D+B_2^D$。

[0412] 即，证明包含在图 8、图 10 所示的类型 1 的扩展 Feistel 结构中连续的 3d 个循环中的差分有效 S 盒的个数为 $B_1^D+B_2^D$ 以上。

[0413] 考察在类型 1 的扩展 Feistel 结构中提供输入不是零的差分（ΔX）的情况。在这种情况下，类型 1 的扩展 Feistel 结构具有以下四个性质。

[0414] （性质 1）在连续的 d 个循环中至少一个循环中存在不是 0 的差分有效 S 盒

[0415] （性质 2）如果 $D_k = 0$，则 $D_{k-d+1} = D_{k+1}$

[0416] （性质 3）如果 $D_k \neq 0$，则 $D_{k-d+1}+D_k+D_{k+1} \geq B_1^D$

[0417] （性质 4）如果 $D_k+D_{k+d} \neq 0$，则 $D_{k-d+1}+D_k+D_{k+d}+D_{k+d+1} \geq B_2^D$

[0418] 利用以上四个性质，进行

[0419] $ActD(3d) \geq B_1^D+B_2^D$

[0420] 的证明、即证明“包含在连续的 3d 个循环中的差分有效 S 盒的个数为 $B_1^D+B_2^D$ 以上”。

[0421] 考虑作为对象的循环为从第 i+1 个到第 i+3d 个的循环。

[0422] 情况 1：假设在从第 i+d+2 个循环到第 i+2d-1 个循环中存在不是 0 的有效 S 盒的情况。

[0423] 当将存在不是 0 的有效 S 盒的循环设为 k 时，表示为 $D_k \neq 0$。

[0424] 情况 1-1：除了情况 1，在 $D_{k+d-1} \neq 0$ 的情况下，

[0425] 根据性质 3，$D_k+D_{k+1}+D_{k-d+1} \geq B_1^D$

[0426] 根据性质 4，$D_{k+d-1}+D_{k-2d}+D_{k-1}+D_{k+d} \geq B_2^D$，

[0427] 因此得出

[0428] [数 12]

[0429] $$\sum_{j=i+1}^{i+3d} D_j \geq B_1^D + B_2^D$$ 。

[0430] 情况 1-2：除了情况 1，在 $D_{k+1} \neq 0$ 的情况下，

[0431] 根据性质 3，$D_{k+1}+D_{k+2}+D_{k-d+2} \geq B_1^D$

[0432] 根据性质 4，$D_k+D_{k-d+1}+D_{k+d}+D_{k+d+1} \geq B_2^D$，

[0433] 因此得出

[0434] [数 13]

[0435] $$\sum_{j=i+1}^{i+3d} D_j \geq B_1^D + B_2^D$$ 。

[0436] 情况 1-3 :除了情况 1,在 $D_{k+d-1} = 0$ 并且 $D_{k+1} = 0$ 的情况下,

[0437] 根据性质 2,$D_k = D_{k+d} \neq 0$

[0438] 根据性质 3,$D_k+D_{k+1}+D_{k-d+1} \geq B_1^D$

[0439] 根据性质 3,$D_{k+d}+D_{k+d+1}+D_{k+1} \geq B_2^D$

[0440] $D_{k+1} = 0$,因此得出

[0441] $$\sum_{j=i+1}^{i+3d} D_j \geq 2B_1^D$$ 。

[0442] 情况 2 :假设在从第 i+d+2 个循环到第 i+2d-1 个循环中不存在不是 0 的有效 S 盒的情况。

[0443] 根据性质 1,$D_{i+d+1} \neq 0$、或者 $D_{i+2d} \neq 0$。

[0444] 情况 2-1 :在 $D_{i+d+1} \neq 0$ 而 $D_{i+2d} = 0$ 的情况下,

[0445] 根据性质 2,$D_{i+d+1} = D_{i+2d+1} \neq 0$

[0446] 根据性质 3,$D_{i+d+1}+D_{i+d+2}+D_{i+2} \geq B_1^D$

[0447] 根据性质 3,$D_{i+2d+1}+D_{i+2d+2}+D_{i+d+2} \geq B_1^D$

[0448] $D_{i+d+2} = 0$,因此得出

[0449] $$\sum_{j=i+1}^{i+3d} D_j \geq 2B_1^D$$ 。

[0450] 情况 2-2 :在 $D_{i+d+1} = 0$ 而 $D_{i+2d} \neq 0$ 的情况下,

[0451] 根据性质 2,$D_{i+2d} = D_{i+d} \neq 0$

[0452] 根据性质 3,$D_{i+d}+D_{i+d+1}+D_{i+1} \geq B_1^D$

[0453] 根据性质 3,$D_{i+2d}+D_{i+2d+1}+D_{i+d+1} \geq B_1^D$

[0454] $D_{i+d+1} = 0$,因此得出

[0455] $$\sum_{j=i+1}^{i+3d} D_j \geq 2B_1^D$$ 。

[0456] 情况 2-3 :在 $D_{i+d+1} \neq 0$ 并且 $D_{i+2d} \neq 0$ 的情况下,

[0457] 根据性质 3,$D_{i+d+1}+D_{i+d+2}+D_{i+2} \geq B_1^D$

[0458] 根据性质 4,$D_{i+2d}+D_{i+2d+1}+D_{i+d}+D_{i+1} \geq B_2^D$,因此得出

[0459] [数 17]

[0460] $$\sum_{j=i+1}^{i+3d} D_j \geq B_1^D + B_2^D$$

。

[0461] 当综合以上的情况 1 和情况 2 时，证明出

[0462] [数 18]

[0463] $$\sum_{j=i+1}^{i+3d} D_j \geq B_1^D + B_2^D$$ 即，

。

[0464] $ActD(3d) \geq B_1^D + B_2^D$

[0465] 成立，证明出包含在图 8、图 10 所示的类型 1 的扩展 Feistel 结构中连续的 3d 个循环中的差分有效 S 盒的个数为 $B_1^D + B_2^D$ 以上。

[0466] （证明 2. $ActL(3d) \geq 2B_2^L$ 的证明）

[0467] 接着，证明 $ActL(3d) \geq 2B_2^L$。

[0468] 即，证明包含在图 8、图 10 所示的类型 1 的扩展 Feistel 结构中连续的 3d 个循环中的线性有效 S 盒的个数为 $2B_2^L$ 以上。

[0469] 此外，B_2^L 如上所述那样，定义为

[0470] [数 19]

[0471] $$B_2^L = \min_i(Branch_n([{}^tM_i^{-1} | {}^tM_{i+d}^{-1}]))$$

。

[0472] 另外，设为用 L_k 表示包含在第 k 个 F 函数中的线性有效 S 盒的数量。

[0473] 在类型 1 的扩展 Feistel 结构中提供了输入不是零的线性掩模的情况下，具有以下两个性质。

[0474] （性质 5）在连续的 d 个循环中的至少一个循环中存在不是 0 的线性有效 S 盒

[0475] （性质 6）$L_k + L_{k+1} + L_{k+d} \geq B_2^L$、或者 $L_k + L_{k+1} + L_{k+d} = 0$。此外，在 $L_k + L_{k+1} + L_{k+d} \geq B_2^L$ 的情况下，左边包含的两个以上的项不会同时为 0。

[0476] 利用以上两个性质，进行

[0477] $ActL(3d) \geq 2B_2^L$

[0478] 的证明、即证明“包含在连续的 3d 个循环中的线性有效 S 盒的个数为 $2B_2^L$ 以上”。

[0479] 考虑作为对象的循环为从第 i+1 个到第 i+3d 个的循环。

[0480] 情况 1：假设在从第 i+d+2 个循环到第 i+2d 个循环中存在不是 0 的有效 S 盒的情况。

[0481] 当将存在不是 0 的有效 S 盒的循环设为 k 时，$L_k \neq 0$。

[0482] 情况 1-1：除了情况 1，在 $L_{k+d} \neq 0$ 或者 $L_{k-1} \neq 0$ 的情况下，

[0483] 根据性质 6，$L_k + L_{k+d} + L_{k+1} \geq B_2^L$

[0484] 根据性质 6，$L_{k-1} + L_{k-1-d} + L_{k-d} \geq B_2^L$，

[0485] 因此得出

[0486] $$\sum_{j=i+1}^{i+3d} L_j \geq 2B_2^L$$

。

[0487] 情况 1-2 :除了情况 1,在 $L_{k+d} = 0$ 并且 $L_{k-1} = 0$ 的情况下,

[0488] 根据性质 6,$L_{k-d+1} \neq 0$

[0489] 根据性质 6,$L_k+L_{k-1}+L_{k+d-1} \geq B_2^L$

[0490] 根据性质 6,$L_{k-d+1}+L_{k+1}+L_{k-d+2} \geq B_2^L$

[0491] 此时如果 d ≥ 4,则得出

[0492] [数 21]

[0493] $$\sum_{j=i+1}^{i+3d} L_j \geq 2B_2^L$$

。

[0494] 如果 d = 3,则虽然 L_{k-1} 重复,但是已知 $L_{k-1} = 0$,因此同样得出

[0495] [数 22]

[0496] $$\sum_{j=i+1}^{i+3d} L_j \geq 2B_2^L$$

。

[0497] 情况 2 :假设在从第 i+d+2 个循环到第 i+2d-1 个循环中不存在不是 0 的有效 S 盒的情况。

[0498] 根据性质 5,得出 $L_{i+d+1} \neq 0$。

[0499] 根据性质 6,$L_{i+d} \neq 0$

[0500] 根据性质 6,$L_{i+d+1}+L_{i+d+2}+L_{i+2d+1} \geq B_2^L$

[0501] 根据性质 6,$L_{i+d}+L_{i+d-1}+L_{i+2d-1} \geq B_2^L$

[0502] 此时,如果 d ≥ 4,则得出

[0503] [数 23]

[0504] $$\sum_{j=i+1}^{i+3d} L_j \geq 2B_2^L$$

。

[0505] 如果 d = 3,则虽然 L_{i+5} 重复,但是已知 $L_{i+5} = 0$,因此同样得出

[0506] [数 24]

[0507] $$\sum_{j=i+1}^{i+3d} L_j \geq 2B_2^L$$

。

[0508] 当综合以上的情况 1 和情况 2 时,证明出

[0509] $\sum_{j=i+1}^{i+3d} L_j \geq 2B_2^L$ 即，

。

[0510] ActL(3d) ≥ $2B_2^L$ 成立，证明出包含在图 8、图 10 所示的类型 1 的扩展 Feistel 结构中连续的 3d 个循环中的线性有效 S 盒的个数为 $2B_2^L$ 以上。

[0511] (6-2. 扩展 Feistel 结构的类型 2 的有效 S 盒数与基于 F 函数中的线性变换矩阵的最小分支数之间的关系式的证明）

[0512] 接着，说明参照图 9 所说明的扩展 Feistel 结构的类型 2 的有效 S 盒数与基于 F 函数中的线性变换矩阵的最小分支数之间的关系式的证明。

[0513] 即，证明将包含在类型 2 的扩展 Feistel 结构中的连续的 p 个循环中的差分有效 S 盒数记载为 ActD(p)、将线性有效 S 盒数记载为 ActL(p) 的情况下的关系式

[0514] ActD(6) ≥ $B_1^D+B_2^D$

[0515] ActL(6) ≥ $2B_2^L$

[0516] 该关系式成立。

[0517] 能够如图 11 所示那样以其它的形式表示之前参照图 9 所说明的扩展 Feistel 结构的类型 2 的结构。在图 9 中，在每个循环中轮换表示各数据序列的排列，但是图 11 不进行数据序列的轮换，而以一条直线表示。在图 11 中，表示循环 1 ～ 12。将两个循环 (1 ～ 2、3 ～ 4、• •) 的 F 函数排列在一条横线上来显示。例如，在第一个循环中并行地执行图 11 所示的循环 1 ～ 2 的横线上表示出的 F 函数 $F_{1,0}$ ～ $F_{1,d-1}$ 中的 $F_{1,0}$、$F_{1,2}$、…、$F_{1,d-2}$ 的每隔一个的 F 函数（输出的箭头向上）。在接下来的第二个循环中并行地执行剩余的 $F_{1,1}$、$F_{1,3}$、…、$F_{1,d-1}$ 的每隔一个的 F 函数（输出的箭头向下）。

[0518] 在图 11 中，用于识别 F 函数的编号是为了容易理解证明而新导入的编号，使用两个数字决定 F 函数的位置。

[0519] $F_{i,j}$ 的 i 表示循环数 (1 = 1、2 循环，2 = 3、4 循环 • •)，j 表示两个循环中的 F 函数之一。此外，如果 j 是 0、2、4 的偶数，则为先行循环中的 F 函数，如果 j 是 1、3、5 的奇数，则为后续循环中的 F 函数。此外，将包含在 F 函数 $F_{i,j}$ 中的线性变换矩阵称为 $[M_{i,j}]$。

[0520] 证明在该扩展 Feistel 结构的类型 2 的结构中之前在 (5-2. 对于扩展 Feistel 结构的类型 2 的 DSM 的应用）中说明的关系式

[0521] ActD(6) ≥ $B_1^D+B_2^D$

[0522] ActL(6) ≥ $2B_2^L$

[0523] 成立。

[0524] 在上式中，

[0525] ActD(6)、ActL(6) 意味着包含在图 9 或图 11 所示的类型 2 的扩展 Feistel 结构中的连续的 6 个循环中的差分有效 S 盒数和线性有效 S 盒数。

[0526] B_1^D 是包含在类型 2 的扩展 Feistel 结构中的 F 函数中的线性变换矩阵的分支数中的最小的分支数，

[0527] B_2^D、B_2^L 是包含在之前在 (4-2)、(4-3) 中所说明的扩展 Feistel 结构中的对一个数据序列进行输入的连续的 F 函数中的线性变换矩阵的关联矩阵的最小分支数、以及逆矩阵

的转置矩阵的关联矩阵的最小分支数。

[0528] 将 B_1^D、B_2^D、B_2^L 定义为如下。

[0529] [数 26]

[0530] $$B_1^D = \min_{i,j}(Branch_n(M_{i,j}))$$

[0531] $$B_2^D = \min_{i,j}(Branch_n([M_{i,j} \mid M_{i+1,j}]))$$

[0532] $$B_2^L = \min_{i,j}(Branch_n([{}^tM_{i,j}^{-1} \mid {}^tM_{i+1,j}^{-1}]))$$

[0533] 此外，在上述定义中，

[0534] $B_1^D \geqslant B_2^D$

[0535] 的关系成立。

[0536] 另外，用 $D_{p,q}$ 表示包含在 $F_{p,q}$ 中的有效 S 盒数。此外，以后，在下标 q 的部分具有负值或 d 以上的值的情况下，设为利用 d 进行剩余运算 (q mod d) 来进行补正使得总是成为 $0 \leqslant q < d$。

[0537] (证明 3. ActD(6) $\geqslant B_1^D+B_2^D$ 的证明)

[0538] 首先，证明 ActD(6) $\geqslant B_1^D+B_2^D$。

[0539] 即，证明包含在图 9、图 11 所示的类型 2 的扩展 Feistel 结构中连续的 6 个循环中的差分有效 S 盒的个数为 $B_1^D+B_2^D$ 以上。

[0540] 考察在类型 2 的扩展 Feistel 结构中提供输入了不是零的差分 (ΔX) 的情况。在这种情况下，类型 2 的扩展 Feistel 结构具有以下四个性质。

[0541] (性质 1) 对于某个 i，在 $F_{p,q}$ ($p = i$、$q \in \{0、\cdots d-1\}$) 中存在不是 0 的差分有效 S 盒

[0542] (性质 2) 如果 $D_{p,q} = 0$，则

[0543] $D_{p-1,q+1} = D_{p,q+1}$ (q 是偶数时)

[0544] $D_{p,q+1} = D_{p+1,q+1}$ (q 是奇数时)

[0545] (性质 3) 如果 $D_{p,q} \neq 0$，则

[0546] $D_{p,q}+D_{p-1,q+1}+D_{p,q+1} \geqslant B_1^D$ (q 是偶数时)

[0547] $D_{p,q}+D_{p,q+1}+D_{p+1,q+1} \geqslant B_1^D$ (q 是奇数时)

[0548] (性质 4) 如果 $D_{p,q}+D_{p+1,q} \neq 0$，则

[0549] $D_{p,q}+D_{p+1,q}+D_{p-1,q+1}+D_{p+1,q+1} \geqslant B_2^D$ (q 是偶数时)

[0550] $D_{p,q}+D_{p+1,q}+D_{p,q+1}+D_{p+2,q+1} \geqslant B_2^D$ (q 是奇数时)

[0551] 利用以上四个性质，进行

[0552] ActD(6) $\geqslant B_1^D+B_2^D$

[0553] 的证明、即证明“对于 1 以上的任意整数 i，包含在满足 $p \in \{i、i+1、i+2\}$、$q \in \{0、1、\cdots d-1\}$ 的 3d 个 F 函数 $F_{p,q}$ 中的差分有效 S 盒的总数为 $B_1^D+B_2^D$ 以上”。

[0554] 在任意取出 $D_{p,q}$ ($p = i+1$、$q \in \{0、\cdots d-1\}$) 的非零要素时，将其设为 $D_{j,k} \neq 0$。根据上述的 (性质 1) 示出一定存在。

[0555] 情况 1 :在 $D_{j,k-1} \neq 0$ 的情况下，

[0556] 根据性质 3，

[0557] $D_{j,k}+D_{j-1,k+1}+D_{j,k+1} \geq B_1^D$(k 是偶数时)

[0558] $D_{j,k}+D_{j,k+1}+D_{j+1,k+1} \geq B_1^D$(k 是奇数时)

[0559] 根据性质 4，

[0560] $D_{j-1,k-1}+D_{j,k-1}+D_{j-1,k}+D_{j+1,k} \geq B_2^D$(k 是偶数时)

[0561] $D_{j,k-1}+D_{j+1,k-1}+D_{j-1,k}+D_{j+1,k} \geq B_2^D$(k 是奇数时)，

[0562] 因此

[0563] [数 27]

[0564] $$\sum_{p=i}^{i+2}\sum_{q=0}^{d-1} D_{p,q} \geq B_1^D + B_2^D$$

[0565] 成立。

[0566] 情况 2 :在 $D_{j,k+1} \neq 0$ 的情况下，

[0567] 根据性质 3，

[0568] $D_{j,k+1}+D_{j,k+2}+D_{j+1,k+2} \geq B_1^D$(k 是偶数时)

[0569] $D_{j,k+1}+D_{j-1,k+2}+D_{j,k+2} \geq B_1^D$(k 是奇数时)

[0570] 根据性质 4，

[0571] $D_{j,k}+D_{j+1,k}+D_{j-1,k+1}+D_{j+1,k+1} \geq B_2^D$(k 是偶数时)

[0572] $D_{j-1,k}+D_{j,k}+D_{j-1,k+1}+D_{j+1,k+1} \geq B_2^D$(k 是奇数时)，

[0573] 因此

[0574] $$\sum_{p=i}^{i+2}\sum_{q=0}^{d-1} D_{p,q} \geq B_1^D + B_2^D$$

[0575] 成立。

[0576] 情况 3 :在 $D_{j,k-1} = 0$ 并且 $D_{j,k+1} = 0$ 的情况下，

[0577] 根据性质 2，$D_{j,k-1} = 0$，因此

[0578] $D_{j+1,k} = D_{j,k} \neq 0$(k 是偶数时)

[0579] $D_{j-1,k} = D_{j,k} \neq 0$(k 是奇数时)

[0580] 根据性质 3，

[0581] $D_{j,k}+D_{j-1,k+1}+D_{j,k+1} \geq B_1^D$(k 是偶数时)

[0582] $D_{j,k}+D_{j,k+1}+D_{j+1,k+1} \geq B_1^D$(k 是奇数时)

[0583] 还根据性质 3，

[0584] $D_{j+1,k}+D_{j,k+1}+D_{j+1,k+1} \geq B_1^D$(k 是偶数时)

[0585] $D_{j-1,k}+D_{j-1,k+1}+D_{j,k+1} \geq B_1^D$(k 是奇数时)

[0586] $D_{j,k+1} = 0$，因此

[0587] $$\sum_{p=i}^{i+2}\sum_{q=0}^{d-1} D_{p,q} \geq B_1^D + B_2^D$$

[0588] 成立。

[0589] 当综合以上时，证明出

[0590] $$\sum_{p=i}^{i+2}\sum_{q=0}^{d-1} D_{p,q} \geq B_1^D + B_2^D$$

。

[0591] 即，

[0592] $ActD(6) \geqslant B_1^D + B_2^D$

[0593] 成立，证明出包含在图9、图11所示的类型2的扩展Feistel结构中连续6个循环中的差分有效S盒的个数为 $B_1^D+B_2^D$ 以上。

[0594] （证明4.$ActL(6) \geqslant 2B_2^L$ 的证明）

[0595] 接着，证明 $ActL(6) \geqslant 2B_2^L$。

[0596] 即，证明包含在图9、图11所示的类型2的扩展Feistel结构中连续6个循环中的线性有效S盒的个数为 $2B_2^L$ 以上。

[0597] 此外，如上所述，B_2^L 定义为

[0598] $$B_2^L = \min_{i,j}(Branch_n([{}^tM_{i,j}^{-1}|{}^tM_{i+1,j}^{-1}]))$$

。

[0599] 另外，设为用 $L_{p,q}$ 表示包含在第 $F_{p,q}$ 个F函数中的线性有效S盒数。

[0600] 在类型2的扩展Feistel结构中提供了输入不是零的线性掩模的情况下，具有以下两个性质。

[0601] （性质5）对于某个i，在 $F_{p,q}$（$p = i$、$q \in \{0、\cdots d-1\}$）中存在不是0的线性有效S盒

[0602] （性质6）

[0603] $L_{j,k}+L_{j+1,k}+L_{j,k+1} \geqslant B_2^L$、或者 $L_{j,k}+L_{j+1,k}+L_{j,k+1} = 0$（k是偶数时）

[0604] $L_{j,k}+L_{j+1,k}+L_{j+1,k+1} \geqslant B_2^L$、或者 $L_{j,k}+L_{j+1,k}+L_{j+1,k+1} = 0$（k是奇数时）

[0605] 此外，在 $L_a+L_b+L_c \geqslant B_2^L$ 的形式的情况下，左边包含的两个以上的项不会同时为0。

[0606] 利用以上两个性质，进行

[0607] $ActL(6) \geqslant 2B_2^L$

[0608] 的证明、即证明“对于1以上的任意整数i，包含在满足 $p \in \{i、i+1、i+2\}$、$q \in \{0、1、\cdots d-1\}$ 的3d个F函数 $F_{p,q}$ 中的线性有效S盒的总数为 $2B_2^L$ 以上”。

[0609] 在任意取出 $L_{p,q}$（$p = i+1$、$q \in \{0、\cdots d-1\}$）的不是0的要素时，将其设为 $L_{j,k} \neq 0$。根据性质5示出一定存在上述 $L_{j,k}$。

[0610] 根据性质6，

[0611] $L_{j-1,k}+L_{j,k}+L_{j-1,k+1} \geqslant B_2^L$（k是偶数时）

[0612] $L_{j,k}+L_{j+1,k}+L_{j+1,k+1} \geqslant B_2^L$（k是奇数时）

[0613] 情况1：在 $L_{j,k-1} \neq 0$ 的情况下，

[0614] 根据性质6，

[0615] $L_{j,k-1}+L_{j+1,k-1}+L_{j+1,k} \geqslant B_2^L$（k是偶数时）

[0616] $L_{j-1,k-1}+L_{j,k-1}+L_{j-1,k} \geqslant B_2^L$（k是奇数时）

[0617] 因而，在这种情况下，

[0618] $$\sum_{p=i}^{i+2}\sum_{q=0}^{d-1} L_{p,q} \geq B_2^L$$

[0619] 成立。

[0620] 情况 2 :在 $L_{j,k-1} = 0$ 的情况下，

[0621] 根据性质 6，

[0622] $L_{j-1,k-1} \neq 0$(k 是偶数时)

[0623] $L_{j+1,k-1} \neq 0$(k 是奇数时)

[0624] 因此，

[0625] $L_{j-1,k-2}+L_{j,k-2}+L_{j-1,k-1} \geq B_2^L$(k 是偶数时)

[0626] $L_{j,k-2}+L_{j+1,k-2}+L_{j+1,k-1} \geq B_2^L$(k 是奇数时)

[0627] 此时 d ≥ 4，因此，在这种情况下

[0628] $$\sum_{p=i}^{i+2}\sum_{q=0}^{d-1} L_{p,q} \geq B_2^L$$

[0629] 成立。

[0630] 当综合以上的情况 1 和情况 2 时，证明出

[0631] $$\sum_{p=i}^{i+2}\sum_{q=0}^{d-1} L_{p,q} \geq B_2^L$$ 即，

。

[0632] $ActL(6) \geq 2B_2^L$

[0633] 成立，证明出包含在图 9、图 11 所示的类型 2 的扩展 Feistel 结构中连续的 6 个循环中的线性有效 S 盒的个数为 $2B_2^L$ 以上。

[0634] 如上所述，在本发明中实现如下结构 :在将数据序列数 :d 设为 d ≥ 2 的整数的扩展 Feistel 结构中，作为各循环的 F 函数的线性变换处理，应用选择性地应用至少两个以上的不同的矩阵的所谓的扩散矩阵切换机构 (DSM)，由此提高对线性分析、差分分析的抵抗性。

[0635] 这样，在利用硬件来实现执行选择应用不同的多个矩阵的运算处理的结构的情况下，需要具有进行与各个矩阵对应的运算的硬件结构的不同的 F 函数处理部。特别是要在一个循环中并行地执行多个 F 函数的情况下，需要用于进行并行处理的多个 F 函数用电路。

[0636] 即，在之前参照图 9、图 11 说明的类型 2 的扩展 Feistel 结构中，是并行地执行在同一循环中应用了多个 F 函数的数据变换处理的结构，在利用硬件执行基于该类型 2 的结构的处理的情况下，需要安装在一个循环中并行执行的个数的 F 函数的硬件。即使在这种被要求并行执行的 F 函数是相同结构的情况下，也必须具备多个具有该相同结构的 F 函数的硬件。

[0637] 如上所述，本发明的密码处理结构具有如下结构 :通过设为在各循环的 F 函数中执行的线性变换处理中选择性地应用至少两个以上的多个不同的矩阵的结构，提高了对各

种攻击的抵抗性。即，设为具备扩散矩阵切换机构 (DSM :DiffusionSwitching Mechanism) 的结构。

[0638] 为了满足该扩散矩阵切换机构 (DSM)，只要满足设定为多个不同的矩阵等条件即可，并不特别限定在各循环中并行执行的 F 函数，其中，上述多个不同的矩阵满足如下条件 :从根据线性变换矩阵而算出的与数据序列对应的最小分支数 $[B_k^D(s(i))]$ 中选择的全部数据序列中的最小分支数 $[B_k^D]$ 为 3 以上，其中，所述线性变换矩阵包含在对扩展 Feistel 结构的各数据序列 s(i) 进行输入的连续的 k 个 (其中，k 为 2 以上的整数)F 函数中。

[0639] 下面，根据该特性说明在扩展 Feistel 结构中维持基于扩散矩阵切换机构 (DSM) 的抵抗性的同时提高了安装效率的结构例。

[0640] (7-1. 扩展 Feistel 的类型 2 的有效的 F 函数配置方法)

[0641] 首先，说明之前参照图 9、图 11 所说明的扩展 Feistel 的类型 2 的有效的 F 函数配置结构。如在之前所说明的项目 (5-2. 对于扩展 Feistel 结构的类型 2 的 DSM 的应用) 中记述的那样，类型 2 的扩展 Feistel 结构具有以下参数。

[0642] 参数

[0643] (a) 数据分割数 :d(其中，d 为 4 以上的偶数)

[0644] (b) 输入输出数据长度 :dmn 比特

[0645] (c) 分割数据长度 :mn 比特

[0646] (d) 每一个循环的 F 函数的数量 :d/2

[0647] 即，如图 9 所示，在各循环内，对从左端起处于第奇数个的 mn 比特的数据序列应用 F 函数，将 F 函数的处理结果输出到紧邻的数据序列并进行异或。此外，在图 9 中省略异或的运算标记。

[0648] 下面，说明提高对于具有这种结构的类型 2 的扩展 Feistel 结构的安装效率的结构。作为一例，参照图 12 说明数据序列数 (分割数)d = 4 的情况。在图 12 中，将由两个不同的线性变换矩阵 M_1、M_2 执行线性变换的不同的两个 F 函数分别设为 F1、F2。

[0649] 图 12 所示的 Feistel 结构是使用 F 函数 F1、F2 这两个 F 函数的 d = 4 的扩展 Feistel 结构的类型 2。即，是具有

[0650] (a) 数据分割数 :4

[0651] (b) 输入输出数据长度 :4mn 比特

[0652] (c) 分割数据长度 :mn 比特

[0653] (d) 每一个循环的 F 函数的数量 :4/2 = 2

[0654] 的结构。

[0655] 在该图 12 所示的结构的情况下，为了使用两个 F 函数满足 DSM 条件而考虑几种配置。即，为了满足 DSM 条件，如上所述那样，只要满足设定为多个不同的矩阵等条件即可，并不特别限定在各循环中并行执行的 F 函数，其中，上述多个不同的矩阵满足以下条件 :从根据线性变换矩阵而算出的与数据序列对应的最小分支数 $[B_k^D(s(i))]$ 中选择的全部数据序列中的最小分支数 $[B_k^D]$ 为 3 以上，其中，所述线性变换矩阵包含在对各数据序列 s(i) 进行输入的连续的 k 个 (其中，k 为 2 以上的整数)F 函数中。

[0656] 因而，作为 F 函数的设定方式，

[0657] (a) 将设定在一个循环中的多个 F 函数设为相同的 F 函数的设定、

[0658] (b) 将设定在一个循环中的多个 F 函数设为不同的 F 函数的设定

[0659] 能够设定为上述两种方式。

[0660] 在此，如图 12 所示，采用如下结构：选择在一个循环中存在的两个 F 函数使得相互成为 F1、F2。在以一个循环的处理为基础进行硬件 (H/W) 安装的情况下，该结构的优点表现得明显。

[0661] 即，作为硬件 (H/W) 安装，设定具有仅能够执行一个循环的处理的结构、即如图 13 所示那样能够并行地执行 F 函数 F1 和函数 F2 的结构的硬件。图 13 是表示具有执行基于图 12 所示的扩展 Feistel 结构的密码处理的硬件结构的密码处理装置 250 的框图。

[0662] 密码处理装置 250 由执行 F 函数 F1 的第一 F 函数 (F1) 专用处理电路 251、执行 F 函数 F2 的第二 F 函数 (F2) 专用处理电路 252、控制电路 253 以及辅助电路 254 构成。第一 F 函数 (F1) 专用处理电路 251 和第二 F 函数 (F2) 专用处理电路 252 是能够并行地进行动作的结构，在各循环中，应用这两个电路执行基于两个不同的 F 函数的数据变换。

[0663] 控制电路 253 执行对各 F 函数专用处理电路 251、252 以及辅助电路 254 的输入输出数据的控制。辅助电路 254 执行 F 函数以外的运算处理等。

[0664] 通过应用该结构，应用第一 F 函数 (F1) 专用处理电路 251、第二 F 函数 (F2) 专用处理电路 252 能够进行仅所需的循环数的循环运算。在所有的循环中并行地执行两个 F 函数专用电路，能够实现没有设置多余的电路的安装。

[0665] 如图 12 所示，在各循环中并行地执行的 F 函数是两个的情况下，通过将这两个 F 函数设定为不同的 F 函数，利用图 13 所示的硬件安装，能够进行所有的循环运算。顺便提及，在设为在一个循环中执行的 F 函数相同的设定、例如在第一循环中并行地执行 F1、F1，在第二循环中执行 F2、F2 的结构的情况下，作为硬件，需要设置 F1 执行电路和 F2 执行电路各两个，与图 13 所示的结构相比，需要增大电路规模。

[0666] 通过如图 12 所示那样将在各循环中执行的 F 函数的组合全部设定为 F1、F2，应用图 13 所示的硬件，能够在各循环中始终同时执行 F1、F2，不会产生多余的电路，而实现减小电路规模的小型装置。

[0667] 图 12 所示的结构是数据序列 d ＝ 4 的情况，但是在其它数据序列数的情况下，通过设为同样的设定，也能够实现有效的安装。例如在数据序列数 d ＝ 8 的情况下，设为如下结构：在一个循环中设定 4 个 F 函数，将该 4 个 F 函数设定为两个不同的 F 函数 F1、F2 各两个。

[0668] 这种情况下的安装结构设为如下结构：设置 F 函数 F1、F2 各两个，能够并行地执行 4 个 F 函数 (F1、F1、F2、F2)。通过该结构，能够在所有的循环中并行地执行全部 4 个 F 函数，实现没有设置多余的电路的安装。

[0669] 另外，在数据序列数 d ＝ 16 的情况下，将在一个循环中存在的 8 个 F 函数设定为 F1、F2 各四个。并且，一般化为在数据序列数 d ＝ 4x 的情况下在各循环中利用 F 函数 F1、F2 各 x 个的结构，作为硬件安装，如果设为设定 F 函数 F1、F2 各 x 个的结构，则由于在每个循环中需要的 F1、F2 的个数相同，因此不会过多或过少地执行 F 函数，能够提高安装效率。

[0670] 上述的处理例是为了满足扩散矩阵切换机构 (DSM) 而设定了应用两个线性变换矩阵的两个不同的 F 函数的例子，但是即使在使用三种以上的线性变换矩阵来设定三种以上的 F 函数的情况下也可以说是相同的。

[0671] 图 14 示出用于有效安装三种 F 函数的配置例。图 14 是数据序列数 d ＝ 6 的扩展 Feistel 的类型 2 的结构例。在该图 14 所示的结构中，进行设定使其成为在一个循环中存在的三个 F 函数一定利用 F1、F2、F3 各一个的结构。

[0672] 通过该结构，在硬件 (H/W) 安装时仅安装 F1、F2、F3 各一个，就能够成为在各循环中并行地执行 F 函数的结构，从 H/W 方面来看实现没有多余的电路的电路结构。

[0673] 并且，在数据序列数 d ＝ 12 的情况下，将在一个循环中存在的 6 个 F 函数设定为 F1、F2、F3 各两个。另外，在数据序列数 d ＝ 18 的情况下，关于在一个循环中设定的 9 个 F 函数，设定为 F1、F2、F3 各三个。将它们一般化为在数据序列数 d ＝ 6x 的情况下将在各循环中设定的 F 函数设定为 F1、F2、F3 各 x 个。即，设为在各循环中均等地利用不同的 F 函数的结构。

[0674] 通过设为这种 F 函数的设定结构，能够将每个循环中需要的 F1、F2、F3 的个数设定为相同的数量，在硬件安装中能够设定不会过多或者过少地利用的电路，能够提高安装效率。在软件的情况下，也由于用于获取输入输出值的表的利用方式在各循环中相同，因此不用构成设想各种模式的表，而能够设定与一个利用方式相应的表并保存到存储器中。

[0675] 当将上述各处理例进一步一般化时，如下所述。

[0676] (1) 在构成利用了 a 种 F 函数的 Type2 的扩展 Feistel 结构的情况下，通过设为如下结构能够提高安装效率：当设数据序列数 (分割数)d ＝ 2ax、其中 a 为 2 以上的整数、x 为 1 以上的整数时，均等地设定全部种类的 F 函数各 x 个作为在一个循环内设定的 ax 个 F 函数。

[0677] 此外，在上述 F 函数的设定中，通过将对各数据序列进行输入的 F 函数的设定设为满足上述 DSM 条件的设定，能够维持抵抗性。

[0678] (7-2. Feistel 结构与扩展 Feistel 结构中的部件的共用化)

[0679] 如上所述，通过对目前为止所说明的 Feistel 结构、扩展 Feistel 的类型 1、扩展 Feistel 的类型 2 中的任一个利用 DSM 机构，而具有提高对攻击的抵抗性的优点。

[0680] 即，将 Feistel 结构大致分类为

[0681] (a) 设为数据序列数 (分割数)d ＝ 2 的 Feistel 结构

[0682] (b) 设为数据序列数 (分割数)d ≥ 2 的任意数的扩展 Feistel 结构，

[0683] 并且，扩展 Feistel 结构为

[0684] (b1) 在各循环中仅允许执行一个 F 函数的类型 1、

[0685] (b2) 在各循环中允许并行执行多个 F 函数的类型 2，

[0686] 从而，能够将 Feistel 结构分类为 (a)、(b1)、(b2) 这三种。

[0687] 在这三种 Feistel 结构的任一种中都通过应用 DSM 机构实现抵抗性的提高。

[0688] 为了应用 DSM 机构，需要安装执行至少两个以上不同的线性变换矩阵的不同的 F 函数，但是，通过具有该不同的多个 F 函数的安装结构，能够实现可选择性地执行上述多个不同的 Feistel 结构 (a)、(b1)、(b2) 的装置。下面说明执行这种选择处理的装置结构。

[0689] 决定执行满足扩散矩阵切换机构 (DSM) 的线性变换矩阵的多个不同的 F 函数，将这些各 F 函数中的输入输出数据的数据大小设为 mn 比特。通过应用这种 F 函数，例如在如图 15 所示的数据序列 d ＝ 2 的 Feistel 结构中执行 2mn 比特的块密码。

[0690] 图 15 所示的数据序列 d ＝ 2 的 Feistel 结构的各 F 函数 F1、F2 的输入输出数据

大小是 mn 比特。该数据序列 d = 2 的 Feistel 结构进行将 2mn 比特的明文转换为 2mn 比特的密文的处理、或者与其相反的解密处理，执行 2mn 比特的块密码。

[0691] 另外，通过利用该图 15 所示的输入输出数据大小为 mn 比特的 F 函数 F1、F2，能够构成满足扩散矩阵切换机构 (DSM) 的数据序列数 d = 4 的扩展 Feistel 结构。图 16 示出该结构。

[0692] 图 16 所示的数据序列 d = 4 的扩展 Feistel 结构的各 F 函数 F1、F2 是输入输出数据大小为 mn 比特、按原样应用图 15 所示的 F 函数 F1、F2 的 F 函数。该数据序列 d = 4 的扩展 Feistel 结构进行将 4mn 比特的明文转换为 4mn 比特的密文的处理、或者与其相反的解密处理，执行 4mn 比特的块密码。

[0693] 并且，一般化为在设为数据序列数 d = x、其中 x 为 2 以上的整数的情况下，能够使用相同的 F 函数执行结构来构建执行 xmn 比特的加密或者解密处理的块密码结构。

[0694] 例如，仅使用输入输出比特为 64 比特的不同的 F 函数 F1、F2，就能够构成可选择性地执行实现 DSM 机构的输入输出 128 比特块密码处理和 256 比特块密码处理。

[0695] 即，安装输入输出比特为 64 比特的不同的两个 F 函数 F1、F2 作为 F 函数，并控制它们的利用方式。例如，在执行基于设为数据序列数 d = 2 的 Feistel 结构 (图 15) 的密码处理的情况下，设为在各循环中执行各 F 函数 F1、F2 之一的结构。另一方面，在执行基于设为数据序列数 d = 4 的扩展 Feistel 结构 (图 16) 的密码处理的情况下，设为在各循环中并行地执行各 F 函数 F1、F2 的结构。这样，通过安装两种 F 函数，实现能够选择性地执行输入输出 128 比特块密码和 256 比特块密码的装置。即，通过使用相同的 F 函数、改变连接方法，能够执行不同比特数的块密码，在 S/W、H/W 两者中能够期望通过电路、代码的共享等来提高安装效率。

[0696] 图 17 示出具有这种结构的密码处理装置的结构例。图 17 所示的密码处理装置 270 由执行 F 函数 F1 的第一 F 函数 (F1) 专用处理电路 271、执行 F 函数 F2 的第二 F 函数 (F2) 专用处理电路 272、控制电路 273 以及辅助电路 274 构成。第一 F 函数 (F1) 专用处理电路 271 和第二 F 函数 (F2) 专用处理电路 272 是能够并行地进行动作的结构。控制电路 273 对各处理部进行数据输入输出控制，并且执行 Feistel 结构选择处理。辅助电路 274 执行 F 函数以外的运算处理等。

[0697] 作为 Feistel 结构选择处理，控制电路 273 选择执行基于以下的任一个结构的密码处理 ：

[0698] (a) 设为数据序列数 (分割数)d = 2 的 Feistel 结构

[0699] (b1) 是设为数据序列数 (分割数)d ≥ 2 的任意数的扩展 Feistel 结构，在各循环中仅允许执行一个 F 函数的类型 1、

[0700] (b2) 是设为数据序列数 (分割数)d ≥ 2 的任意数的扩展 Feistel 结构，在各循环中允许并行执行多个 F 函数的类型 2。

[0701] 此外，例如从外部输入设定信息。或者也可以设为根据成为加密或解密处理的对象的数据的比特长度来选择要执行的处理方式的结构。控制电路 273 进行根据选择变更各 F 函数专用电路的应用顺序，执行按照各 Feistel 结构的循环函数的控制。

[0702] 通过应用该结构，应用第一 F 函数 (F1) 专用处理电路 271 和第二 F 函数 (F2) 专用处理电路 272 能够进行应用了各种 Feistel 结构的密码处理，能够执行加密处理或解密

处理的处理比特不同的对应各种比特的密码处理。

[0703] 另外，图 17 示出具有两个 F 函数的例子，但是并不限于使用两个 F 函数的例子，在使用任意个数的 F 函数的结构中也能够期望得到同样的效果。例如，在之前参照图 14 所说明的扩展 Feistel 结构中，应用三个不同的 F 函数 F1、F2、F3 构成满足扩散矩阵切换机构 (DSM) 的数据序列数 d = 6 的扩展 Feistel 结构。能够应用与其相同的三种 F 函数 F1、F2、F3 的 F 函数来构建图 18 所示的具有数据序列 d = 2 的 Feistel 结构的密码处理结构。在该数据序列 d = 2 的结构中，也利用满足 DSM 机构的设定来配置各函数 F1、F2、F3。

[0704] 图 19 示出执行这样的三种 F 函数 F1、F2、F3 的密码处理装置的结构例。图 19 所示的密码处理装置 280 由执行 F 函数 F1 的第一 F 函数 (F1) 专用处理电路 281、执行 F 函数 F2 的第二 F 函数 (F2) 专用处理电路 282、执行 F 函数 F3 的第三 F 函数 (F3) 专用处理电路 283、控制电路 284 以及辅助电路 285 构成。第一 F 函数 (F1) 专用处理电路 281、第二 F 函数 (F2) 专用处理电路 282 以及第三 F 函数 (F3) 专用处理电路 283 是能够并行地进行动作的结构。控制电路 284 对各处理部进行数据输入输出控制，并且执行 Feistel 结构选择处理。辅助电路 285 执行 F 函数以外的运算处理等。

[0705] 作为 Feistel 结构选择处理，控制电路 284 选择执行基于以下的任一个结构的密码处理 ：

[0706] (a) 设为数据序列数 (分割数)d = 2 的 Feistel 结构

[0707] (b1) 是设为数据序列数 (分割数)d ≥ 2 的任意数的扩展 Feistel 结构，在各循环中仅允许执行一个 F 函数的类型 1、

[0708] (b2) 是设为数据序列数 (分割数)d ≥ 2 的任意数的扩展 Feistel 结构，在各循环中允许并行执行多个 F 函数的类型 2。

[0709] 此外，例如从外部输入设定信息。控制电路 284 进行根据设定变更各 F 函数专用电路的应用顺序，执行按照各 Feistel 结构的循环函数的控制。

[0710] 通过应用该结构，应用第一 F 函数 (F1) 专用处理电路 281 ～第三 F 函数 (F3) 专用处理电路 283 能够进行应用了各种 Feistel 结构的密码处理，能够执行加密处理或解密处理的处理比特不同的对应各种比特的密码处理。此外，也可以是具有 4 个以上 F 函数执行部的结构。

[0711] 如上所述，决定执行满足扩散矩阵切换机构 (DSM) 的线性变换矩阵的多个不同的 F 函数，安装这些各 F 函数，变更应用了 F 函数的处理顺序，由此实现选择性地执行基于以下任一个结构的密码处理的结构，并实现能够变更加密处理或解密处理中的处理比特数的装置，

[0712] (a) 设为数据序列数 (分割数)d = 2 的 Feistel 结构

[0713] (b1) 是设为数据序列数 (分割数)d ≥ 2 的任意数的扩展 Feistel 结构，在各循环中仅允许执行一个 F 函数的类型 1、

[0714] (b2) 是设为数据序列数 (分割数)d ≥ 2 的任意数的扩展 Feistel 结构，在各循环中允许并行执行多个 F 函数的类型 2。

[0715] 例如，通过构成 a 种 (a 为 2 以上的整数)F 函数、执行基于上述三种 Feistel 结构的密码处理、并且满足扩散矩阵切换机构 (DSM) 的处理结构，能够进行抵抗性较高的密码处理。

[0716] 最后统一说明上述的本发明的密码处理以及密码算法构建处理。

[0717] 如参照图 1、图 2 所说明的那样，本发明的密码处理装置具有密码处理部，该密码处理部执行将 SP 型 F 函数反复多次循环的 Feistel 型共用密钥块密码处理，其中，上述 SP 型 F 函数执行包括非线性变换处理和线性变换处理的数据变换处理。并且，如参照图 5 之后的图所说明的那样，密码处理部是执行应用了将数据序列数 :d 设为 d ≥ 2 的整数的扩展 Feistel 结构的密码处理的结构，具有在各循环的 F 函数中执行的线性变换处理中选择性地应用至少两个以上的多个不同的矩阵的结构。

[0718] 设定这些两个以上的多个不同的矩阵使其实现扩散矩阵切换机构 (DSM : Diffusion Switching Mechanism)，通过DSM实现提高对差分攻击、线性攻击的抵抗性的密码处理。为了通过该 DSM 实现提高抵抗性，按照特定的条件进行矩阵的选择、配置。

[0719] 即，作为在 F 函数中执行的线性变换处理所应用的多个矩阵，选择满足条件的多个不同的矩阵，在对扩展 Feistel 结构的各数据序列进行输入的 F 函数中反复配置这些多个不同的矩阵，其中，上述条件为从基于对扩展 Feistel 结构的各数据序列进行输入的 F 函数所包含的线性变换矩阵的与数据序列对应的最小分支数中选择的全部数据序列中的最小分支数为预先决定的值以上。

[0720] 并且，具体地说，在密码处理部中利用的多个不同的矩阵是满足如下条件的多个不同的矩阵 :从根据线性变换矩阵而算出的与数据序列对应的最小分支数 $[B_k^D(s(i))]$ 中选择的全部数据序列中的最小分支数 $[B_k^D]$ 为 3 以上，其中，上述线性变换矩阵包含在对扩展 Feistel 结构的各数据序列 s(i) 进行输入的连续的 k 个 (其中，k 为 2 以上的整数)F 函数中。

[0721] 或者，是满足如下条件的多个不同的矩阵 :从根据线性变换矩阵而算出的与数据序列对应的最小分支数 $[B_2^L(s(i))]$ 中选择的全部数据序列中的最小分支数 $[B_2^L]$ 为 3 以上，其中，上述线性变换矩阵包含在对扩展 Feistel 结构的各数据序列 s(i) 进行输入的连续的两个 F 函数中。

[0722] 本发明的密码处理装置的密码处理部具有如下结构 :在将这些多个不同的矩阵设为 n 个 (其中，n 为 2 以上的整数) 不同的矩阵 M_0、M_1、・・M_{n-1} 时，在对扩展 Feistel 结构的各数据序列进行输入的 F 函数中依次反复配置这些矩阵。作为具体的扩展 Feistel 结构的例子，例如具有参照图 8、图 10 所说明的在一个循环中仅执行一个 F 函数的类型 1 的扩展 Feistel 结构、参照图 9、图 11 所说明的在一个循环中并行地执行多个 F 函数的类型 2 的扩展 Feistel 结构。

[0723] 此外，本发明包括执行应用了这种扩展 Feistel 结构的密码处理的密码处理装置和方法、以及执行密码处理的计算机程序，还包括构建用于执行应用了上述扩展 Feistel 结构的密码处理的密码处理算法的信息处理装置、方法以及计算机程序。

[0724] 构建密码处理算法的信息处理装置例如能够应用一般的 PC 等信息处理装置，具有能够执行以下处理步骤的控制部。即，

[0725] 矩阵决定步骤，在应用了将数据序列数 :d 设为 d ≥ 2 的整数的扩展 Feistel 结构的密码处理算法的结构中，决定在各循环的 F 函数中执行的线性变换处理中应用的至少两个以上的多个不同的矩阵 ;以及

[0726] 矩阵设定步骤，在对扩展 Feistel 结构的各数据序列进行输入的 F 函数中反复配

置在矩阵决定步骤中决定的多个不同的矩阵。

[0727] 上述矩阵决定步骤作为执行如下处理的步骤而被执行：作为两个以上的多个不同的矩阵，将满足从基于线性变换矩阵的与数据序列对应的最小分支数中选择的全部数据序列中的最小分支数为预先决定的值以上的条件的多个不同的矩阵决定为应用矩阵，其中，上述线性变换矩阵包含在对扩展 Feistel 结构的各数据序列进行输入的 F 函数中。

[0728] 在应用了通过这种处理算法设定的扩展 Feistel 结构的密码处理中，实现扩散矩阵切换机构 (DSM：Diffusion SwitchingMechanism)，通过 DSM 实现提高对差分攻击、线性攻击的抵抗性的密码处理。

[0729] [9. 密码处理装置的结构例]

[0730] 最后，在图 20 中示出了作为执行按照上述实施例的密码处理的密码处理装置的 IC 模块 300 的结构例。能够在例如 PC、IC 卡、读写器、其它各种信息处理装置中执行上述处理，图 20 所示的 IC 模块 300 能够构成在这些各种设备中。

[0731] 图 20 所示的 CPU(Central processing Unit：中央处理单元)301 是执行密码处理的开始、结束、数据的发送和接收的控制、各结构部之间的数据传输控制、其它各种程序的处理器。存储器 302 由 ROM(Read-Only-Memory：只读存储器)、RAM(Random Access Memory：随机存取存储器) 等构成，其中，上述 ROM 保存由 CPU 301 所执行的程序、或运算参数等固定数据，上述 RAM 作为在 CPU 301 的处理中执行的程序以及在程序处理中适当变化的参数的保存区域、工作区域而使用。另外，存储器 302 能够作为密码处理所需的密钥数据、在密码处理中应用的变换表 (置换表)、在变换矩阵中应用的数据等的保存区域而使用。此外，数据保存区域优选构成为具有耐短波结构的存储器。

[0732] 密码处理部 303 例如执行按照上述 Feistel 型共用密钥块密码处理算法的密码处理、解密处理。此外，在此示出了将密码处理单元设为单独模块的例子，但是也可以构成为不设置这种独立的密码处理模块，例如将密码处理程序保存在 ROM 中，由 CPU 301 读出 ROM 保存程序来执行。

[0733] 随机数产生器 304 执行在密码处理所需的密钥的生成等中所必需的随机数的产生处理。

[0734] 发送接收部 305 是执行与外部的数据通信的数据通信处理部，例如执行与读写器等 IC 模块之间的数据通信，执行在 IC 模块内生成的密文的输出、或者来自外部读写器等设备的数据输入等。

[0735] 该 IC 模块 300 例如按照上述实施例执行将数据序列数 d 设为 $d \geq 2$ 的整数的扩展 Feistel 型密码处理。按照上述实施例的方式设定不同的线性变换矩阵作为扩展 Feistel 结构中的 F 函数的线性变换矩阵，由此实现扩散矩阵切换机构 (DSM：DiffusionSwitching Mechanism)，能够提高对差分攻击、线性攻击的抵抗性。

[0736] 以上，参照特定的实施例详细说明了本发明。然而，显然在不脱离本发明的要旨的范围内，本领域技术人员可进行该实施例的修改、代用。即，以例示的形式公开了本发明，但不是限定性地解释本发明。为了判断本发明的要旨，应该参考权利要求书的范围一栏。

[0737] 此外，在说明书中说明的一系列处理能够通过硬件、或软件、或两者的复合结构来执行。在通过软件执行处理的情况下，能够将记录了处理顺序的程序安装到嵌入在专用硬件中的计算机内的存储器中来执行、或将程序安装到可执行各种处理的通用计算机中来执

行。

[0738] 例如，可将程序预先记录在作为记录介质的硬盘、ROM(Read Only Memory)中。或者，可将程序暂时或永久性地保存（记录）在软盘、CD-ROM(Compact Disc Read Only Memory：光盘只读存储器)、MO(Magneto optical：磁光）盘、DVD(DigitalVersatile Disc：数字多功能光盘)、磁盘、半导体存储器等可移动记录介质中。可将这种可移动记录介质作为所谓的封装软件进行提供。

[0739] 此外，程序除了从如上所述的可移动记录介质安装到计算机之外，还能够从下载站点无线传送到计算机、或通过称为LAN(Local Area Nerwork：局域网)、因特网的网络而有线传送到计算机，在计算机中接收这样传送来的程序并安装到内置的硬盘等记录介质中。

[0740] 此外，不仅按照记载以时间序列执行，也可以根据执行处理的装置的处理能力或需要来并行或单独地执行说明书中记载的各种处理。另外，在本说明书中系统是多个装置的逻辑集合结构，并不限于各结构的装置在同一壳体内。

[0741] 产业上的可利用性

[0742] 如上所述，根据本发明的一个实施例的结构，在反复多个循环执行具有非线性变换部和线性变换部的SP型F函数的Feistel型共用密钥块密码处理中，在扩展具有两个数据序列的Feistel结构得到的Feistel结构、即具有例如三个、四个等两个以上的任意的数据序列的扩展型Feistel结构中，通过设定应用了多个不同的线性变换矩阵的循环函数部来实现扩散矩阵切换机构(DSM)，能够构建对线性分析、差分分析的抵抗性较高的共用密钥块密码算法以及执行密码处理。

[0743] 根据本发明的一个实施例的结构，在执行应用了将数据序列数：d设为$d \geq 2$的整数的扩展Feistel结构的密码处理的结构中，具有在各循环的F函数中执行的线性变换处理中选择性地应用至少两个以上的多个不同的矩阵的结构，作为两个以上的多个不同的矩阵，设定为满足从基于包含在对扩展Feistel结构的各数据序列进行输入的F函数中的线性变换矩阵的与数据序列对应的最小分支数中选择的全部数据序列中的最小分支数为预先决定的值以上的条件的多个不同的矩阵，由此实现扩散矩阵切换机构(DSM)，能够构建对线性分析、差分分析的抵抗性较高的共用密钥块密码算法以及执行密码处理。

[0744] 并且，根据本发明的一个实施例的结构，执行应用了数据序列数：$d = 2ax$的扩展Feistel结构($x \geq 1$)的密码处理的结构中，设为在一个循环中均等地执行所有种类(a种类）的F函数各x个的结构，因此实现没有设置多余的电路的小型的密码处理装置，其中，所述扩展Feistel结构利用了由多个不同的矩阵执行不同的线性变换处理的$a(a \geq 2)$种F函数。

[0745] 并且，根据本发明的一个实施例的结构，构成由多个不同的矩阵执行不同的线性变换处理的多个F函数执行部，设为根据设定来变更多个F函数执行部的利用顺序的结构，由此实现能够选择性地执行(a)、(b1)、(b2)中的任一个的密码处理的密码处理装置，其中，上述(a)、(b1)、(b2)为

[0746] (a)通过设为数据序列数$d = 2$的Feistel结构进行的密码处理、或者

[0747] (b1)是设为数据序列数$d \geq 2$的任意数的扩展Feistel结构，在各循环中仅允许执行一个F函数的密码处理、或者

[0748] (b2) 是设为数据序列数 d ≥ 2 的任意数的扩展 Feistel 结构，在各循环中允许并行执行多个 F 函数的密码处理。

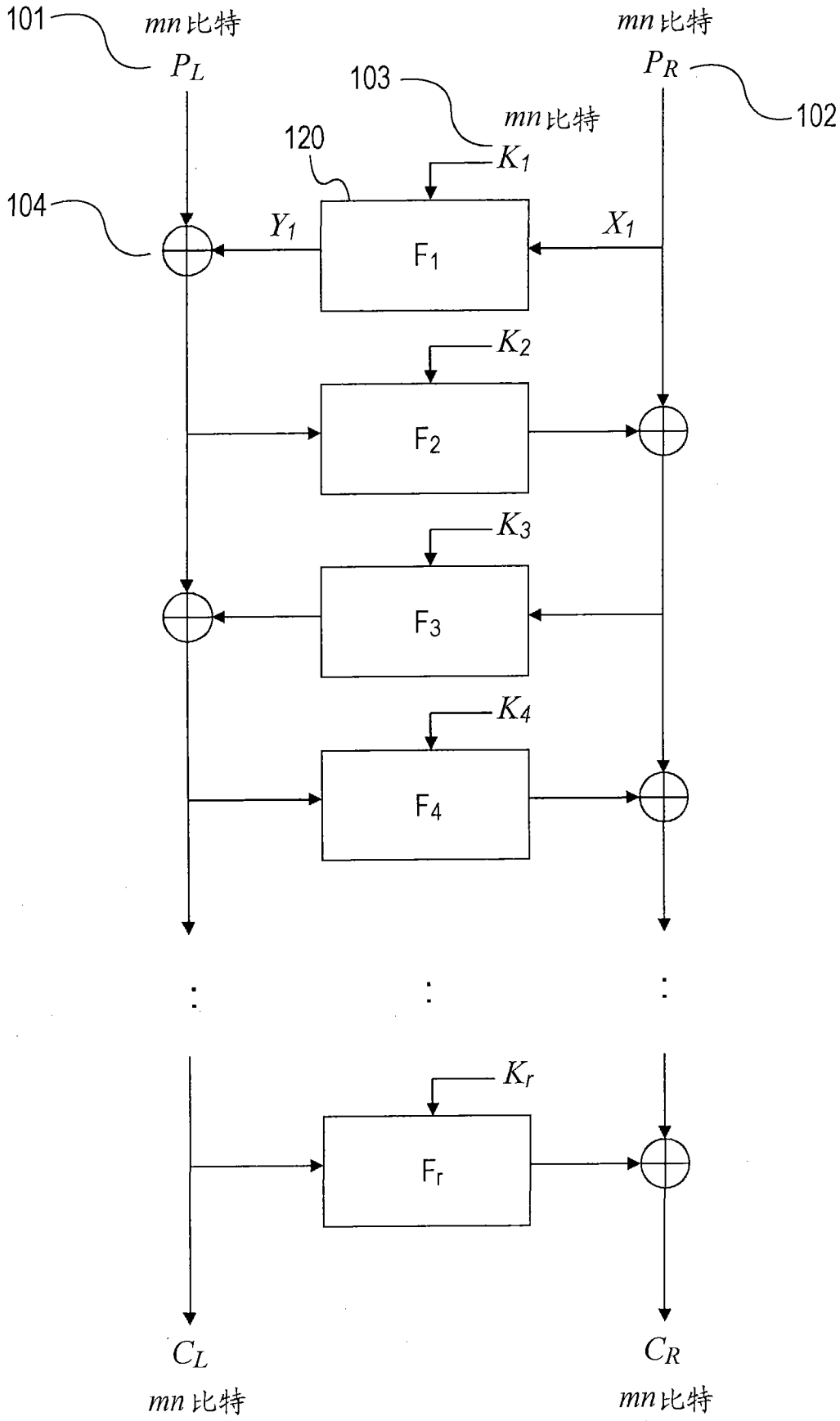

101
mn比特
P_L
103
mn比特
K_1
120
mn比特
P_R
102
104
Y_1
X_1
F_1
K_2
F_2
K_3
F_3
K_4
F_4
K_r
F_r
C_L
mn比特
C_R
mn比特

图 1

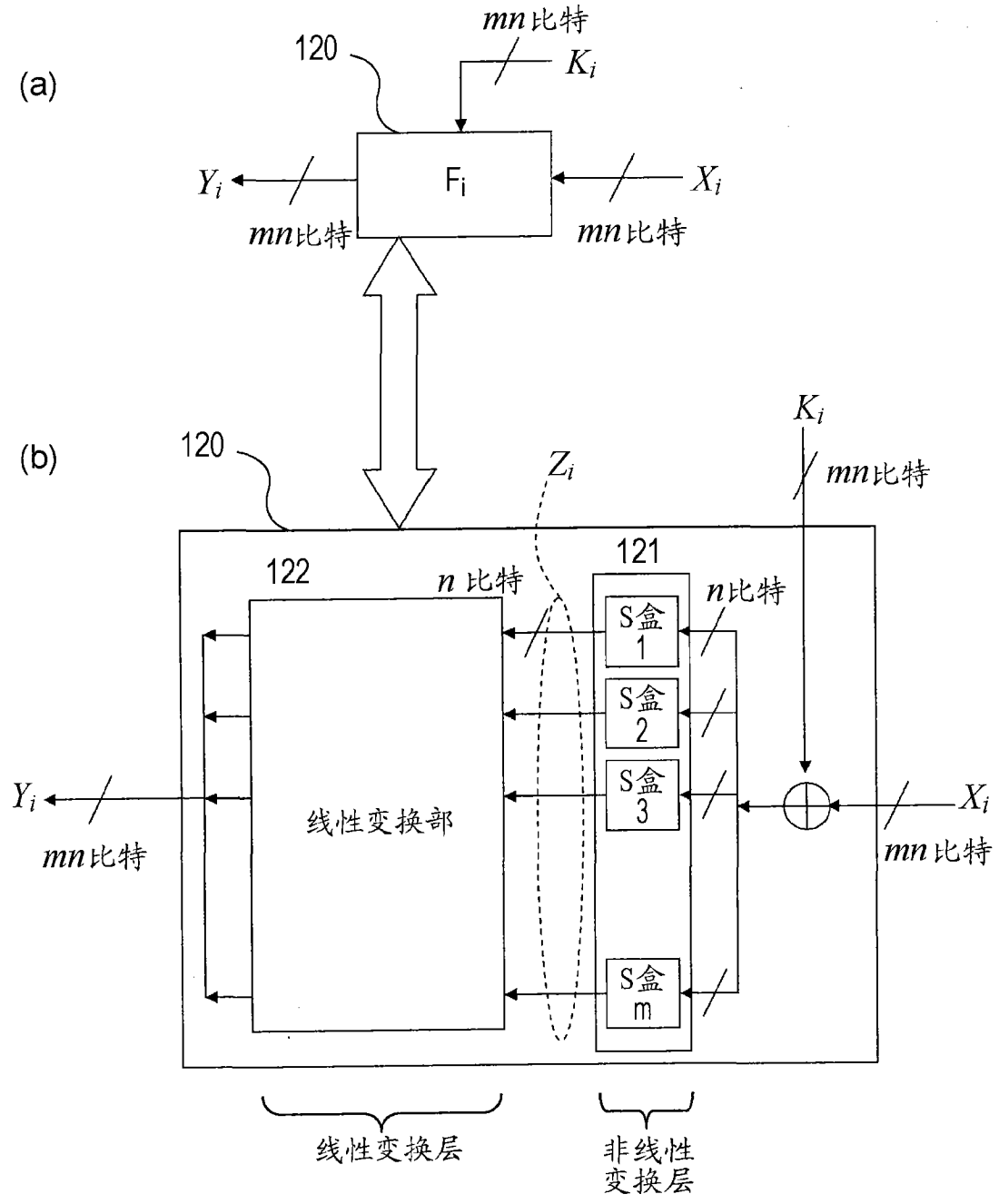

(a)
120
mn比特
K_i
Y_i
Fi
X_i
mn比特
mn比特
(b)
120
Z_i
K_i
mn比特
121
122
n 比特
n比特
S盒 1
S盒 2
S盒 3
S盒 m
Y_i
mn比特
线性变换部
X_i
mn比特
线性变换层
非线性 变换层

图 2

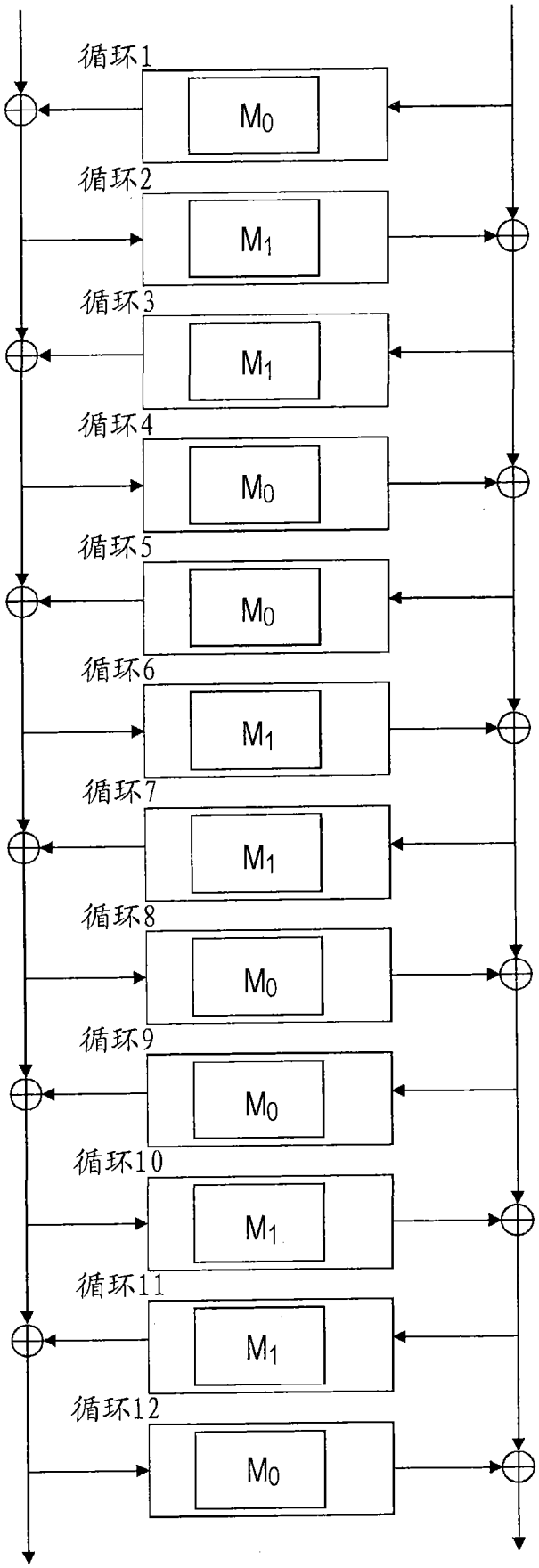

循环1
M0
循环2
M1
循环3
M1
循环4
M0
循环5
M0
循环6
M1
循环7
M1
循环8
M0
循环9
M0
循环10
M1
循环11
M1
循环12
M0

图 3

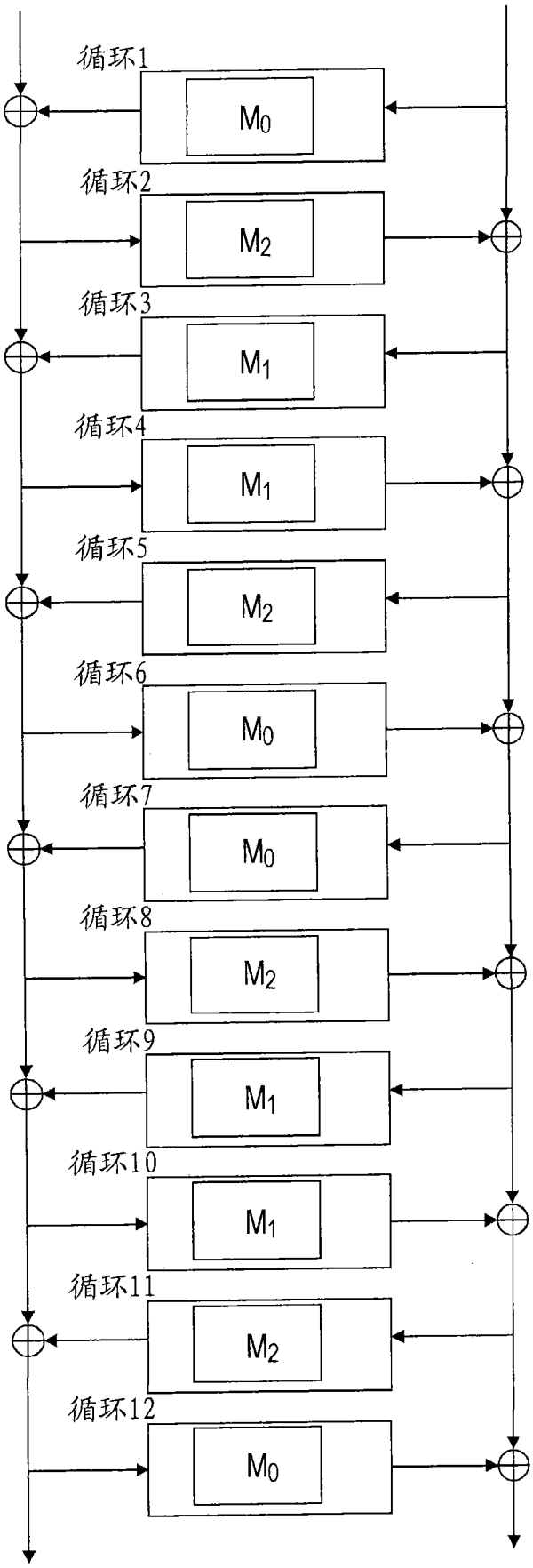

循环1
M0
循环2
M2
循环3
M1
循环4
M1
循环5
M2
循环6
M0
循环7
M0
循环8
M2
循环9
M1
循环10
M1
循环11
M2
循环12
M0

图 4

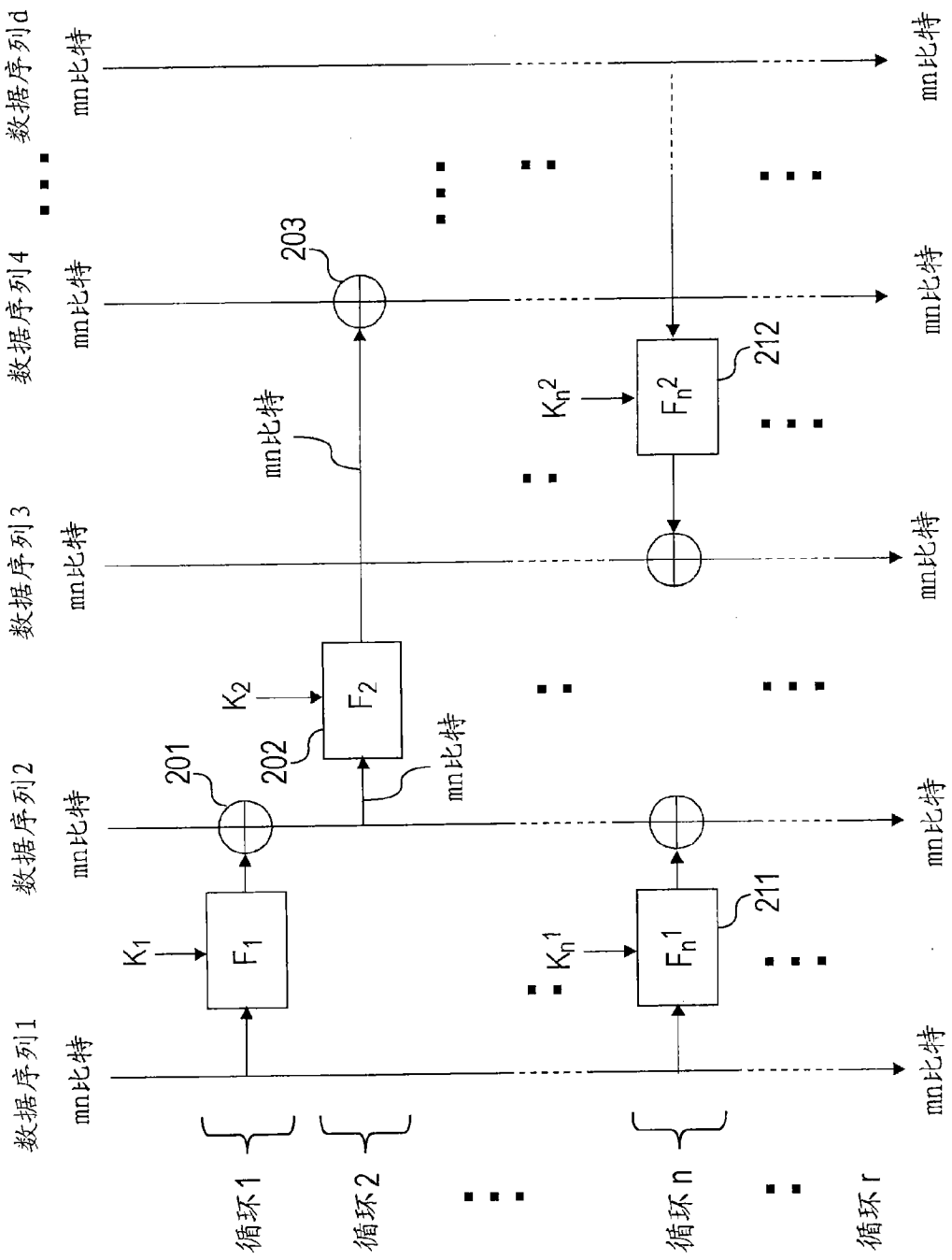

数据序列1
数据序列2
数据序列3
数据序列4
数据序列d
mn比特
K1
F1
K2
F2
Kn1
Fn1
Kn2
Fn2
201
202
203
211
212
循环1
循环2
循环n
循环r

图 5

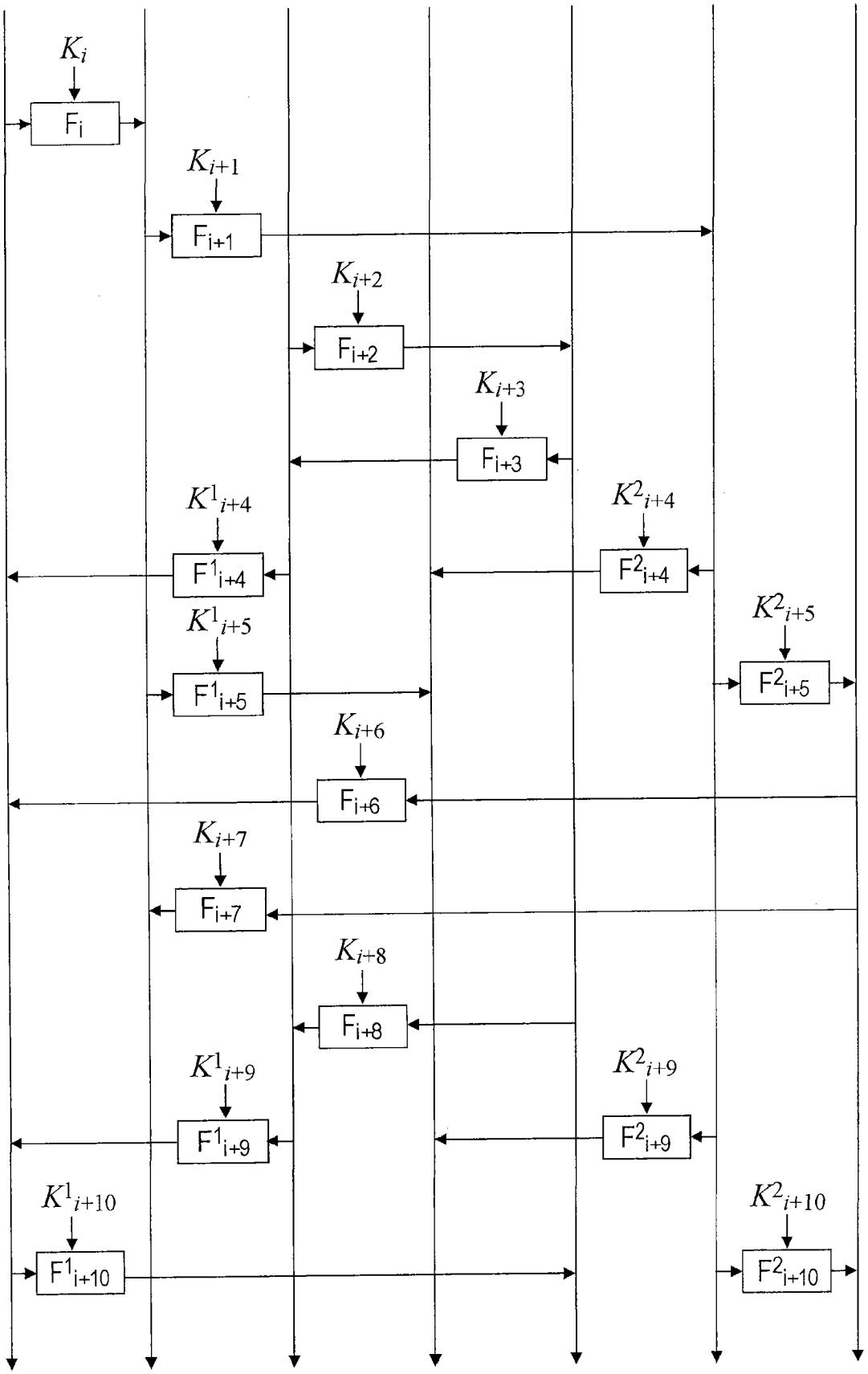

K_i
Fi
K_{i+1}
Fi+1
K_{i+2}
Fi+2
K_{i+3}
Fi+3
K^1_{i+4}
F1i+4
K^2_{i+4}
F2i+4
K^1_{i+5}
F1i+5
K^2_{i+5}
F2i+5
K_{i+6}
Fi+6
K_{i+7}
Fi+7
K_{i+8}
Fi+8
K^1_{i+9}
F1i+9
K^2_{i+9}
F2i+9
K^1_{i+10}
F1i+10
K^2_{i+10}
F2i+10

图 6

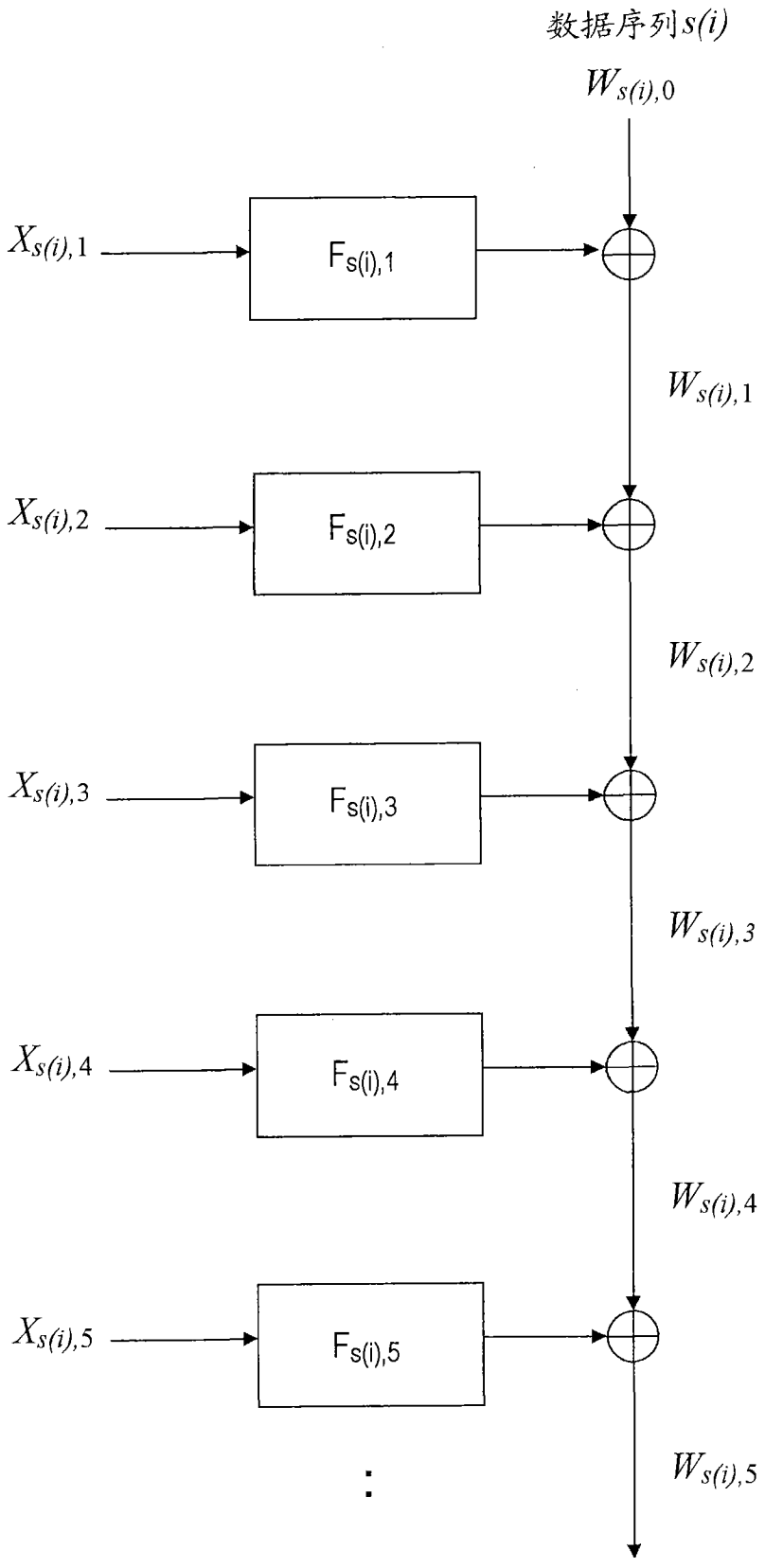

数据序列s(i)
$W_{s(i),0}$
$X_{s(i),1}$
Fs(i),1
$W_{s(i),1}$
$X_{s(i),2}$
Fs(i),2
$W_{s(i),2}$
$X_{s(i),3}$
Fs(i),3
$W_{s(i),3}$
$X_{s(i),4}$
Fs(i),4
$W_{s(i),4}$
$X_{s(i),5}$
Fs(i),5
$W_{s(i),5}$

图 7

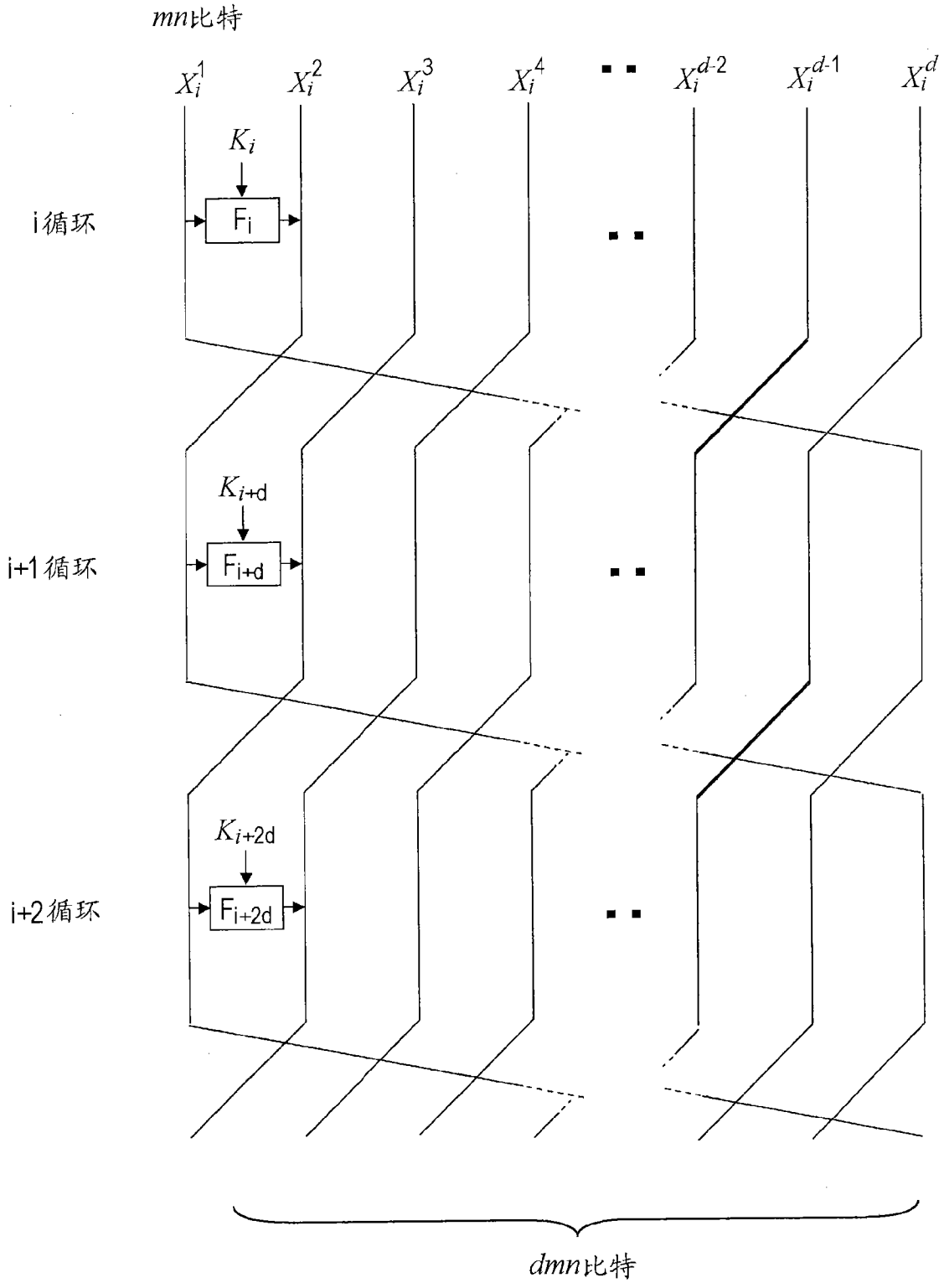

mn比特
X_i^1
X_i^2
X_i^3
X_i^4
X_i^{d-2}
X_i^{d-1}
X_i^d
K_i
Fi
i循环
K_{i+d}
Fi+d
i+1循环
K_{i+2d}
Fi+2d
i+2循环
dmn比特

图 8

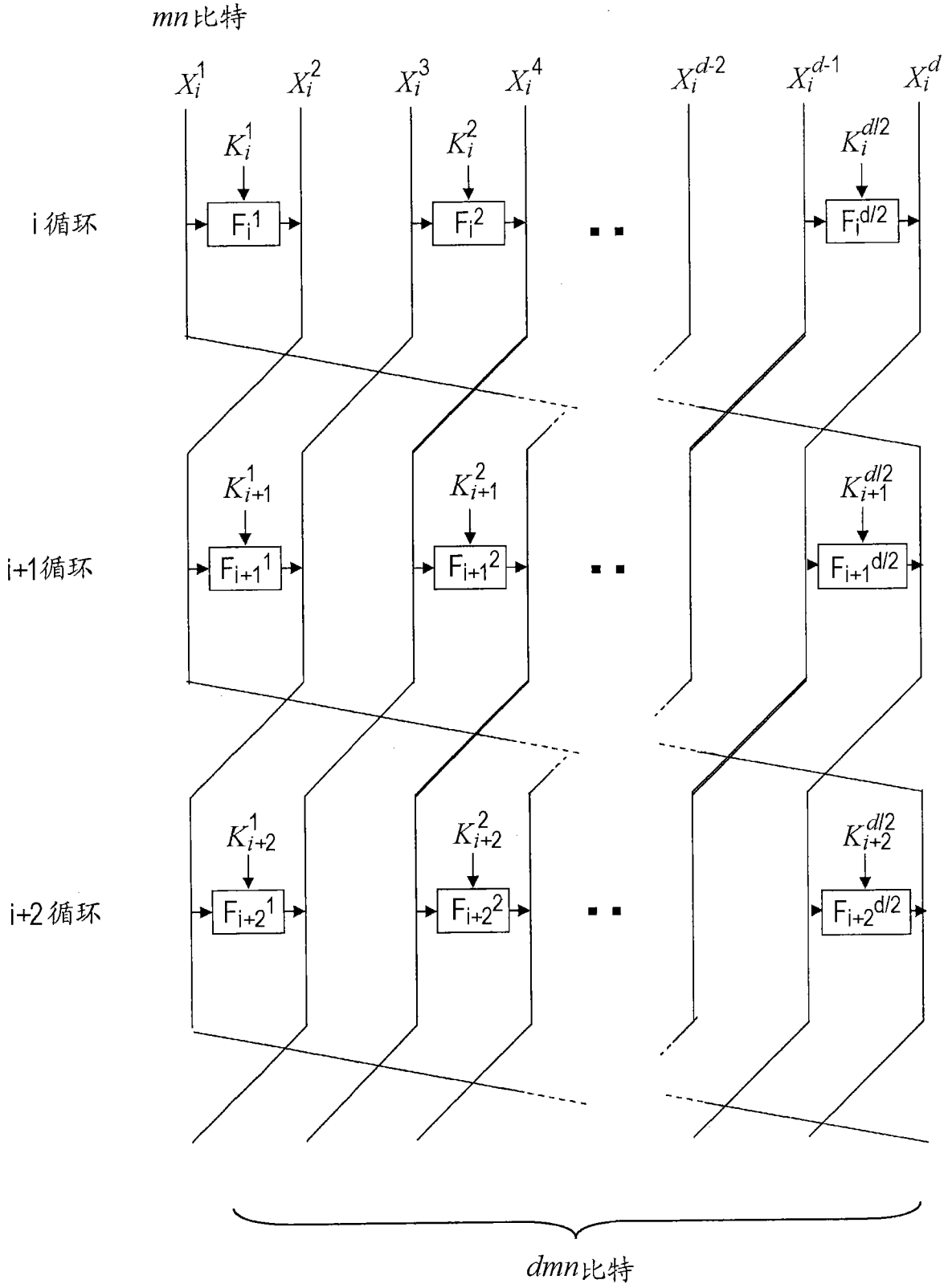

mn比特
X_i^1
X_i^2
X_i^3
X_i^4
X_i^{d-2}
X_i^{d-1}
X_i^d
K_i^1
K_i^2
$K_i^{d/2}$
i 循环
F_i^1
F_i^2
$F_i^{d/2}$
K_{i+1}^1
K_{i+1}^2
$K_{i+1}^{d/2}$
i+1循环
F_{i+1}^1
F_{i+1}^2
$F_{i+1}^{d/2}$
K_{i+2}^1
K_{i+2}^2
$K_{i+2}^{d/2}$
i+2 循环
F_{i+2}^1
F_{i+2}^2
$F_{i+2}^{d/2}$
dmn比特

图 9

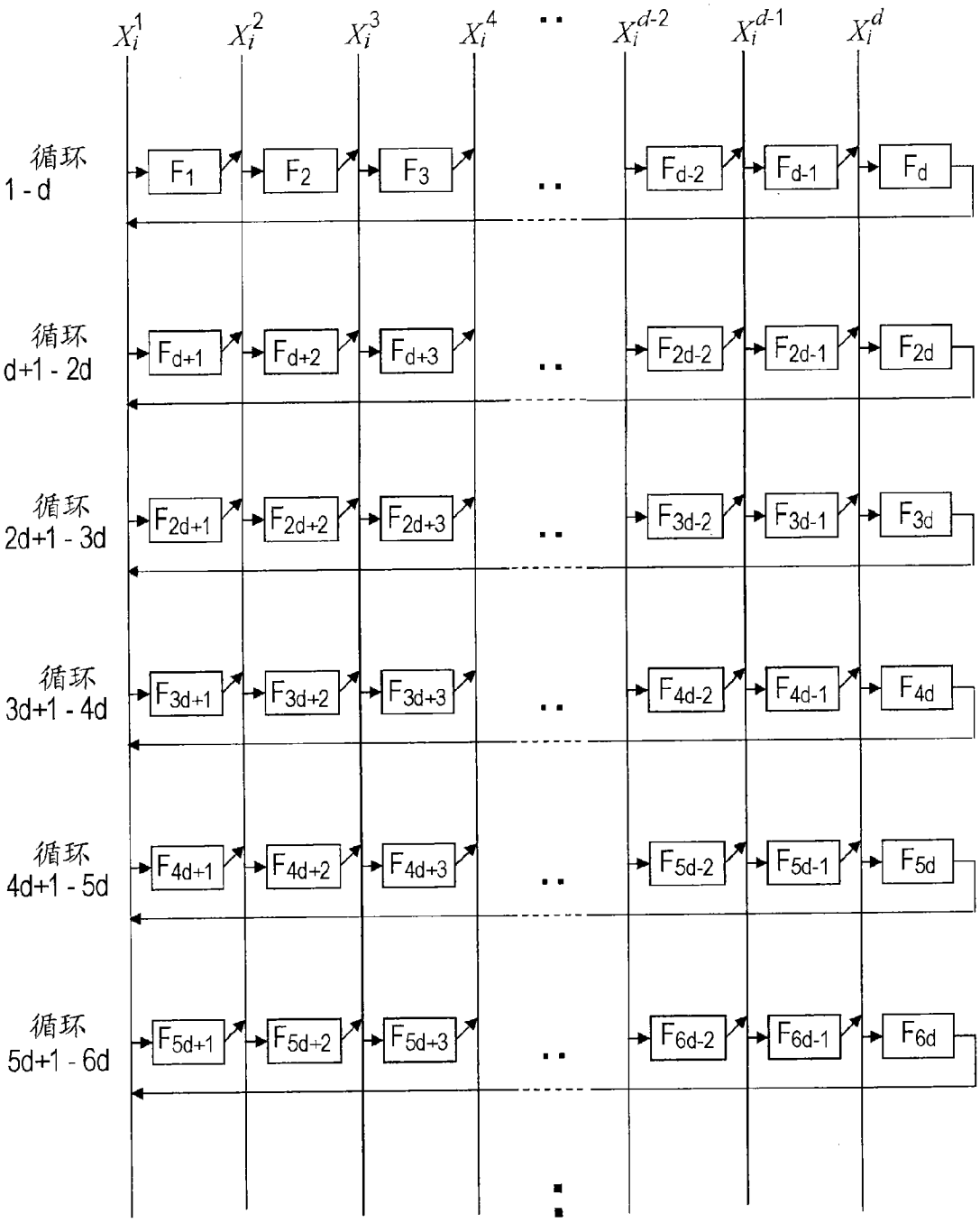

X_i^1
X_i^2
X_i^3
X_i^4
X_i^{d-2}
X_i^{d-1}
X_i^d
循环 1 - d
F1
F2
F3
Fd-2
Fd-1
Fd
循环 d+1 - 2d
Fd+1
Fd+2
Fd+3
F2d-2
F2d-1
F2d
循环 2d+1 - 3d
F2d+1
F2d+2
F2d+3
F3d-2
F3d-1
F3d
循环 3d+1 - 4d
F3d+1
F3d+2
F3d+3
F4d-2
F4d-1
F4d
循环 4d+1 - 5d
F4d+1
F4d+2
F4d+3
F5d-2
F5d-1
F5d
循环 5d+1 - 6d
F5d+1
F5d+2
F5d+3
F6d-2
F6d-1
F6d

图 10

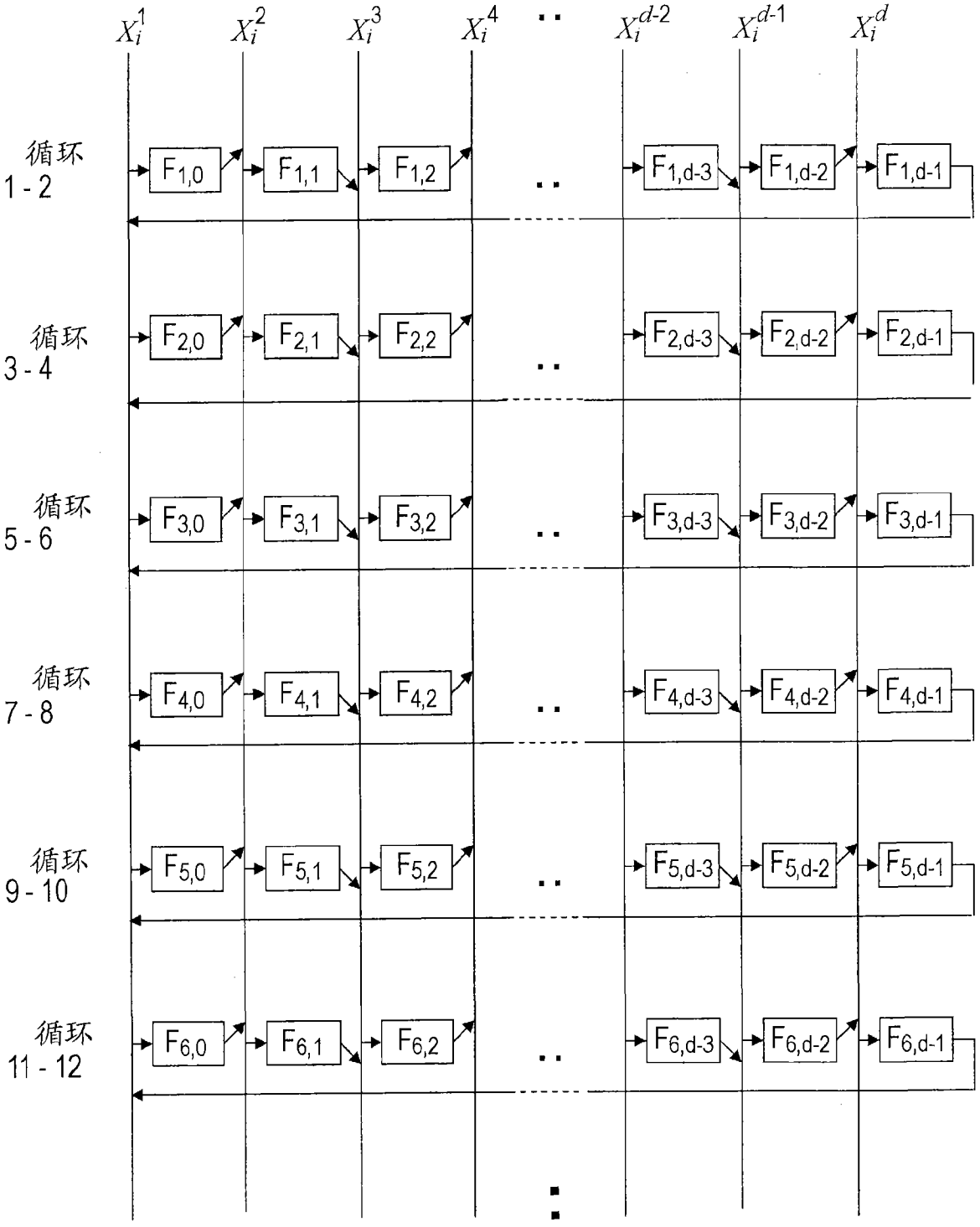

X_i^1
X_i^2
X_i^3
X_i^4
X_i^{d-2}
X_i^{d-1}
X_i^d
循环 1 - 2
循环 3 - 4
循环 5 - 6
循环 7 - 8
循环 9 - 10
循环 11 - 12
F1,0
F1,1
F1,2
F1,d-3
F1,d-2
F1,d-1
F2,0
F2,1
F2,2
F2,d-3
F2,d-2
F2,d-1
F3,0
F3,1
F3,2
F3,d-3
F3,d-2
F3,d-1
F4,0
F4,1
F4,2
F4,d-3
F4,d-2
F4,d-1
F5,0
F5,1
F5,2
F5,d-3
F5,d-2
F5,d-1
F6,0
F6,1
F6,2
F6,d-3
F6,d-2
F6,d-1

图 11

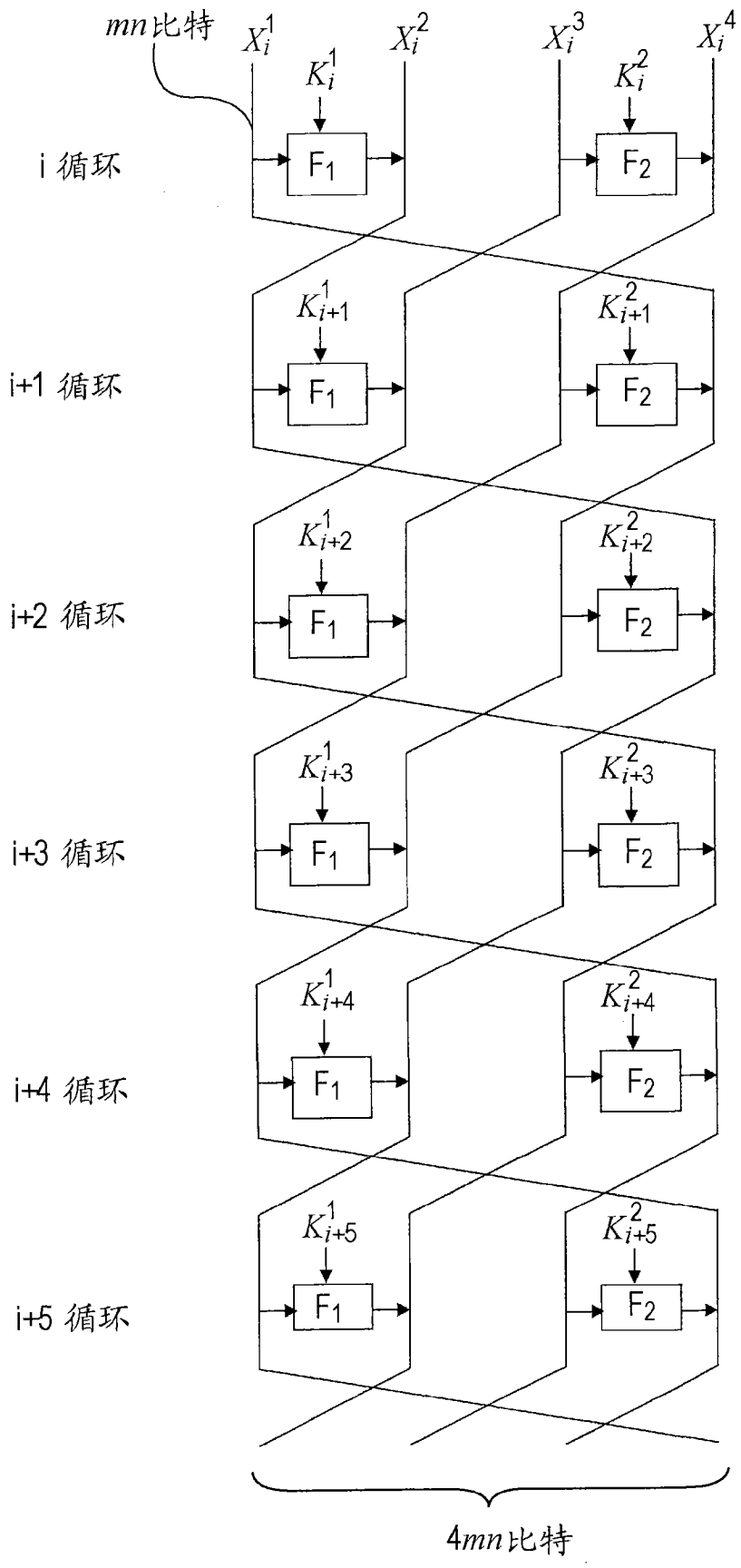

mn比特
X_i^1
X_i^2
X_i^3
X_i^4
K_i^1
K_i^2
F1
F2
i 循环
K_{i+1}^1
K_{i+1}^2
i+1 循环
K_{i+2}^1
K_{i+2}^2
i+2 循环
K_{i+3}^1
K_{i+3}^2
i+3 循环
K_{i+4}^1
K_{i+4}^2
i+4 循环
K_{i+5}^1
K_{i+5}^2
i+5 循环
4mn比特

图 12

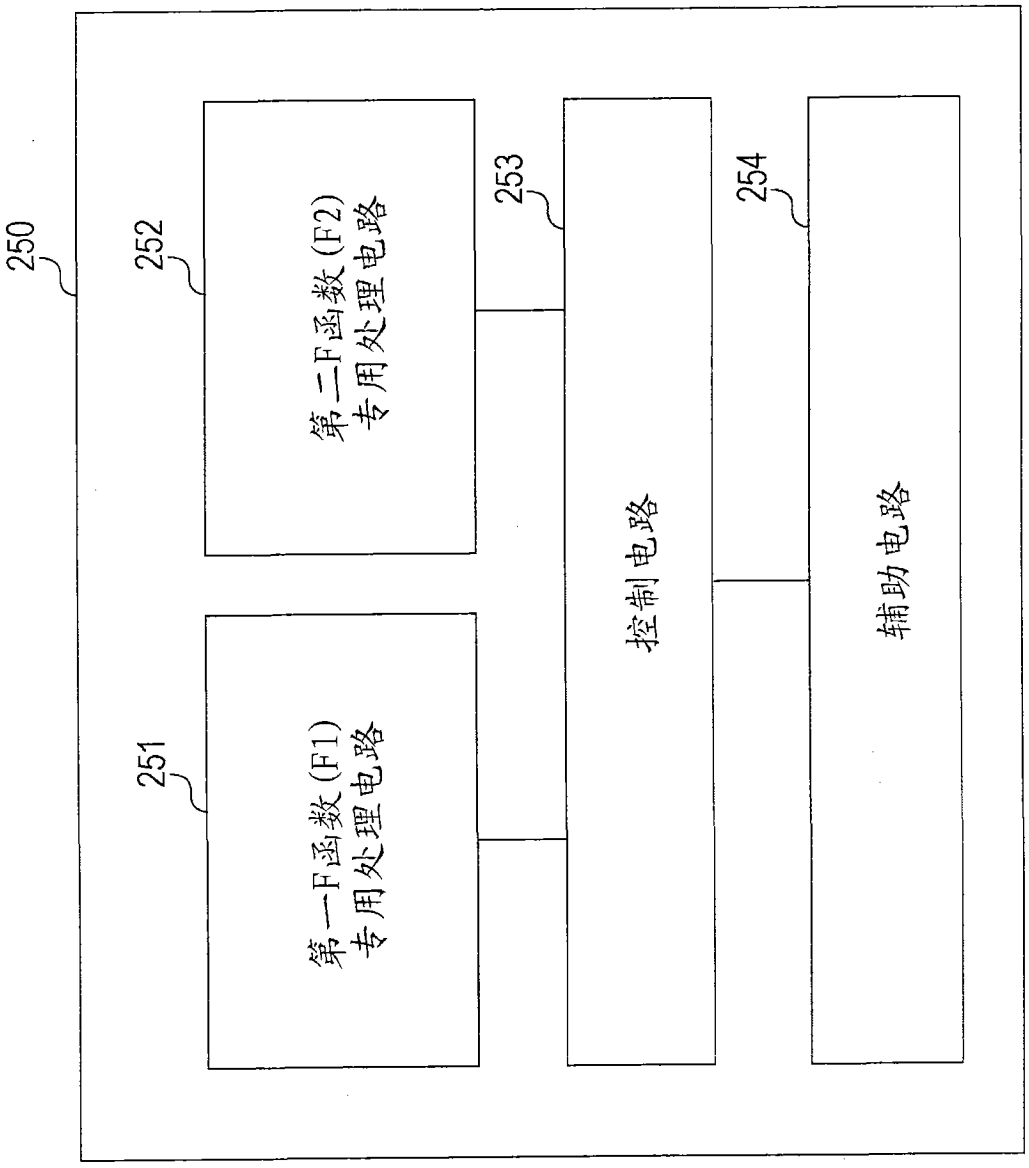


图 13

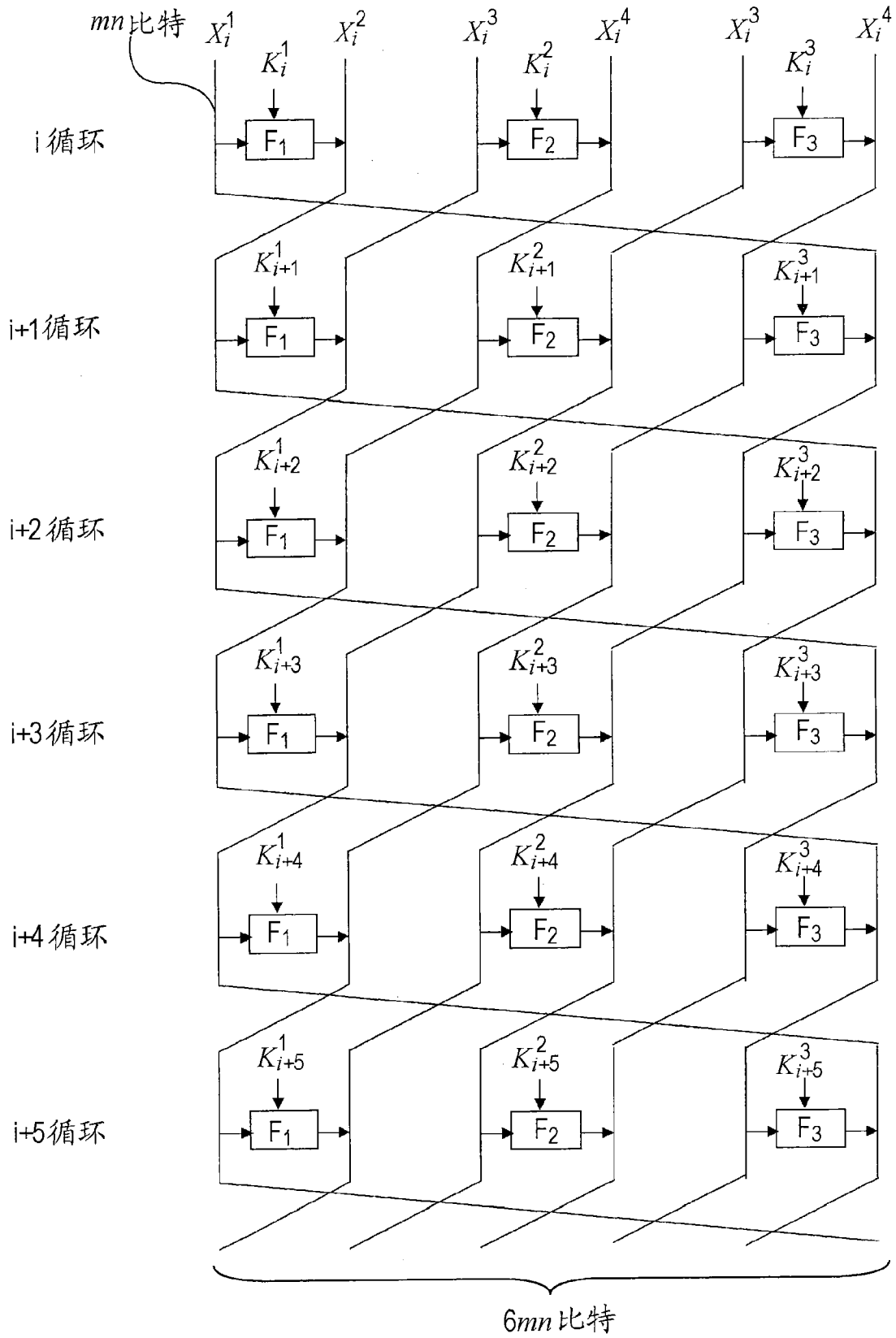

mn比特
X_i^1
X_i^2
X_i^3
X_i^4
X_i^3
X_i^4
K_i^1
K_i^2
K_i^3
i循环
i+1循环
i+2循环
i+3循环
i+4循环
i+5循环
K_{i+1}^1
K_{i+1}^2
K_{i+1}^3
K_{i+2}^1
K_{i+2}^2
K_{i+2}^3
K_{i+3}^1
K_{i+3}^2
K_{i+3}^3
K_{i+4}^1
K_{i+4}^2
K_{i+4}^3
K_{i+5}^1
K_{i+5}^2
K_{i+5}^3
F1
F2
F3
6mn比特

图 14

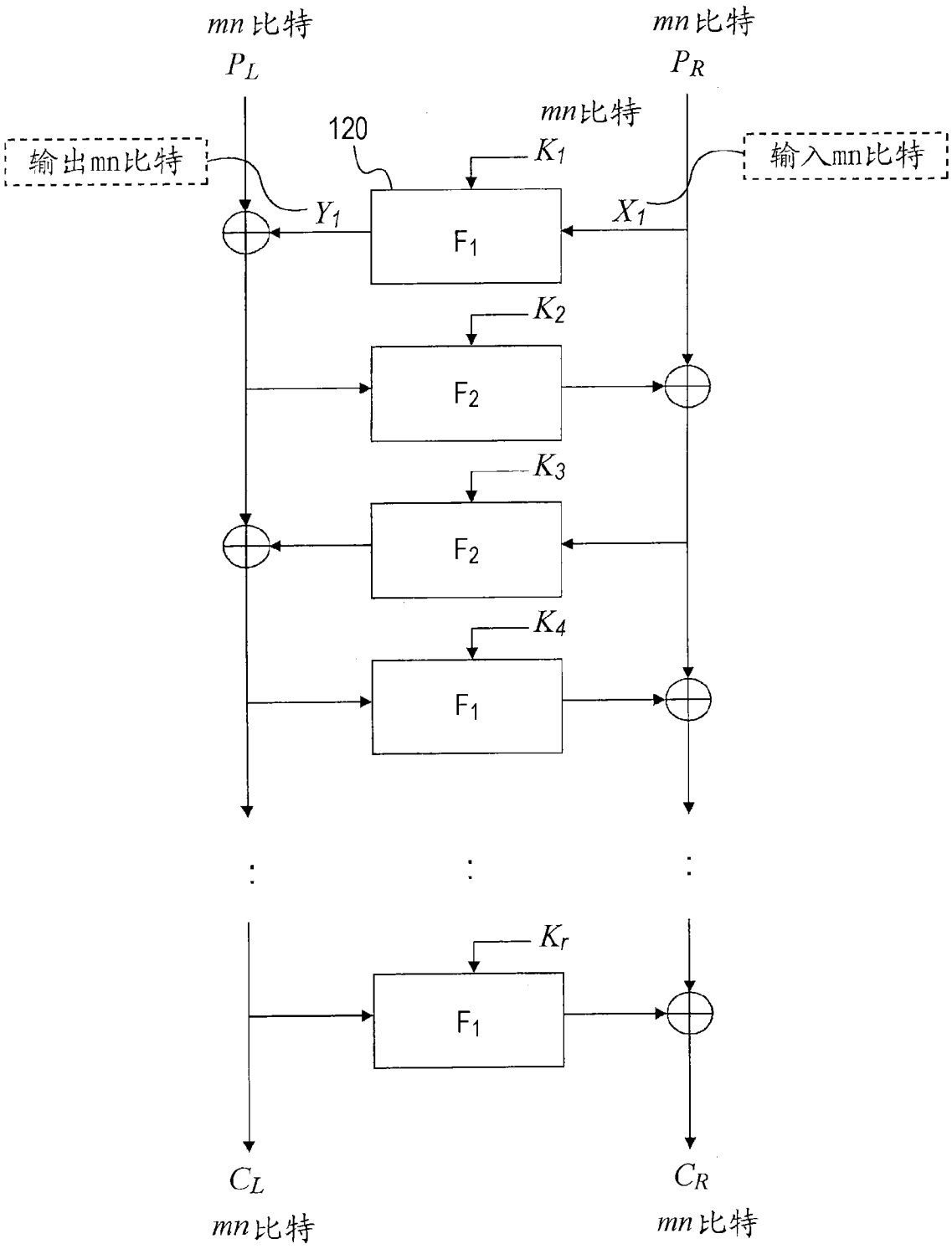

mn比特
P_L
mn比特
P_R
120
mn比特
K_1
输出mn比特
输入mn比特
Y_1
X_1
F_1
K_2
F_2
K_3
F_2
K_4
F_1
K_r
F_1
C_L
mn比特
C_R
mn比特

图 15

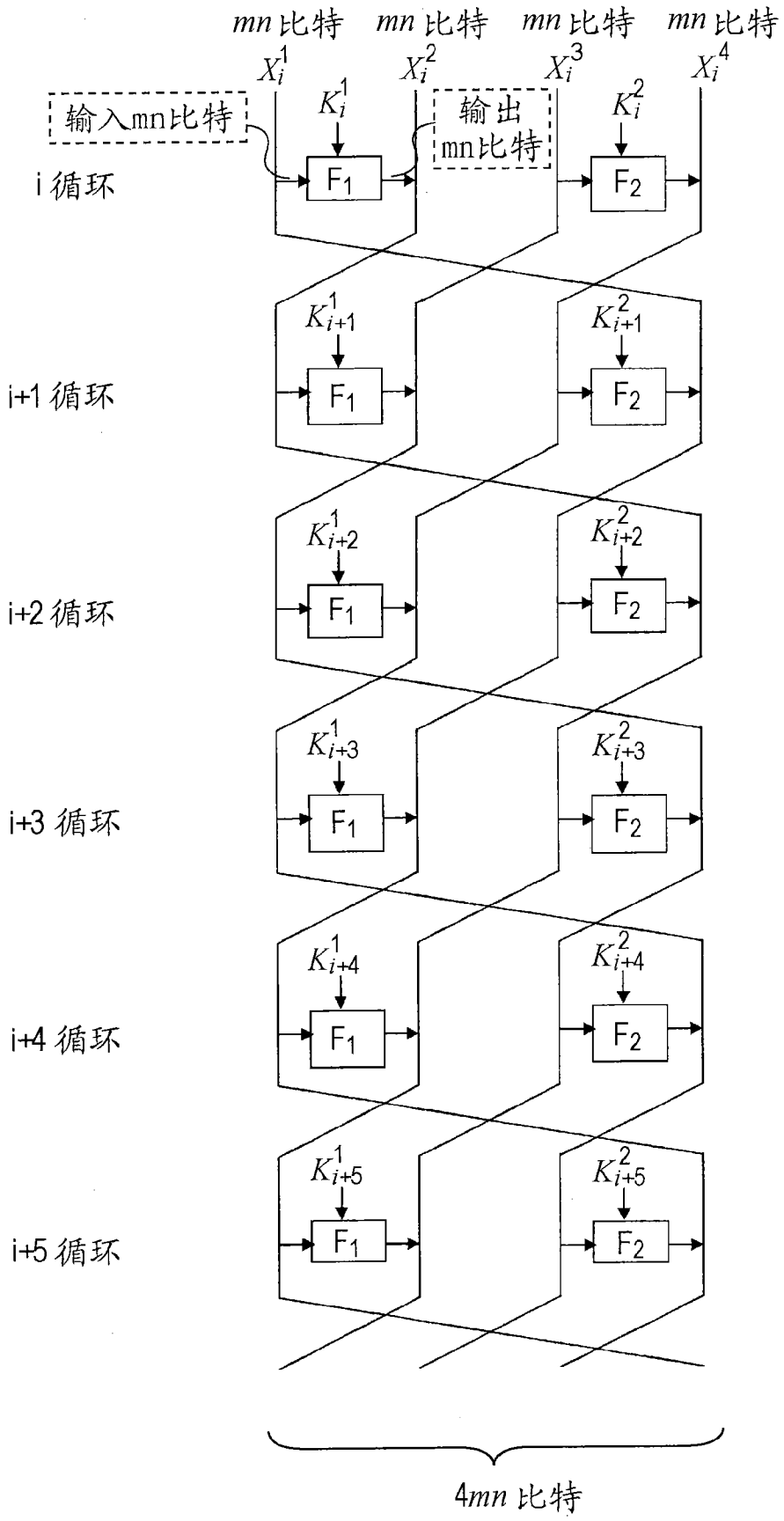

mn 比特
mn 比特
mn 比特
mn 比特
X_i^1
X_i^2
X_i^3
X_i^4
输入mn比特
输出
mn比特
K_i^1
K_i^2
F1
F2
i 循环
K_{i+1}^1
K_{i+1}^2
i+1 循环
K_{i+2}^1
K_{i+2}^2
i+2 循环
K_{i+3}^1
K_{i+3}^2
i+3 循环
K_{i+4}^1
K_{i+4}^2
i+4 循环
K_{i+5}^1
K_{i+5}^2
i+5 循环
4mn 比特

图 16

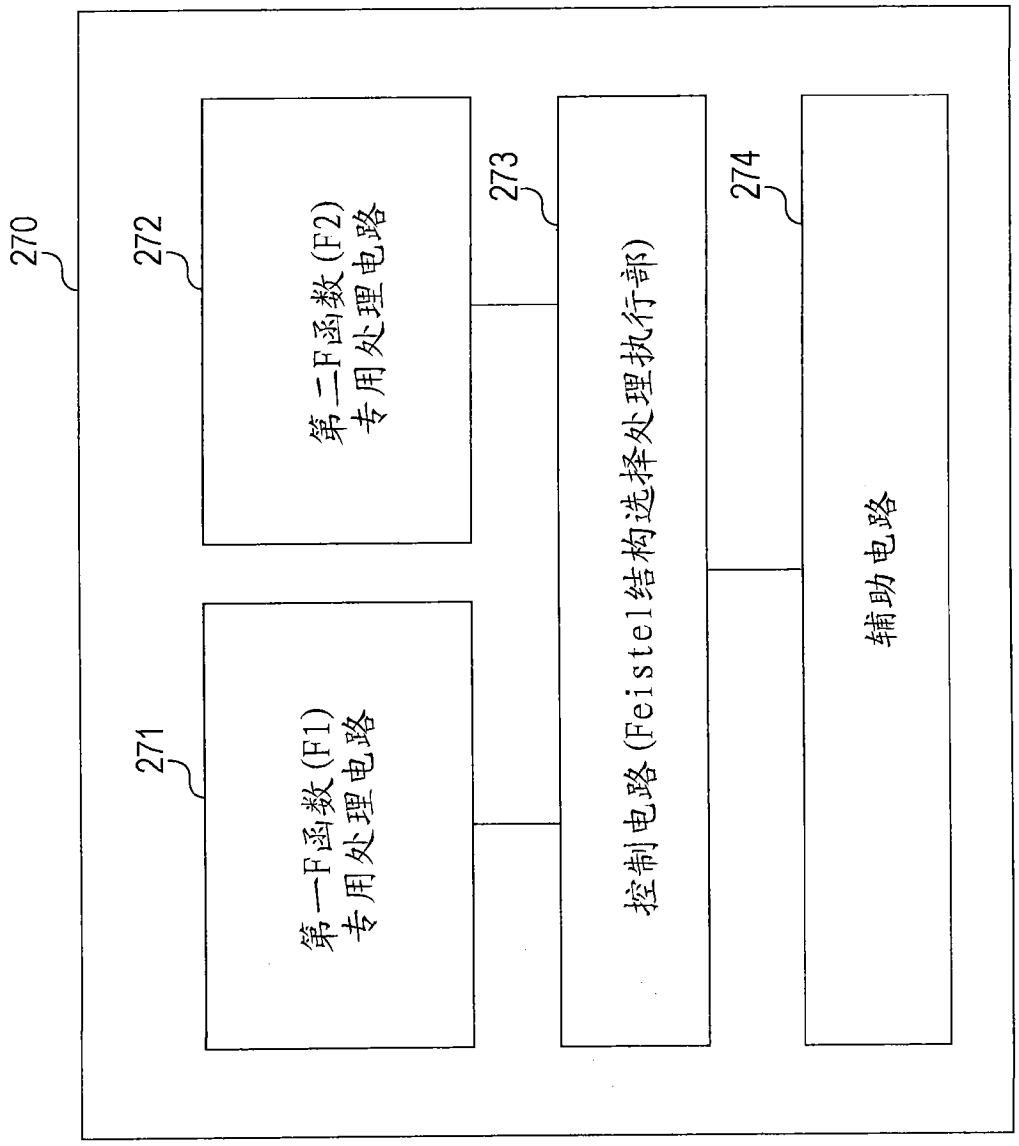

270
271
第一F函数(F1)
专用处理电路
272
第二F函数(F2)
专用处理电路
273
控制电路(Feistel结构选择处理执行部)
274
辅助电路

图 17

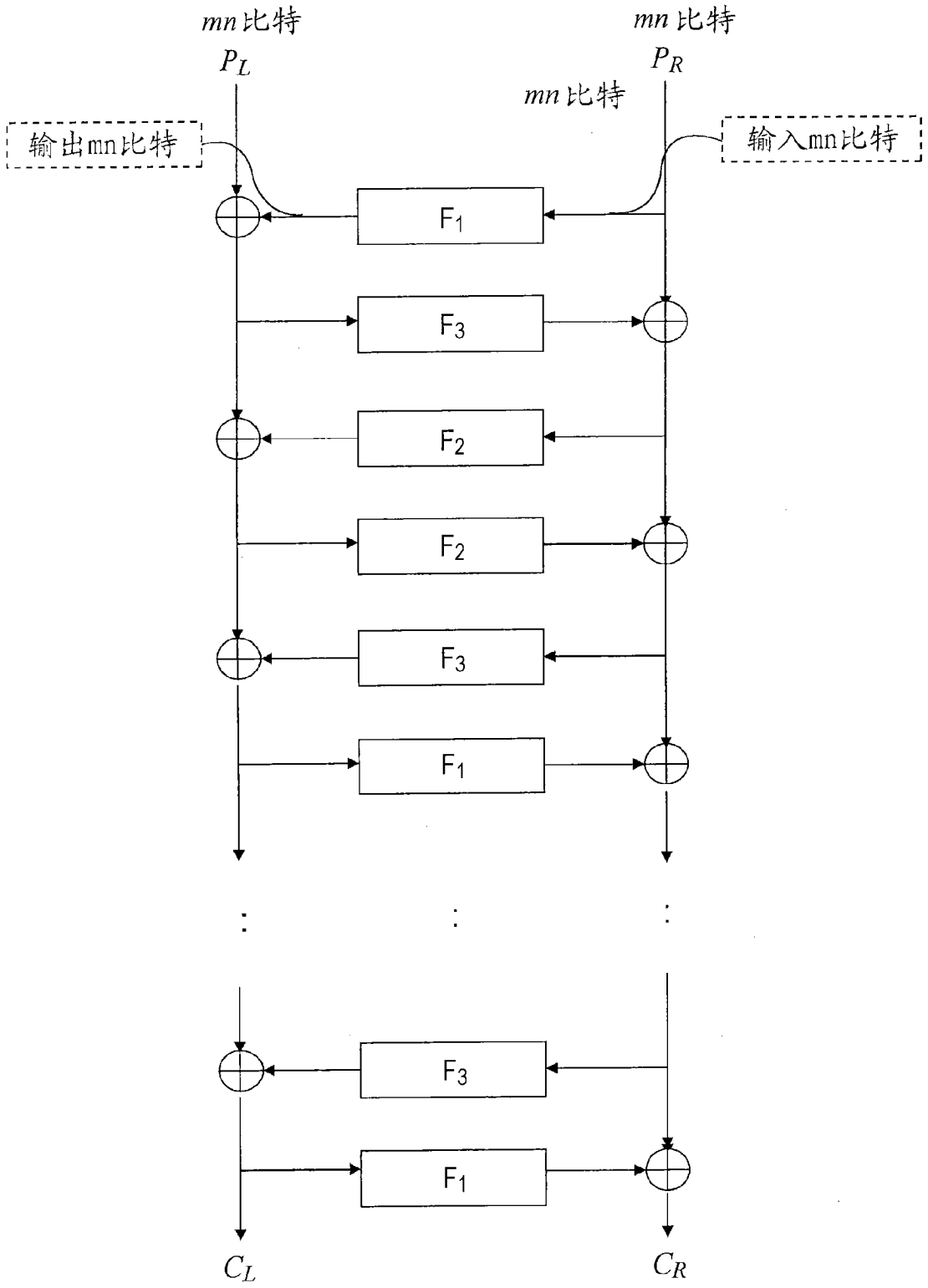


图 18

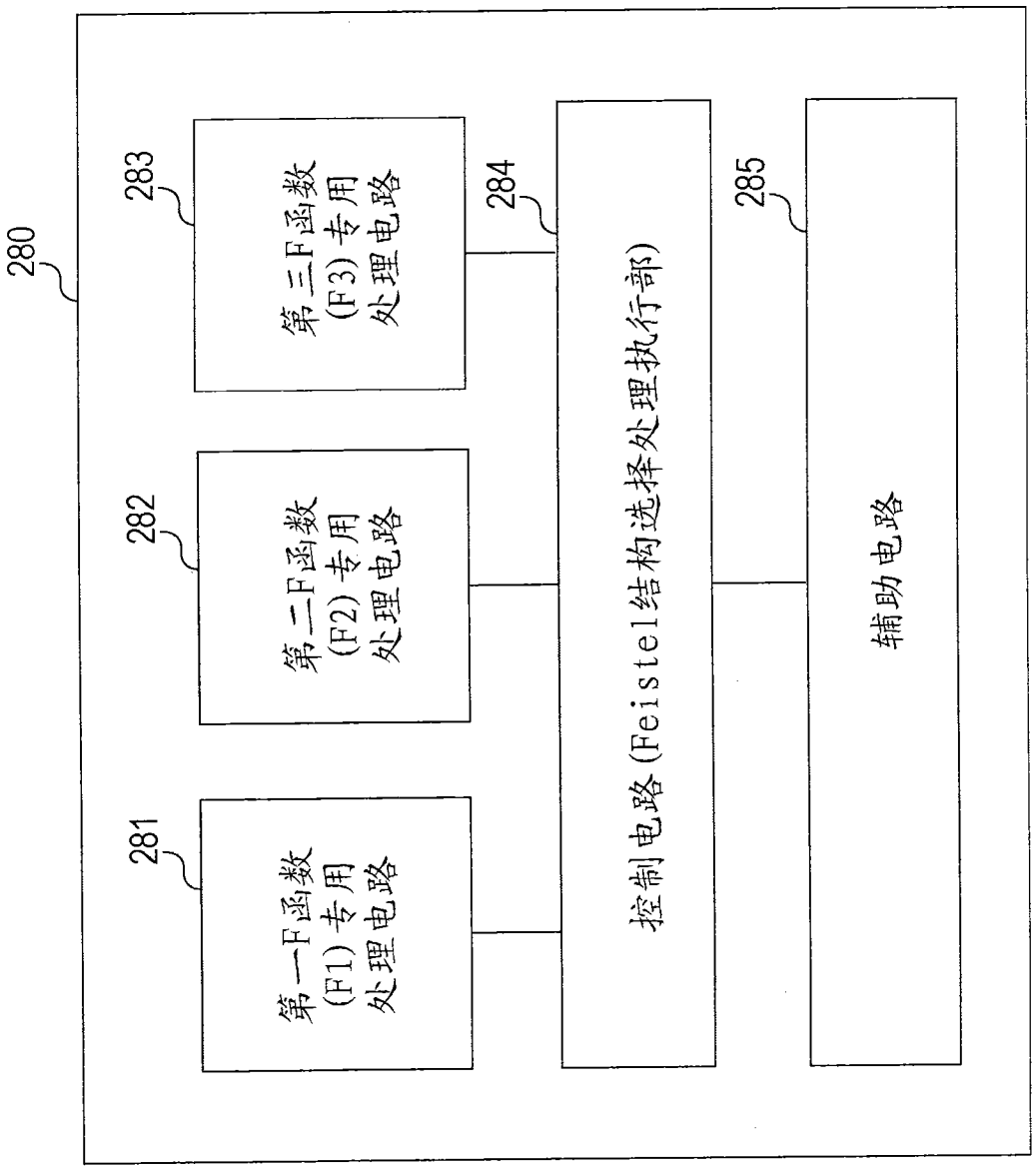

280
281
第一F函数
(F1)专用
处理电路
282
第二F函数
(F2)专用
处理电路
283
第三F函数
(F3)专用
处理电路
284
控制电路(Feistel结构选择处理执行部)
285
辅助电路

图 19

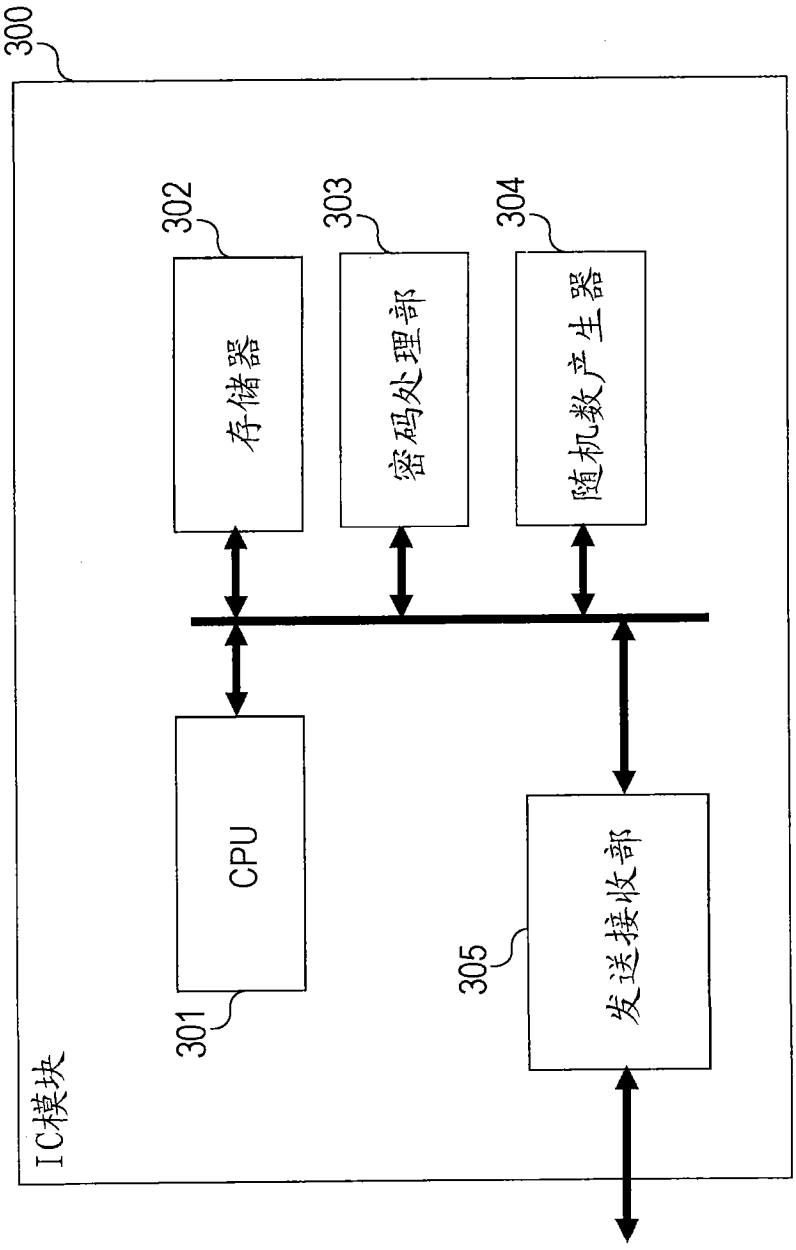


图 20