(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 102594546 B
(45)授权公告日 2015.04.22

(21)申请号 201210050602.9
(22)申请日 2007.08.29
(30)优先权数据
2006-238227 2006.09.01 JP
(62)分案原申请数据
200780032104.9 2007.08.29
(73)专利权人 索尼株式会社
地址 日本东京都
(72)发明人 涩谷香士 白井太三 秋下彻
盛合志帆
(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)

审查员 刘莉

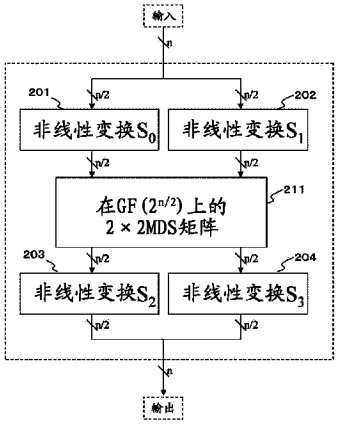
权利要求书2页 说明书19页 附图19页

(54)发明名称

信息处理装置

(57)摘要

实现安装效率以及安全性较高的非线性变换处理结构。执行应用了第一级非线性变换部、线性变换部以及第二级非线性变换部的数据变换，其中，上述第一级非线性变换部利用多个较小的S盒(S-box)执行非线性变换，上述线性变换部输入来自第一级非线性变换部的所有输出并执行应用了进行最优扩散变换的矩阵的数据变换，上述第二级非线性变换部由执行分割线性变换部的输出数据得到的各分割数据的非线性变换处理的多个小型非线性变换部构成。通过本结构，能够不使关键路径过大而实现适当的数据扩散，实现安装效率以及安全性较高的结构。



CN 102594546 B

1. 一种信息处理装置，其具备：

存储器，其保存在密码处理中使用的密钥；

处理器，其执行程序；以及

密码处理部，其执行将 F 函数反复执行多个循环的扩展 Feistel 型共用密钥块密码处理，

其中，该密码处理部具有：

第一数据分割部，其对明文数据进行分割，并调整 F 函数的各循环的循环密钥的比特数使其与通过明文数据的分割得到的比特数相同；

密钥异或运算部，其对由上述第一数据分割部分割得到的数据执行与上述循环密钥异或的密钥异或运算；

第二数据分割部，其对由上述密钥异或运算部进行密钥异或运算得到的数据进一步进行分割；

第一级非线性变换部，其由执行由上述第二数据分割部分割得到的各个数据的非线性变换处理的多个小型非线性变换部构成；

线性变换部，其被输入来自构成上述第一级非线性变换部的小型非线性变换部的所有输出并执行线性变换；

第三数据分割部，其对上述线性变换部的输出数据进行分割；以及

第二级非线性变换部，其由在上述线性变换之后紧接着执行由上述第三数据分割部分割得到的各个数据的非线性变换处理的多个小型非线性变换部构成。

2. 根据权利要求 1 所述的信息处理装置，其特征在于，

上述线性变换部是如下结构：利用具有与由上述第二数据分割部进行分割而得到的数据的比特大小相同大小的要素的矩阵运算来执行数据变换，在矩阵是 m×m 矩阵的情况下，执行应用了具有至少 m 以上的分支数的高分支数的矩阵的数据变换处理。

3. 根据权利要求 1 所述的信息处理装置，其特征在于，

在上述输入数据是 n 比特数据的情况下，

上述第一级非线性变换部由 k 个小型非线性变换部构成，其中，上述 k 个小型非线性变换部分别输入作为输入数据的 n 比特数据的分割数据即 n/k 比特并输出作为非线性变换处理结果的 n/k 比特，

上述线性变换部是如下结构：输入由上述 k 个小型非线性变换部所输出的总计 n 比特的数据，通过应用了高分支数的矩阵的数据变换处理来生成 n 比特的输出，

上述第二级非线性变换部是具有 k 个小型非线性变换部的结构，其中，上述 k 个小型非线性变换部分别输入从上述线性变换部输出的 n 比特数据的分割数据即 n/k 比特并输出作为非线性变换处理结果的 n/k 比特。

4. 根据权利要求 1 所述的信息处理装置，其特征在于，

上述线性变换部是执行应用了最大距离可分 MDS(Maximum Distance Separable) 矩阵的数据变换处理的结构，其中，上述最大距离可分 MDS 矩阵执行最优扩散变换 ODM(Optimal Diffusion Mappings) 处理。

5. 根据权利要求 1 所述的信息处理装置，其特征在于，

在上述输入数据是 n 比特数据的情况下，上述线性变换部是执行应用了由在 GF(2) 上

定义的 n 次既约多项式 p(x) 定义的扩展域 GF(2^n) 上的矩阵的数据变换处理的结构。

6. 根据权利要求 1 所述的信息处理装置，其特征在于，

上述信息处理装置是执行 n 比特输入输出的非线性变换处理的 S 盒，

包含在上述第一级非线性变换部和上述第二级非线性变换部中的多个小型非线性变换部由执行比特数少于 n 比特的非线性变换处理的小型 S 盒构成。

7. 根据权利要求 1 所述的信息处理装置，其特征在于，

代替上述明文数据，上述第一数据分割部对密文数据进行分割，并且上述密码处理部反复执行 F 函数的多个循环时应用应用顺序与权利要求 1 的循环密钥的应用顺序相反的循环密钥，由此来进行上述密文数据的解密。

信息处理装置

[0001] 本申请是申请日为 2007 年 8 月 29 日、申请号为 PCT/JP2007/066732 的国际申请进入中国国家知识产权局的国家阶段（国家申请号为 200780032104.9）、发明名称为“数据变换装置和数据变换方法、以及计算机程序”的申请的分案申请。

技术领域

[0002] 本发明涉及一种数据变换装置和数据变换方法、以及计算机程序。更详细地说，例如涉及一种进行能够应用于共用密钥块密码处理、哈希 (hash) 函数等中的非线性变换处理的数据变换装置和数据变换方法、以及计算机程序。

背景技术

[0003] 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。

[0004] 例如实际应用了如下系统：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。

[0005] 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。

[0006] 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性的方式是共用密钥块密码方式。

[0007] 作为代表性的共用密钥块密码的算法，例如已知有过去作为美国标准密码的 DES(Data Encryption Standard：数据加密标准）算法、当前的作为美国标准密码的 AES(Advanced Encryption Standard：高级加密标准）算法等。

[0008] 这种共用密钥块密码的算法主要由密码处理部和密钥调度部构成，其中，上述密码处理部具有反复执行输入数据的变换的循环函数执行部，上述密钥调度部生成在循环函数部的各循环中应用的循环密钥。密钥调度部根据作为私人密钥的主密钥 (master key)，首先生成增加比特数的扩展密钥，根据所生成的扩展密钥生成在密码处理部的各循环函数部中应用的循环密钥（副密钥）。

[0009] 作为执行这种算法的具体结构，已知有反复执行具有线性变换部和非线性变换部的循环函数的结构。例如在代表性的结构中存在 Feistel 结构。Feistel 结构具有如下结构：通过作为数据变换函数的循环函数 (F 函数）的简单的重复，将明文变换为密文。在循环函数 (F 函数）中执行线性变换处理和非线性变换处理。此外，作为记载了应用 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。

[0010] 在该共用密钥块密码处理、例如哈希函数等中利用非线性变换处理执行数据变

换。在非线性变换中能够应用被称为S盒(S-box)的非线性变换函数。S盒是块密码、哈希函数的结构要素,是决定其安全性、安装性能的非常重要的函数。S盒一般为n-bit输入、m-bit输出的非线性变换函数。输入输出比特数相同、并且输入输出一一对应的S盒被称为双射型S盒。

[0011] 在密码处理的非线性变换中应用S盒的情况下,所应用的S盒的性质对密码的安全性产生较大的影响。即,例如已知有差分分析、线性分析等各种密码攻击,通过这种密码攻击来分析密钥、算法的困难性越高,密码的安全性越高。该安全性根据在块密码、哈希函数中利用的S盒的性质而有很大不同。

[0012] 例如,一般因为在整个密码算法、密码处理中应用的循环函数自身的输入输出大小较大(例如64比特、128比特等),因此难以对其进行严密的安全性评价。但是,S盒的输入输出大小一般较小。例如是8-bit输入输出左右,能够进行严密的安全性评价。已知有为了提高密码算法整体的安全性而要求在S盒中至少具有以下特性:

[0013] (1)最大差分概率足够小

[0014] (2)最大线性概率足够小

[0015] (3)进行布尔多项式表现时的布尔代数次数足够大

[0016] (4)将输入输出进行多项式表现时的项数足够多。

[0017] (1)主要决定对差分攻击的抵抗性,(2)主要决定对线性攻击的抵抗性,(3)主要决定对高阶差分攻击的抵抗性,(4)主要决定对插值攻击的抵抗性。并且,为了提高安全性,S盒的输入输出的比特相关性较低、使输入变化1比特时输出的变化为1/2左右等很重要。

[0018] 另外,对S盒除了要求安全性以外,还要求较高的安装性能。例如,在利用软件执行密码处理、哈希函数的安装结构中,通常进行设为如下结构的安装:在存储器中保持表示对于输入的输出的表,通过被称为查表(表安装)的方法执行非线性变换处理,因此该结构的安装性能不怎么依赖于S盒的内部结构。然而,在硬件安装中,例如构成用于根据输入值算出特定的输出的电路。该电路结构根据所应用的S盒而发生较大变化,从而对电路规模产生影响。

[0019] 非专利文献1:K.Nyberg,“Generalized Feistel networks”,ASIACRYPT’96,Springer Verlag,1996,pp.91--104.

[0020] 非专利文献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

发明内容

[0021] 发明要解决的问题

[0022] 本发明是鉴于上述问题点而完成的,其目的在于提供一种对执行在密码处理、哈希函数等中利用的非线性变换处理的S盒的结构进行改进来提高对各种密码攻击的抵抗性的结构、即提高了安全性的数据变换装置和数据变换方法、以及计算机程序。

[0023] 用于解决问题的方案

[0024] 本发明的第一侧面在于一种数据变换装置,其特征在于,具有:第一级非线性变换部,其由多个小型非线性变换部构成,该多个小型非线性变换部对分割输入数据得到的各

分割数据执行非线性变换处理的；线性变换部，其输入来自构成上述第一级非线性变换部的多个小型非线性变换部的所有输出并执行线性变换；以及第二级非线性变换部，其由多个小型非线性变换部构成，该多个小型非线性变换部对分割上述线性变换部的输出数据得到的各分割数据执行非线性变换处理的，其中，上述线性变换部是如下结构：利用具有与上述输入数据的比特大小相同大小的要素的矩阵运算执行数据变换，在矩阵是 m×m 矩阵的情况下，执行应用了具有至少 m 以上的分支数的高分支数的矩阵的数据变换处理。

[0025] 并且，在本发明的数据变换装置的一个实施方式中，其特征在于，在上述输入数据是 n 比特数据的情况下，上述第一级非线性变换部由 k 个小型非线性变换部构成，其中，上述 k 个小型非线性变换部分别输入作为输入数据的 n 比特数据的分割数据即 n/k 比特并输出作为非线性变换处理结果的 n/k 比特，上述线性变换部是如下结构：输入上述 k 个小型非线性变换部所输出的总计 n 比特的数据，通过应用了高分支数的矩阵的数据变换处理来生成 n 比特的输出，上述第二级非线性变换部是具有 k 个小型非线性变换部的结构，上述 k 个小型非线性变换部分别输入从上述线性变换部输出的 n 比特数据的分割数据即 n/k 比特并输出作为非线性变换处理结果的 n/k 比特。

[0026] 并且，在本发明的数据变换装置的一个实施方式中，其特征在于，上述线性变换部是执行应用了 MDS(Maximum Distance Separable) 矩阵的数据变换处理的结构，其中，上述 MDS 矩阵执行最优扩散变换 ODM(Optimal Diffusion Mappings) 处理。

[0027] 并且，在本发明的数据变换装置的一个实施方式中，其特征在于，在上述输入数据是 n 比特数据的情况下，上述线性变换部是执行应用了由在 GF(2) 上定义的 n 次既约多项式 p(x) 定义的扩展域 $GF(2^n)$ 上的矩阵的数据变换处理的结构。

[0028] 并且，在本发明的数据变换装置的一个实施方式中，其特征在于，上述数据变换装置是执行 n 比特输入输出的非线性变换处理的 S 盒，包含在上述第一级非线性变换部和上述第二级非线性变换部中的多个小型非线性变换部由执行比特数少于 n 比特的非线性变换处理的小型 S 盒构成。

[0029] 并且，在本发明的数据变换装置的一个实施方式中，其特征在于，上述数据变换装置是执行伴随有非线性变换处理的密码处理的结构。

[0030] 并且，在本发明的数据变换装置的一个实施方式中，其特征在于，上述密码处理是共用密钥块密码处理。

[0031] 并且，本发明的第二侧面在于一种数据变换方法，在数据变换装置中执行，其特征在于，具有以下步骤：第一级非线性变换步骤，在第一级非线性变换部中，应用多个小型非线性变换部对分割输入数据得到的各分割数据执行非线性变换处理；线性变换步骤，在线性变换部中，输入来自构成上述第一级非线性变换部的多个小型非线性变换部的所有输出并执行线性变换；以及第二级非线性变换步骤，在第二级非线性变换部中，应用多个小型非线性变换部对分割上述线性变换部的输出数据得到的各分割数据执行非线性变换处理，其中，上述线性变换步骤是如下步骤：利用具有与上述输入数据的比特大小相同大小的要素的矩阵运算执行数据变换，在矩阵是 m×m 矩阵的情况下，执行应用了具有至少 m 以上的分支数的高分支数的矩阵的数据变换处理。

[0032] 并且，本发明的第三侧面在于一种计算机程序，使数据变换装置执行数据变换处理，其特征在于，具有以下步骤：第一级非线性变换步骤，在第一级非线性变换部中，应用多

个小型非线性变换部对分割输入数据得到的各分割数据执行非线性变换处理；线性变换步骤，在线性变换部中，输入来自构成上述第一级非线性变换部的多个小型非线性变换部的所有输出并执行线性变换；以及第二级非线性变换步骤，在第二级非线性变换部中，应用多个小型非线性变换部对分割上述线性变换部的输出数据得到的各分割数据执行非线性变换处理，其中，上述线性变换步骤是如下步骤：利用具有与上述输入数据的比特大小相同大小的要素的矩阵运算执行数据变换，在矩阵是 m×m 矩阵的情况下，执行应用了具有至少 m 以上的分支数的高分支数的矩阵的数据变换处理。

[0033] 此外，本发明的计算机程序例如是能够通过以计算机可读形式提供对的存储介质、通信介质、例如 CD、FD、MO 等记录介质、或者网络等通信介质对执行各种程序代码的计算机系统提供的计算机程序。通过以计算机可读的形式提供这种程序，在计算机系统上实现与程序相应的处理。

[0034] 本发明还提供一种信息处理装置，其具备：存储器，其保存在密码处理中使用的密钥；处理器，其执行程序；以及密码处理部，其执行将 F 函数反复执行多个循环的扩展 Feistel 型共用密钥块密码处理，其中，该密码处理部具有：第一数据分割部，其对明文数据进行分割，并调整 F 函数的各循环的循环密钥的比特数使其与通过明文数据的分割得到的比特数相同；密钥异或运算部，其对由上述第一数据分割部分割得到的数据执行与上述循环密钥异或的密钥异或运算；第二数据分割部，其对由上述密钥异或运算部进行密钥异或运算得到的数据进一步进行分割；第一级非线性变换部，其由执行由上述第二数据分割部分割得到的各个数据的非线性变换处理的多个小型非线性变换部构成；线性变换部，其被输入来自构成上述第一级非线性变换部的小型非线性变换部的所有输出并执行线性变换；第三数据分割部，其对上述线性变换部的输出数据进行分割；以及第二级非线性变换部，其由在上述线性变换之后紧接着执行由上述第三数据分割部分割得到的各个数据的非线性变换处理的多个小型非线性变换部构成。

[0035] 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。

[0036] 发明的效果

[0037] 根据本发明的一个实施例的结构，例如将在共用密钥块密码处理、哈希函数等处理中执行的非线性变换处理设为进行应用了第一级非线性变换部、线性变换部以及第二级非线性变换部的数据变换的结构，其中，上述第一级非线性变换部利用多个较小的 S 盒 (S-box) 执行非线性变换，上述线性变换部输入来自第一级非线性变换部的所有输出并执行线性变换，上述第二级非线性变换部由执行分割线性变换部的输出数据得到的各分割数据的非线性变换处理的多个小型非线性变换部构成，在线性变换部中设为执行应用了进行最优扩散变换的矩阵的数据变换的结构，因此能够不使从数据的输入起直到输出的关键路径过大，而能够实现适当的数据扩散，实现对各种密码攻击的抵抗性较强的安全性较高的数据变换。

附图说明

[0038] 图 1 是表示共用密钥块密码算法的基本结构的图。

[0039] 图 2 是说明图 1 所示的共用密钥块密码处理部 E10 的内部结构的图。

[0040] 图 3 是说明图 2 所示的密码处理部 12 的详细结构的图。

[0041] 图 4 是说明作为循环函数执行部的一个结构例的 SPN 结构循环函数的图。

[0042] 图 5 是说明作为循环函数执行部的一个结构例的 Feistel（菲斯特尔）结构的图。

[0043] 图 6 是说明作为循环函数执行部的一个结构例的扩展 Feistel 结构的图。

[0044] 图 7 是说明非线性变换处理部的具体例的图。

[0045] 图 8 是说明线性变换处理部的具体例的图。

[0046] 图 9 是说明 CRYPTON ver.0.5 的 S 盒的结构的图。

[0047] 图 10 是说明 CRYPTON ver.1.0 的 S 盒的结构的图。

[0048] 图 11 是说明 Whirlpool 的 S 盒的结构的图。

[0049] 图 12 是说明 FOX 的 S 盒的结构的图。

[0050] 图 13 是表示本发明的一个实施例所涉及的作为非线性变换处理结构的 n 比特输入输出 S 盒的结构例的图。

[0051] 图 14 是说明本发明的一个实施例所涉及的执行具体的 8 比特输入输出的非线性变换的 S 盒的结构例的图。

[0052] 图 15 是说明本发明的一个实施例所涉及的执行具体的 8 比特输入输出的非线性变换的 S 盒的结构例的图。

[0053] 图 16 是说明本发明的一个实施例所涉及的执行具体的 8 比特输入输出的非线性变换的 S 盒的结构例的图。

[0054] 图 17 是说明本发明的一个实施例所涉及的执行具体的 8 比特输入输出的非线性变换的 S 盒的结构例的图。

[0055] 图 18 是说明本发明的一个实施例所涉及的执行非线性变换的 S 盒的结构例的图。

[0056] 图 19 是表示本发明所涉及的作为装置例的密码处理装置结构例的图。

具体实施方式

[0057] 下面，详细说明本发明的数据变换装置和数据变换方法、以及计算机程序。按照以下项目进行说明。

[0058] 1. 共用密钥块密码的概要

[0059] 2. 密码攻击的概要

[0060] 3. 由多个小型 S 盒的组合构成的非线性变换处理结构

[0061] (3-1) 关于由多个小型 S 盒的组合构成的非线性变换处理结构的有效性

[0062] (3-2) 以往的由多个小型 S 盒的组合构成的非线性变换处理结构和问题点

[0063] (3-3) 本发明所涉及的由多个小型 S 盒的组合构成的非线性变换处理结构

[0064] 4. 密码处理装置的结构例

[0065] [1. 共用密钥块密码的概要]

[0066] 首先，说明可应用本发明的共用密钥块密码的概要。在本说明书中设为共用密钥块密码（以下为块密码）是指以下定义的块密码。

[0067] 块密码输入明文 P 和密钥 K，输出密文 C。将明文和密文的比特 (bit) 长度称为块大小，在此用 n 表示。n 可取任意的整数值，但是通常在每个块密码算法中是预先决定的一

个值。有时也将块长度为 n 的块密码称为 n 比特块密码。

[0068] 用 k 表示密钥的比特长度。密钥可取任意的整数值。共用密钥块密码算法与一个或多个密钥大小对应。例如，某个块密码算法 A 可以是块大小 n = 128、与密钥的比特长度 k = 128 或 k = 192 或 k = 256 的各种密钥大小对应的结构。

[0069] 将明文 [P]、密文 [C]、密钥 [K] 各自比特大小表示为如下。

[0070] 明文 P :n 比特

[0071] 密文 C :n 比特

[0072] 密钥 K :k 比特

[0073] 图 1 示出与 k 比特的密钥长度对应的 n 比特共用密钥块密码算法 E 的图。如图 1 所示，共用密钥块密码处理部 E10 输入 n 比特的明文 P 和 k 比特的密钥 K，执行预先决定的密码算法，输出 n 比特的密文 C。此外，图 1 仅示出从明文生成密文的加密处理。从密文生成明文的解密处理一般使用密码处理部 E10 的反函数。但是，根据密码处理部 E10 的结构，在解密处理中也能够应用同样的共用密钥块密码处理部 E10，能够通过密钥的输入顺序等顺序的变更来进行解密处理。

[0074] 参照图 2 说明图 1 所示的共用密钥块密码处理部 E10 的内部结构。能够将块密码分为两个部分考虑。一个是密钥调度部 11，另一个是密码处理部 12，其中，上述密钥调度部 11 以密钥 K 为输入，通过某个决定的步骤扩展输入密钥 K 的比特长度，从而输出扩展密钥 K’（比特长度 k’），上述密码处理部 12 接受明文 P 和从密钥调度部 11 输入的扩展密钥 K’，以明文 P 为输入，执行应用了扩展密钥 K’的密码处理，执行用于生成密文 C 的数据的变换。此外，如之前所说明的那样，根据密码处理部 12 的结构，有时在将密文恢复为明文的数据解密处理中也能够应用密码处理部 12。

[0075] 接着，参照图 3 说明图 2 所示的密码处理部 12 的详细结构。如图 3 所示，密码处理部 12 具有反复执行应用了循环函数执行部 20 的数据变换的结构。即，能够以称为循环函数执行部 20 的处理单位来分割密码处理部 12。循环函数执行部 20 接受前级的循环函数执行部的输出 X_i 和根据扩展密钥而生成的循环密钥 RK_i 这两个数据作为输入，在内部执行数据变换处理，将输出数据 X_{i+1} 输出到下一个循环函数执行部。此外，在第一循环中输入是明文或对明文的初始化处理数据。另外，最终循环的输出为密文。

[0076] 在图 3 所示的例子中，密码处理部 12 是如下结构 :具有 r 个循环函数执行部 20，反复进行 r 次循环函数执行部中的数据变换来生成密文。将循环函数的重复次数称为循环数。在图示的例子中循环数为 r。

[0077] 各循环函数执行部的输入数据 X_i 是加密过程中的 n 比特数据，提供某个循环中的循环函数的输出 X_{i+1} 作为下一个循环的输入。各循环函数执行部的另一个输入数据使用从密钥调度输出的基于扩展密钥 K’的数据。将输入到各循环函数执行部、在循环函数的执行中应用的密钥称为循环密钥。在图中将在第 i 循环中应用的循环密钥表示为 RK_i。扩展密钥 K’例如构成为 r 个循环的循环密钥 $RK_1 \sim RK_r$ 的连接数据。

[0078] 图 3 所示的结构是从密码处理部 12 的输入侧看、将第一循环的输入数据表示为 X_0、将从第 i 循环函数输出的数据表示为 X_i、将循环密钥表示为 RK_i 的密码处理部 12 的结构。此外，根据该密码处理部 12 的结构，例如可以是如下结构 :将所应用的循环密钥的应用顺序设定为与加密处理相反，将密文输入到密码处理部 12 来输出解密文。

[0079] 图 3 所示的密码处理部 12 的循环函数执行部 20 可采用各种方式。循环函数能够根据其密码算法所采用的结构 (structure) 进行分类。作为代表性的结构存在如下结构 :

[0080] (a)SPN(Substitution Permutation Network :置换组合网路) 结构 ;

[0081] (b)Feistel 结构 ;

[0082] (c) 扩展 Feistel 结构。

[0083] 下面,参照图 4 ～图 6 说明这些具体结构。

[0084] (a)SPN 结构循环函数

[0085] 首先,参照图 4 说明作为循环函数执行部 20 的一个结构例的 SPN 结构循环函数。SPN 结构循环函数执行部 20a 具有连接了非线性变换层 (S 层) 与线性变换层 (P 层) 的、所谓的 SP 型的结构。如图 4 所示,由异或运算部 21、非线性变换处理部 22、线性变换处理部 23 等构成,其中,上述异或运算部 21 对所有 n 比特的输入数据执行与循环密钥之间的异或 (XOR) 运算,上述非线性变换处理部 22 输入异或运算部 21 的运算结果,执行输入数据的非线性变换,上述线性变换处理部 23 输入非线性变换处理部 22 中的非线性变换处理结果,执行对输入数据的线性变换处理。将线性变换处理部 23 的线性变换处理结果输出到下一个循环。在最终循环中输出为密文。此外,在图 4 所示的例子中,示出了异或运算部 21、非线性变换处理部 22、线性变换处理部 23 的处理顺序,但是并不限定这些处理部的顺序,也可以是以其它的顺序进行处理的结构。

[0086] (b)Feistel 结构

[0087] 接着,参照图 5 说明作为循环函数执行部 20 的一个结构例的 Feistel(菲斯特尔) 结构。如图 5 所示,Feistel 结构将来自前一循环的作为输入 (在第一循环中是输入文) 的 n 比特的输入数据分割为 n/2 比特的两个数据,在各循环中进行替换并且执行处理。

[0088] 如图所示,在应用了具有 Feistel 结构的循环函数执行部 20b 的处理中,将一个 n/2 比特数据和循环密钥输入到 F 函数部 30。F 函数部 30 与上述的 SPN 结构同样地具有连接了非线性变换层 (S 层) 与线性变换层 (P 层) 的、所谓的 SP 型的结构。

[0089] 将来自前一循环的 n/2 比特数据和循环密钥输入到 F 函数部 30 的异或运算部 31 并进行异或 (XOR) 处理。并且,将该结果数据输入到非线性变换处理部 32 来执行非线性变换,并且,将该非线性变换结果输入到线性变换处理部 33 来执行线性变换。输出该线性变换结果作为 F 函数处理结果数据。

[0090] 并且,将该 F 函数输出与从前一循环输入的另一个 n/2 比特输入输入到异或运算部 34,执行异或运算 (XOR),将执行结果设定为下一个循环中的 F 函数的输入。此外,将被设定为图示的第 i 循环的 F 函数输入的 n/2 比特应用在与下一个循环的 F 函数输出的异或运算中。这样,Feistel 结构在各循环中交替地替换输入并且执行应用了 F 函数的数据变换处理。

[0091] (c) 扩展 Feistel 结构

[0092] 接着,参照图 6 说明作为循环函数执行部 20 的一个结构例的扩展 Feistel 结构。之前参照图 5 所说明的 Feistel 结构将 n 比特的明文分割为两个并分配为各 n/2 比特来执行处理。即,是设为分割数 :d = 2 的处理。此外,该分割数也被称为数据序列数。

[0093] 在扩展 Feistel 结构中,是将该数据序列数 (分割数)d 设为 3 以上的任意整数的设定。能够定义与数据序列数 (分割数)d 的值相应的各种扩展 Feistel 结构。在图 6 所

示的例子中，数据序列数（分割数）d = 4，对各序列输入 n/4 比特的数据。在各循环中执行一个以上的作为循环函数的 F 函数。图示的例子是在一个循环中进行两个 F 函数部的循环运算的结构例。

[0094] F 函数部 41、42 的结构与之前参照图 5 所说明的 F 函数部 30 的结构相同，是执行循环密钥与输入值之间的异或运算、以及非线性变换处理、线性变换处理的结构。此外，调整输入到各 F 函数部的循环密钥使得比特数与输入比特一致。在图示的例子中，输入到各 F 函数部 41、42 的循环密钥为 n/4 比特。对构成扩展密钥的循环密钥进一步进行比特分割而生成这些密钥。此外，在将数据序列数（分割数）设为 d 时，输入到各序列的数据是 n/d 比特，输入到各 F 函数的密钥的比特数也被调整为 n/d 比特。

[0095] 此外，在图 6 所示的扩展 Feistel 结构中，是将数据序列数（分割数）设为 d、在各循环中并行地执行 d/2 个 F 函数的结构例，但是扩展 Feistel 结构可以是在各循环中执行一个以上 d/2 个以下的 F 函数的结构。

[0096] 如参照图 4 ～图 6 所说明的那样，共用密钥块密码中的密码处理部 12 的循环函数执行部 20 可采用如下结构：

[0097] (a)SPN(Substitution Permutation Network) 结构；

[0098] (b)Feistel 结构；

[0099] (c) 扩展 Feistel 结构。

[0100] 这些循环函数执行部都具有连接了非线性变换层 (S 层）与线性变换层 (P 层）的、所谓的 SP 型的结构。即，具有执行非线性变换处理的非线性变换处理部和执行线性变换处理的线性变换处理部。下面，说明这些变换处理结构。

[0101] （非线性变换处理部）

[0102] 参照图 7 说明非线性变换处理部的具体例。如图 7 所示，具体地说，非线性变换处理部 50 是并列 m 个被称为 S 盒 (S-box)51 的 s 比特输入 s 比特输出的非线性变换表而得到的，将 ms 比特的输入数据以每 s 比特进行分割并分别输入到对应的 S 盒 (S-box)51 中进行数据变换。在各 S 盒 51 中，例如执行应用了变换表的非线性变换处理。

[0103] 如果所输入的数据的大小变大，则安装方面的成本有变高的趋势。如图 7 所示，为了避免这种趋势，多采用如下结构：将处理对象数据 X 分割为多个单位，对各个单位实施非线性变换。例如，在将输入大小设为 ms 比特时，分割为各 s 比特的 m 个数据，对 m 个 S 盒 (S-box)51 分别输入 s 比特，例如执行应用了变换表的非线性变换处理，合成 m 个这些各 S 比特输出，得到 ms 比特的非线性变换结果。

[0104] （线性变换处理部）

[0105] 参照图 8 说明线性变换处理部的具体例。线性变换处理部将输入值、例如作为来自 S 盒的输出数据的 ms 比特的输出值作为输入值 X 而输入，对该输入实施线性变换而输出 ms 比特的结果。线性变换处理例如执行输入比特位置的替换处理等线性变换处理，输出 ms 比特的输出值 Y。线性变换处理例如对输入应用线性变换矩阵来进行输入比特位置的替换处理。该矩阵的一例是图 8 所示的线性变换矩阵。

[0106] 在线性变换处理部中应用的线性变换矩阵的要素是扩展域：$GF(2^8)$ 的域的要素、GF(2) 的要素等，一般能够构成为应用了各种表现的矩阵。图 8 表示具有 ms 比特输入输出、由在 $GF(2^S)$ 上定义的 m×m 矩阵定义的线性变换处理部的一个结构例。

[0107] [2. 密码攻击的概要]

[0108] 作为对上述的共用密钥块密码的密码攻击、即所应用的密钥的分析或者算法的分析方法，已知各种方法。下面说明该密码攻击的概要。依次说明下面的各攻击。

[0109] (2-1) 差分攻击

[0110] (2-2) 线性攻击

[0111] (2-3) 高阶差分攻击

[0112] (2-4) 插值攻击

[0113] (2-1) 差分攻击

[0114] 作为共用密钥密码的攻击法之一存在差分解读法 (Differential Cryptanalysis)。例如在文献“E.Biham,A.Shamir, ‘Differential Cryptanalysis of DES-like Cryptosystems,’Journal of Cryptology,Vol.4,No.1,pp.3-72,1991.”中记载了差分解读法。

[0115] 该攻击法是如下的攻击法：对某个密码观测被称为差分值的数据的传播，在以高概率发生该差分值的传播的情况下，能够进行攻击、即能够进行密钥的估计。将该被称为差分值的数据的传播概率称为差分概率。

[0116] 当对 n 比特输入输出的函数 f 定义输入为 x(n-bit)、输入差分值为 Δx(n-bit)、输出差分值为 Δy(n-bit) 时，将对于函数 f 的输入差分值 Δx、输出差分值 Δy 的差分概率 $DP_f(\Delta x, \Delta y)$ 定义为如下。

[0117] [式 1]

[0118] $$DP_f(\Delta x, \Delta y) = \frac{\#\{x \in \{0,1\}^n \mid f(x) \oplus f(x \oplus \Delta x) = \Delta y\}}{2^n}$$

[0119] 另外，将对于函数 f 的最大差分概率 MDP_f 定义为如下。

[0120] [式 2]

[0121] $$MDP_f = \max_{\Delta x \neq 0, \Delta y} DP_f(\Delta x, \Delta y)$$

[0122] 这些值是根据函数 f 唯一求出的值，最大差分概率 MDP_f 较大的函数 f 是对差分攻击的抵抗性较弱的函数。因此，希望在设计密码时设计函数 f 以使 MDP_f 尽可能小。

[0123] (2-2) 线性攻击

[0124] 作为共用密钥密码的攻击法之一还存在线性解读法 (Linear Cryptanalysis)。例如在文献“M.Matsui, ‘Linear Cryptanalysis Method for DES Cipher,’EUROCRYPT’93, LNCS765,pp.386-397,1994.”中记载了线性解读法。

[0125] 该攻击法是如下的攻击法：对某个密码观测输入的特定比特的异或与输出的特定比特的异或之间的相关性，在发现较强的相关关系的情况下，能够进行攻击、即能够进行密钥的估计。将该输入输出的特定比特的相关系数称为线性概率。

[0126] 在对 n 比特输入输出的函数 f 定义输入为 x(n-bit)、输入掩模值为 Γx(n-bit)、输出掩模值为 Γy(n-bit) 时，将对于函数 f 的输入掩模值 Γx、输出掩模值 Γy 的线性概率 $LP_f(\Gamma x, \Gamma y)$ 定义为如下。

[0127] [式 3]

[0128] $$LP_f(\Gamma x,\Gamma y)=\left(2\cdot\frac{\#\{x\in\{0,1\}^n \mid x\bullet\Gamma x=f(x)\bullet\Gamma y\}}{2^n}-1\right)^2$$

[0129] 其中，在上式中［·］表示 n 比特向量之间的内积运算。

[0130] ［式 4］

[0131] $$x\bullet y=\oplus_{i=1}^{n}(x_i\cdot y_i)$$

[0132] 另外，将对于函数 f 的最大线性概率 MLP_f 定义为如下。

[0133] ［式 5］

[0134] $$MLP_f=\max_{\Gamma x,\Gamma y\neq 0}LP_f(\Gamma x,\Gamma y)$$

[0135] 这些值是根据函数 f 唯一求出的值，最大线性概率 MLP_f 较大的函数 f 是对线性攻击的抵抗性较弱的函数。因此，希望在设计密码时设计函数 f 以使 MLP_f 尽可能小。

[0136] (2-3) 高阶差分攻击

[0137] 作为共用密钥密码的攻击法之一还存在高阶差分攻击法 (Higher Order Differential Attack)。例如在文献“L.R.Knudsen、‘Truncated and Higher Order Differentials.’FSE’94、LNCS 1008,pp.196-211”中记载了高阶差分攻击法。

[0138] 该攻击法是利用了密码算法所具有的代数性质的攻击法，是如下的攻击法：在用明文的所有比特对密文进行布尔多项式表现时，在对于明文的特定数量比特该布尔代数次数小于某个次数的情况下，能够进行攻击、即能够进行密钥的估计。

[0139] (2-4) 插值攻击

[0140] 作为共用密钥密码的攻击法之一还存在插值攻击法 (Interpolation Attack)。例如在文献“T.Jakobsen and L.R.Knudsen, ‘The Interpolation Attack on Block Cipher,’FSE’97,LNCS1267,pp.28-40,1997.”中记载了插值攻击。

[0141] 该攻击法是利用了密码算法所具有的代数性质的攻击法，是如下的攻击法：在将加密函数表现为多项式函数时其项数较少的情况下，通过复原包含密钥值的加密函数来进行攻击。

[0142] ［3. 由多个小型 S 盒的组合构成的非线性变换处理结构］

[0143] (3-1) 关于由多个小型 S 盒的组合构成的非线性变换处理结构的有效性

[0144] 如上所述，共用密钥块密码是通过循环函数的重复来进行密码处理的结构。该共用密钥块密码处理是反复执行循环函数的结构，在循环函数中执行线性变换处理和非线性变换处理。在非线性变换处理中，例如如参照图 7 所说明的那样，执行应用了 S-box(S 盒）的非线性变换处理。除了上述的共用密钥块密码处理之外，例如在哈希函数等数据变换中也能够在非线性变换处理中应用 S 盒。

[0145] 如之前所说明的那样，该 S 盒的输入输出大小一般比较小，能够进行严密的安全性评价，作为为了提高密码、哈希算法整体的安全性而要求 S 盒具有的特性，已知以下的特性：

[0146] (1) 最大差分概率足够小

[0147] (2) 最大线性概率足够小

[0148] (3) 进行布尔多项式表现时的布尔代数次数足够大

[0149] (4) 将输入输出进行多项式表现时的项数足够多。

[0150] (1) 主要决定对差分攻击的抵抗性，(2) 主要决定对线性攻击的抵抗性，(3) 主要决定对高阶差分攻击的抵抗性，(4) 主要决定对插值攻击的抵抗性。并且，为了提高安全性，S 盒的输入输出的比特相关性较低、使输入变化 1 比特时输出的变化为 1/2 左右等很重要。

[0151] 另外，对 S 盒除了要求安全性以外，还要求较高的安装性能。例如，在利用软件执行密码处理、哈希函数的安装结构中，通常进行设为如下结构的安装：在存储器中保持表示对于输入的输出的表，通过被称为查表（表安装）的方法执行非线性变换处理，因此该结构的安装性能不怎么依赖于 S 盒的内部结构。然而，在硬件安装中，例如构成用于根据输入值来算出特定的输出的电路。该电路结构根据所应用的 S 盒而发生较大变化，因而对电路规模产生影响。

[0152] 如上所述，作为为了维持密码算法、哈希算法的安全性而要求 S 盒具有的特性，存在如下特性：

[0153] (1) 最大差分概率足够小

[0154] (2) 最大线性概率足够小

[0155] (3) 进行布尔多项式表现时的布尔代数次数足够大

[0156] (4) 将输入输出进行多项式表现时的项数足够多，

[0157] 作为高效地生成满足这种要求的 S 盒的方法，通常已知使用扩展域上的乘方函数的方法。在该方法中如果适当地选择扩展域的次数和乘方的指数，则能够生成特性优良的 S 盒。

[0158] 实际上在设 n-bit 输入输出 S 盒的输入为 x、输出为 y、并分别为扩展域 $GF(2^n)$ 的基的情况下，在以

[0159] [式 6]

[0160] $$y = x^{2^t+1}$$

[0161] (t 为任意整数)

[0162] -1

[0163] $y = x$

[0164] 提供 $y = f(x)$ 的情况下，通常已知在最大差分概率、最大线性概率这点上能够构成最适合的 S 盒。

[0165] 作为用这种方法构成的 S 盒的例子，列举出在 AES、Camellia、MISTY 中应用的 S 盒等。

[0166] 关于 AES、Camellia 的 S 盒，也能够设为 $GF((2^4)^2)$ 上的逆元函数来构成 S 盒，因此可以说从安全性的观点出发特性非常好，并且具有非常高的硬件安装性能。

[0167] 然而，近年来，关于这种 S 盒，也被指出与利用其特征性的代数性质的攻击法、其过于均匀的扩散性有关的问题点等。

[0168] 根据上述的问题点考虑不具有特征性的代数性质的 S 盒的构成法，考虑通过如下的方法来生成 S 盒的方法以使 S 盒不具有较强的代数结构：通过随机、或以其为基准的方

法来选择要素。当通过这种方法生成 S 盒时，多数情况下不具有特征性的代数结构，并且不进行如扩展域上的乘方函数那样的均匀的扩散，因此可以说针对如上所述的问题采取了对策。

[0169] 然而，由于存在 2^n 阶乘个 n-bit 输入输出的双射 S 盒的数，因此实际上用随机生成 n-bit 输入输出的 S 盒并逐个检查其特性的方法，当 n 变大到某种程度时，难以高效地生成特性优良的 S 盒。

[0170] 另外，在完全随机地选择 S 盒的要素的情况下，在硬件中安装时也仅能够主要使用被称为表安装的方法，因此安装效率大幅降低。

[0171] 根据这种问题进行了如下试验：随机地生成具有较小的大小的输入输出的 S 盒，组合多个 S 盒来生成更大的 S 盒。例如，可认为

[0172] CRYPTON ver.0.5、

[0173] CRYPTON ver.1.0、

[0174] Whirlpool、

[0175] FOX

[0176] 等的 S 盒等是根据这种方法而生成的 S 盒。下面，说明它们的具体的结构例及其问题点。

[0177] (3-2) 以往的由多个小型 S 盒的组合构成的非线性变换处理结构和问题点

[0178] 下面，对以下的各结构说明以往的由多个小型 S 盒的组合构成的非线性变换处理结构和问题点：

[0179] (a)CRYPTON ver.0.5、

[0180] (b)CRYPTON ver.1.0、

[0181] (c)Whirlpool、

[0182] (d)FOX。

[0183] (a)CRYPTON ver.0.5

[0184] 例如，CRYPTON ver.0.5 的 S 盒具有图 9 所示的结构。具有如下结构：S 盒 $[S4_0]$101、S 盒 $[S4_1]$102、S 盒 $[S4_2]$103 是 4 比特输入输出的 S 盒，将这三个 S 盒与异或运算部 111 ～ 113 组合，对输入 8 比特进行非线性变换从而得到输出 8 比特。此外，在图中示出的 S 盒的标记 $[S4_n]$ 中，4 表示是 4 比特输入输出的 S 盒，n 是 S 盒的标识符。S 盒 $[S4_0]$101、S 盒 $[S4_1]$102、S 盒 $[S4_2]$103 都是 4 比特输入输出的 S 盒，是分别执行不同的非线性变换处理的不同的 S 盒。

[0185] 该结构由于采用所谓的 3 级 Feistel 结构，因此导致布尔代数次数变低，并且关键路径 (critical path) 较长。即，是从输入起直到得到最终输出为止必须通过三个较小的 S 盒的结构。因而，具有安装性能不太高的特征。

[0186] (b)CRYPTON ver.1.0

[0187] 另外，CRYPTON ver.1.0 的 S 盒具有图 10 所示的结构。由 S 盒 $[S4_0]$121、S 盒 $[S4_1]$122、执行 S 盒 $[S4_1]$122 的逆变换的 S 盒 $[S4_1^{-1}]$123、执行 S 盒 $[S4_0]$121 的逆变换的 S 盒 $[S4_0^{-1}]$124、以及利用比特运算执行线性变换处理的比特运算部 131、132 构成。

[0188] 在 S 盒 $[S4_0]$121 中对输入 8 比特的上位 4 比特执行非线性变换之后，输入到比特运算部 131 进行线性变换，将其结果输入到 S 盒 $[S4_1^{-1}]$123 并输出非线性变换结果。关于下

位 4 比特，在 S 盒 [$S4_1$]122 中执行非线性变换之后，输入到比特运算部 131 进行线性变换，将其结果输入到 S 盒 [$S4_0^{-1}$]123 并输出非线性变换结果。

[0189] 该结构必须从 1-bit 要素 8×8 的矩阵、即 64 比特的空间中选择在中间使用的比特运算部 131 中的比特运算，因此很难进行该选择。即，在非线性变换中，要求设为从非线性变换对象的输入 8 比特得到基本上没有偏置的作为与各输入 8 比特对应的非线性变换结果的输出 8 比特的结构，从而存在如下问题：难以进行用于使在中间级的比特运算部 131、132 中应用的矩阵成为满足该要求的矩阵的选择。

[0190] (c)Whirlpool

[0191] 另外，Whirlpool 的 S 盒设为如图 11 那样的结构。具有如下结构：使用 S 盒 [$S4_0$]141、144、执行 S 盒 [$S4_0$] 的逆变换的 S 盒 [$S4_0^{-1}$]142、145、以及 S 盒 [$S4_1$]143，通过异或运算部 151 ～ 153 来结合这些 S 盒。

[0192] 在该结构中，所需的较小的 S 盒数多达 5 个，并且关键路径较长。即，是从输入起直到最终输出为止必须通过三个较小的 S 盒的结构，存在安装性能不太高的问题。

[0193] (d)FOX

[0194] 并且，FOX 的 S 盒设为图 12 所示的结构。具有如下结构：使用三种 4 比特输入输出 S 盒 161 ～ 163、4 比特输入输出 OR 电路 171、172，通过异或运算部来连接它们。

[0195] 在该结构中，所需的较小的 S 盒数较少为 3 个，但是整体上异或运算部 (XOR) 的数量较多，关键路径也较长。为了从输入得到最终输出必须通过三个较小的 S 盒。因此，存在安装性能不太高的问题。

[0196] (3-3) 本发明所涉及的由多个小型 S 盒的组合构成的非线性变换处理结构

[0197] 接着，说明本发明所涉及的由多个小型 S 盒的组合构成的非线性变换处理结构。如上所述，关于由多个小型 S 盒的组合构成的非线性变换处理结构，已经提出多个类型，但是分别具有关键路径较长的问题点、线性变换矩阵的设定困难等问题点。

[0198] 首先，说明下面理解按照本发明的非线性变换处理结构所需的以下的术语：

[0199] (a) 分支数以及最优扩散层、

[0200] (b) 扩展域上的矩阵运算。

[0201] (a) 分支数以及最优扩散层

[0202] 首先，说明分支数以及最优扩散变换 (Optimal Diffusion Mappings)。

[0203] 对从 n×a 比特数据向 n×b 比特数据的映射

[0204] θ :(0,1)na → {0,1)nb,

[0205] 将分支数 Bn(θ) 定义为如下。

[0206] [式 7]

[0207] $$B_n(\theta) = \min_{\alpha \neq 0} \{ hw_n(\alpha) + hw_n(\theta(\alpha)) \}$$

[0208] 其中，设 $\min_{\alpha \neq 0}\{X_\alpha\}$ 表示满足 α ≠ 0 的所有 X_α 中的最小值，设 $hw_n(Y)$ 是在按每 n 比特分割表示比特列 Y 时 n 比特的数据都返回不是 0 的 (非零) 要素数的函数。此时，将分支数 B(θ) 为 b+1 那样的映射 θ 定义为最优扩散变换 (Optimal Diffusion Mappings)。另外，以后将满足 ODM 的矩阵定义为 MDS(Maximum Distance Separable :最大距离可分) 矩阵。

[0209] (b) 扩展域上的矩阵运算

[0210] 将在扩展域 GF(2^n) 上进行的矩阵运算称为扩展域上的矩阵运算，其中，利用在基础域 GF(2) 上定义的 n 次既约多项式 p(x) 制作扩展域 GF(2^n)。

[0211] 例如，

[0212] [式 8]

[0213] $$\begin{pmatrix} y_0 \\ y_1 \end{pmatrix} = \begin{pmatrix} a_{0,0} & a_{0,1} \\ a_{1,0} & a_{1,1} \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \end{pmatrix}$$

[0214] 考虑上述矩阵运算。

[0215] 在上述矩阵运算中，输出 y_0、y_1 分别被表现为

[0216] $y_0 = a_{0,0}x_0 + a_{0,1}x_1$

[0217] $y_1 = a_{1,0}x_0 + a_{1,1}x_1$。

[0218] 此时考虑 $a_{0,0}$、x_0 等变量都是扩展域 GF(2^n) 上的基，在扩展域 GF(2^n) 上进行所有运算。将利用这种方法进行矩阵运算的方法称为扩展域上的矩阵运算。

[0219] 本发明所涉及的非线性变换处理结构实现了如下的非线性变换处理结构：解决了上述的以往的由多个小型 S 盒的组合构成的非线性变换处理结构中的问题点、即关键路径较长的问题点、线性变换矩阵的设定困难等问题点。

[0220] 在本发明的结构中，为了高效地生成难以在扩展域 GF(2^n) 上进行简单的表现、并且具有较高的安装性能（特别是硬件）的 n-bit 输入输出的双射 S 盒，而在较小的 S 盒的组合位置组合分支数较高的具有与较小的 S 盒的输入输出大小相同大小的要素的矩阵运算，来实现作为较大的 S 盒的非线性变换处理结构。具体地说，分支数较高的矩阵运算表示对于 m×m 矩阵具有 m 以上的分支数的矩阵。

[0221] 作为分支数较高的矩阵，例如选择执行上述的最优扩散变换的 MDS(Maximum Distance Separable) 矩阵。MDS 矩阵是构成矩阵的任意的小矩阵为正则矩阵的矩阵。此外，正则矩阵是具有逆矩阵的矩阵，当设矩阵为 A、逆矩阵为 A^{-1} 时，

[0222] $AA^{-1} = A^{-1}A = E$

[0223] 其中，E 是单位矩阵，上式成立的具有逆矩阵 A-1 的矩阵 A 是正则矩阵。

[0224] 图 13 示出本发明的一个实施例所涉及的作为非线性变换处理结构的 n 比特输入输出 S 盒的结构例。图 13 所示的结构是由 4 个 n/2 比特输入输出的双射 S 盒 201 ～ 204、以及线性变换处理部 211 构成的执行 n 比特输入输出的非线性变换处理的结构，其中，上述线性变换处理部 211 由在扩展域 GF($2^{n/2}$) 上定义的 2×2MDS(Maximum Distance Separable) 矩阵构成。

[0225] 是如下结构：输入 n 比特以上位 n/2 比特、下位 n/2 比特分别输入到 n/2 比特输入输出的双射 S 盒 [S_0]201、S 盒 [S_1]202，在各 S 盒中进行非线性变换处理之后，输入到由在扩展域 GF($2^{n/2}$) 上定义的 2×2MDS 矩阵构成的线性变换处理部 211，进行基于 MDS 矩阵的线性变换处理之后，线性变换结果的 n 比特以上位 n/2 比特、下位 n/2 比特分别输入到 n/2 比特输入输出的双射 S 盒 [S_2]203、S 盒 [S_3]204，在各 S 盒中进行非线性变换处理，从而得到作为输出结果的 n 比特。

[0226] 当如在图 13 所示的线性变换处理部 211 中应用的 MDS 矩阵那样利用分支数较高的扩散变换矩阵时，保证将前级的较小的 S 盒 [S_0]201、S 盒 [S_1]202 的输出非常均衡地配置为后级的较小的 S 盒 [S_2]203、S 盒 [S_3]204 的输入，因此能够生成整体特性优良的较大的 S 盒。另外，根据较小的 S 盒的输入输出大小 (n/2) 唯一地决定在线性变换处理部 211 中应用的相当于扩散变换矩阵的 MDS 矩阵的要素的大小，因此即使较大的 S 盒的输入输出大小 (n) 变大，由于限定了可选择的矩阵的空间，因此也能够容易地检查该矩阵的分支数。

[0227] 在图 13 所示的结构中的线性变换处理部 211 中应用的作为扩散变换矩阵的 MDS 矩阵的要素的大小是 n/2 比特，由于是 2×2 的矩阵，因此要素数为 4 个，即使检查整个矩阵，该数也为 $2^{n/2\times 4}$ 种左右，因此能够容易地检查整个矩阵。其中，设矩阵运算是利用在 GF(2) 上定义的 n 次既约多项式 p(x) 制作的扩展域 GF(2^n) 上的矩阵运算。

[0228] 当用该方法生成 S 盒时，考虑到限定为图 13 所示的结构中的输入输出大小 n/2 比特的较小的 S 盒 201 ～ 204 能够进行简单的代数表现，因此在扩展域 GF(2^n) 上的要素看起来是随机的。因此，可以认为难以在 GF(2^n) 上进行简单的代数表现。另外，期待不像扩展域上的乘方运算那样进行均匀的扩散。

[0229] 并且，如果适当地选择矩阵，则能够以简单的运算以及较短的路径构成 S 盒，因此，可以说与以 n-bit 随机生成的 S 盒、以往的组合较小的 S 盒而构成的 S 盒相比，安装效率更高。

[0230] 参照图 14 ～图 17 说明应用了图 13 所示的结构的执行具体的 8 比特输入输出的非线性变换的 S 盒的结构例。

[0231] 图 14 的 (a)、图 15 的 (a) 所示的结构相同，是表示应用了图 13 所示的结构的作为执行具体的 8 比特输入输出的非线性变换的 S 盒的一个结构例的 8 比特 S 盒 300 的结构的图。图 14 的 (b) 表示作为图 14 的 (a) 所示的 8 比特 S 盒 300 的结构要素的 4 个 4 比特输入输出 S 盒 301 ～ 304 的变换表。在该表中使用的数值是 16 进制数。是表示对于输入 :x ＝ 0 ～ F(16 进制数) 的各 S 盒 301 ～ 304 的输出值的表。另外，在图 15 的 (c) 中示出使用分支数较高的扩散变换、具体地说为最优扩散变换 [ODM] 即 MDS 矩阵 (matrix)311 作为图 15 的 (a)(＝图 14 的 (a)) 所示的线性变换处理部 311 的具体例。

[0232] 说明图 14 的 (a) 所示的执行 8 比特输入输出的非线性变换的 S 盒的处理。首先，将作为 8 比特 S 盒 300 的输入的 x(8-bit) 按 1/2、即每 4-bit 分割为 x[0]、x[1]。接着将 x[0] 输入到 4-bit 输入输出的 S 盒 [$S4_0$]301，将 x[1] 输入到 4-bit 输入输出的 S 盒 [$S4_1$]302，得到作为各 S 盒 301、302 中的非线性变换结果的输出 w[0]、w[1]。S 盒 [$S4_0$]301、S 盒 [$S4_1$]302 是随机选择的 4 比特 S 盒，设为按照图 14 的 (b) 的表的变换处理来执行非线性变换。

[0233] 此外，S 盒 [$S4_0$]301、S 盒 [$S4_1$]302 是满足最大差分概率足够低、最大线性概率足够低等 S 盒应该满足的所有性质那样的 S 盒。另外，由于这些 S 盒是 4-bit 输入输出，因此能够实现搜索满足这种性质的 S 盒。

[0234] 将 S 盒 [$S4_0$]301、S 盒 [$S4_1$]302 的输出 w[0]、w[1] 输入到利用最优扩散变换 [ODM] 即 MDS 矩阵 (matrix) 执行线性变换的线性变换处理部 311，作为 MDS 矩阵 (matrix) 的线性变换结果输出 z[0]、z[1]。在线性变换处理部 311 中通过由在 GF(2) 上定义的 4 次既约多项式 :$p(x) = x^4+x+1$ 制作的扩展域 GF(2^4) 上的矩阵运算来执行线性变换，输出 z[0]、z[1]。

作为线性变换处理部 311 的 MDS 矩阵 (matrix) 执行基于具有由 GF(2) 上的 4 次既约多项式定义的扩展域 $GF(2^4)$ 上的基作为要素的由 2×2 的 4 个要素构成的矩阵的线性变换处理。

[0235] 图 15 的 (c) 示出矩阵运算的具体处理。在应用了图 15 的 (c) 所示的 2×2 的 MDS 矩阵的情况下，根据输入 w[0]、w[1]，如下算出输出 z[0]、z[1]。

[0236] z[0] = w[0](XOR)w[1]×2

[0237] z[1] = w[0]×2(XOR)w[1]

[0238] 将作为最优扩散变换 [ODM] 即 MDS 矩阵 (matrix) 的线性变换结果而得到的 8 比特数据中的上位 4 比特 z[0] 输入到 4-bit 输入输出的 S 盒 $[S4_2]$303，将下位 4 比特 z[1] 输入到 4-bit 输入输出的 S 盒 $[S4_3]$304，在这些 4 比特 S 盒中执行非线性变换，得到输出 y[0]、y[1]。S 盒 $[S4_2]$303、S 盒 $[S4_3]$304 与 S 盒 $[S4_0]$301、S 盒 $[S4_1]$302 相同，分别是随机选择的特性优良的 4 比特 S 盒，执行按照图 14 的 (b) 所示的表的数据变换。最后将结合 S 盒 $[S4_2]$303、S 盒 $[S4_3]$304 所输出的 4 比特数据 y[0] 和 y[1] 得到的 8 比特数据设为 8 比特输入输出的 S 盒 300 的最终输出 y(8-bit)。

[0239] 图 16 的 (a) 所示的结构与图 14 的 (a) 所示的结构相同是应用了图 13 所示的结构的执行具体的 8 比特输入输出的非线性变换的 8 比特 S 盒 320 的一个结构例，图 16 的 (b) 表示作为图 16 的 (a) 所示的 8 比特 S 盒 320 的结构要素的 4 个 4 比特输入输出 S 盒 321 ～ 324 的变换表。在该表中使用的数值是 16 进制数。是表示对于输入 :x = 0 ～ F(16 进制数) 的各 S 盒 321 ～ 324 的输出值的表。另外，在图 17 的 (c) 中示出使用最优扩散变换 [ODM] 即 MDS 矩阵 (matrix)331 作为图 17 的 (a)(= 图 16 的 (a)) 所示的线性变换处理部 331 的具体例。

[0240] 关于图 16、图 17 所示的结构例，

[0241] 4 比特输入输出 S 盒 321 ～ 324 执行按照图 16 的 (b) 所示的表的非线性变换、

[0242] 线性变换处理部 331 进行按照图 17 的 (c) 的变换处理、

[0243] 这些处理不同。

[0244] 在线性变换处理部 331 中，通过由在 GF(2) 上定义的 4 次既约多项式 :$p(x) = x^4+x+1$ 制作的扩展域 $GF(2^4)$ 上的矩阵运算来执行线性变换，输出 z[0]、z[1]。作为线性变换处理部 331 的 MDS 矩阵 (matrix) 执行基于具有由 4 次既约多项式定义的以 2 为模的扩展域 $GF(2^4)$ 上的基作为要素的由 2×2 的 4 个要素构成的矩阵的线性变换处理。

[0245] 图 17 的 (c) 示出矩阵运算的具体处理。在应用了图 17 的 (c) 所示的 2×2 的 MDS 矩阵的情况下，根据输入 w[0]、w[1]，如下地算出输出 z[0]、z[1]。

[0246] z[0] = w[0](XOR)w[1]

[0247] z[1] = w[0](XOR)w[1]×2

[0248] 图 14 ～图 17 所示的例子是执行 8 比特输入输出的非线性变换处理的 S 盒，在线性变换处理部 311、331 中应用的 MDS 矩阵的要素的大小都是 n/2 比特，由于是 2×2 的矩阵，因此要素数为 4 个，即使检查整个矩阵，该数也为 $2^{n/2\times4}$ 种左右，因此能够容易地检查整个矩阵，如上所述，当用该方法生成 S 盒时，考虑到限定为较小的 S 盒能够进行简单的代数表现，因此在扩展域 $GF(2^n)$ 上的要素看起来是随机的，能够认为难以在 $GF(2^n)$ 上进行简单的代数表现。另外，不像扩展域上的乘方运算那样进行均匀的扩散。另外，在用于从输入得到输出的路径上仅存在两个较小的 S 盒，如果适当地选择矩阵，则能够以简单的运算以及

较短的路径构成 S 盒，因此与以 n-bit 随机生成的 S 盒、以往的组合较小的 S 盒而构成的 S 盒相比，安装效率更高。

[0249] 在图 13 ～图 17 所示的结构例中，是将输入 n 比特进行二分割并将上位 n/2 比特、下位 n/2 比特分别输入到 n/2 比特输入输出的 S 盒的结构，另外，是将来自线性变换处理部的输出 n 比特的上位 n/2 比特、下位 n/2 比特分别输入到 n/2 比特输入输出的 S 盒 [S2] 从而得到非线性变换处理结果的结构，但是将输入比特分割输入的较小的 S 盒数并不限于两个，也可以是其它的数。图 18 示出利用将输入 n 比特进行四分割来进行每 n/4 比特的非线性变换处理的较小的 n/4 比特输入输出 S 盒的 n 比特 S 盒 400 的结构例。

[0250] 图 18 所示的 n 比特 S 盒 400 的结构是由 8 个 n/4 比特输入输出的双射 S 盒 401 ～ 408、以及线性变换处理部 421 构成的执行 n 比特输入输出的非线性变换处理的结构，其中，上述线性变换处理部 421 由作为分支数较高的扩散变换的最优扩散变换 [ODM] 即在扩展域 $GF(2^{n/4})$ 上定义的 4×4MDS(Maximum Distance Separable) 矩阵构成。

[0251] 是如下结构：将输入 n 比特以每 n/4 比特进行分割，并分别输入到 n/4 比特输入输出的双射 S 盒 $[S_0]$401、S 盒 $[S_1]$402、S 盒 $[S_2]$403、S 盒 $[S_3]$404，在各 S 盒中进行非线性变换处理之后，输入到由在扩展域 $GF(2^{n/4})$ 上定义的 4×4MDS 矩阵构成的线性变换处理部 421，进行基于 MDS 矩阵的线性变换处理之后，将线性变换结果的 n 比特的每 n/4 比特分别输入到 n/4 比特输入输出的 S 盒 $[S_0]$405、S 盒 $[S_1]$406、S 盒 $[S_2]$407、S 盒 $[S_3]$408，在各 S 盒中进行非线性变换处理，得到作为输出结果的 n 比特。

[0252] 在图 18 所示的线性变换处理部 421 中应用的扩散变换也是最优扩散变换 [ODM] 即 MDS 矩阵，保证将前级的四个较小的 S 盒的输出非常均衡地配置为后级的较小的 S 盒的输入，因此能够生成整体特性优良的较大的 S 盒。

[0253] 概述由上述的执行按照本发明的非线性变换处理的 S 盒构成的数据变换装置的结构。本发明的数据变换装置的特征在于具有以下结构。即，具有：第一级非线性变换部，其由执行分割输入数据得到的各分割数据的非线性变换处理的多个小型非线性变换部（较小的 S 盒）构成；线性变换部，其输入来自构成第一级非线性变换部的多个小型非线性变换部的所有输出并执行线性变换；以及第二级非线性变换部，其由执行分割线性变换部的输出数据得到的各分割数据的非线性变换处理的多个小型非线性变换部（较小的 S 盒）构成，其中，线性变换部是如下结构：利用具有与输入数据的比特大小相同大小的要素的矩阵运算来执行数据变换，在矩阵是 m×m 矩阵的情况下，执行应用了具有至少 m 以上的分支数的高分支数的矩阵的数据变换处理。

[0254] 具体地说，在输入数据是 n 比特数据的情况下，第一级非线性变换部由 k 个小型非线性变换部构成，该 k 个小型非线性变换部分别输入作为输入数据的 n 比特数据的分割数据即 n/k 比特，输出作为非线性变换处理结果的 n/k 比特，线性变换部是输入 k 个小型非线性变换部所输出的总计 n 比特的数据，通过应用了高分支数的矩阵的数据变换处理来生成 n 比特的输出的结构，第二级非线性变换部是如下结构：具有 k 个小型非线性变换部，该 k 个小型非线性变换部分别输入作为从线性变换部输出的 n 比特数据的分割数据的 n/k 比特，输出作为非线性变换处理结果的 n/k 比特。

[0255] 在此，线性变换部是执行应用了 MDS(Maximum Distance Separable) 矩阵的数据变换处理的结构，上述 MDS 矩阵执行分支数为 m 以上的扩散变换、例如最优扩散变换

ODM(Optimal Diffusion Mappings)，并且，具体地说，在输入数据是 n 比特数据的情况下，是执行应用了由在 GF(2) 上定义的 n 次既约多项式 p(x) 定义的扩展域 GF(2^n) 上的矩阵的数据变换处理的结构。

[0256] 此外，本发明所涉及的数据变换装置可具体化为执行之前所说明的共用密钥块密码处理的装置，例如，能够在进行应用了

[0257] (a)SPN(Substitution Permutation Network) 结构、

[0258] (b)Feistel 结构、

[0259] (c) 扩展 Feistel 结构

[0260] 这些结构的密码处理的装置中的非线性变换部中应用上述数据变换装置。此外，除了密码处理以外，还能够在哈希函数等进行非线性变换的运算装置中应用本发明的结构。

[0261] [4. 密码处理装置的结构例]

[0262] 最后，在图 19 中示出以作为密码处理装置的 IC 模块 700 作为执行按照上述的实施例的数据变换处理的装置例的结构例。例如能够在 PC、IC 卡、读写器、其它各种信息处理装置中执行上述处理，图 19 所示的 IC 模块 700 能够构成在这些各种设备中。

[0263] 图 19 所示的 CPU(Central processing Unit :中央处理单元)701 是执行密码处理的开始、结束、数据的发送接收的控制、各结构部间的数据传送控制、其它各种程序的处理器。存储器 702 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 CPU701 所执行的程序、或运算参数等固定数据，上述 RAM 作为在 CPU701 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 702 能够作为密码处理中所需的密钥数据、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损害 (tamper) 结构的存储器。

[0264] 密码处理部 703 例如执行按照应用了上述各种密码处理结构、即

[0265] (a)SPN(Substitution Permutation Network) 结构、

[0266] (b)Feistel 结构、

[0267] (c) 扩展 Feistel 结构

[0268] 这些各结构中的任一个结构的共用密钥块密码处理算法的密码处理、解密处理，并且执行应用了哈希函数的运算处理等。

[0269] 另外，作为执行与上述的实施例对应的非线性变换处理的结构、即 n 比特输入输出 S 盒的结构，密码处理部 703 具有执行如下非线性变换处理的结构 :利用执行小于 n 的输入输出比特的非线性变换的较小的 S 盒执行非线性变换，将其结果输入到 MDS 矩阵等分支数较高的扩散变换矩阵并执行应用了矩阵的变换，对其变换结果进一步应用执行小于 n 的输入输出比特的非线性变换的较小的 S 盒来执行非线性变换而得到 n 比特的非线性变换结果。

[0270] 此外，在此，示出将密码处理单元设为单独的模块的例子，但是也可以不设置这种独立的密码处理模块，而构成为例如将密码处理程序保存到 ROM 中，由 CPU701 读取 ROM 保存程序来执行。

[0271] 随机数产生器 704 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。

[0272] 发送接收部 705 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。

[0273] 该 IC 模块 700 具有执行处理的结构，上述处理为应用了按照上述的实施例的作为非线性变换处理部的 S 盒的处理、即应用了具有参照图 13 ～图 18 所说明的结构的 S 盒的非线性变换处理。

[0274] 以上，参照特定的实施例详细说明了本发明。然而，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、代用是显而易见的。即，以例示的形式公开了本发明，并不是限定性地解释本发明。要判断本发明的要旨，需要参考权利要求书范围一栏。

[0275] 此外，在说明书中说明的一系列处理能够通过硬件、或软件、或两者的合成结构来执行。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、或者将程序安装到可执行各种处理的通用计算机中执行。

[0276] 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(Digital Versatile 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。能够将这种可移动记录介质作为所谓的封装软件进行提供。

[0277] 此外，除了从如上所述的可移动记录介质将程序安装到计算机之外，还能够从下载站点无线传送到计算机、或通过称为 LAN(Local Area Network：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过来的程序并安装到内置的硬盘等记录介质中。

[0278] 此外，说明书中记载的各种处理，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。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。

[0279] 产业上的可利用性

[0280] 如上所述，根据本发明的一个实施例的结构，例如将在共用密钥块密码处理、哈希函数等处理中执行的非线性变换处理设为进行应用了第一级非线性变换部、线性变换部以及第二级非线性变换部的数据变换的结构，其中，上述第一级非线性变换部利用多个较小的 S 盒 (S-box) 执行非线性变换，上述线性变换部输入来自第一级非线性变换部的所有输出，执行线性变换，上述第二级非线性变换部由执行分割线性变换部的输出数据得到的各分割数据的非线性变换处理的多个小型非线性变换部构成，在线性变换部中设为执行应用了进行最优扩散变换的矩阵的数据变换的结构，因此能够不使从数据的输入起直到输出的关键路径过大，而实现适当的数据扩散，实现对各种密码攻击的抵抗性较强的安全性较高的数据变换。

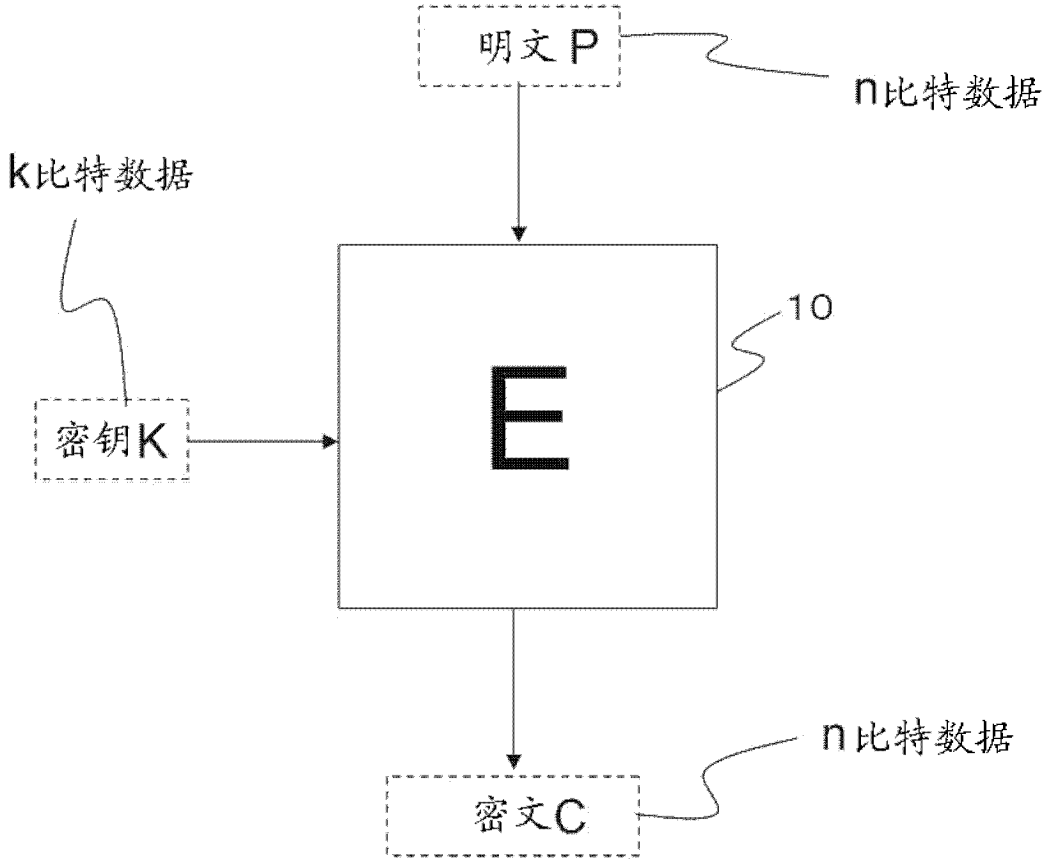


图 1

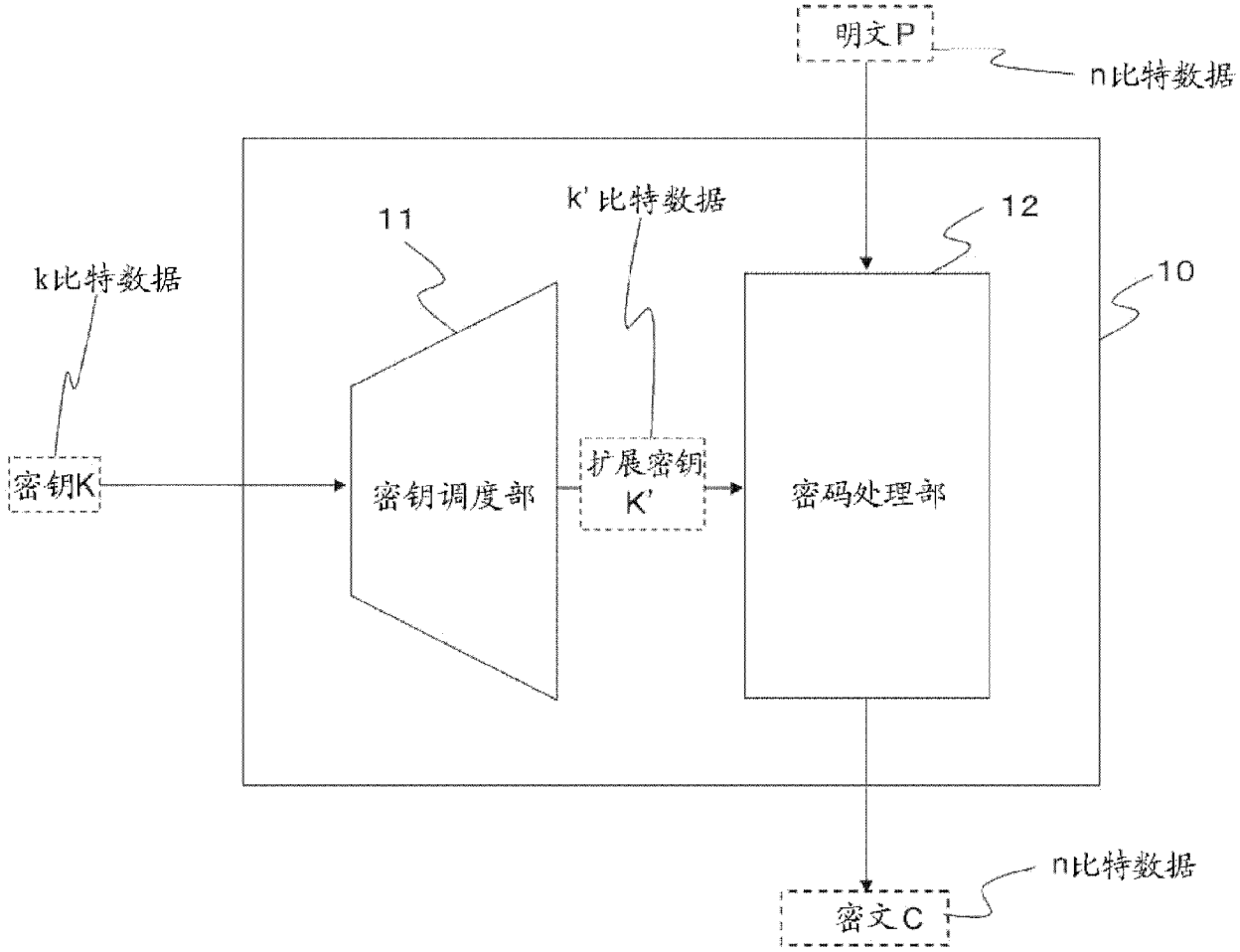

明文P
n比特数据
11
k'比特数据
12
k比特数据
10
密钥K
密钥调度部
扩展密钥K'
密码处理部
n比特数据
密文C

图 2

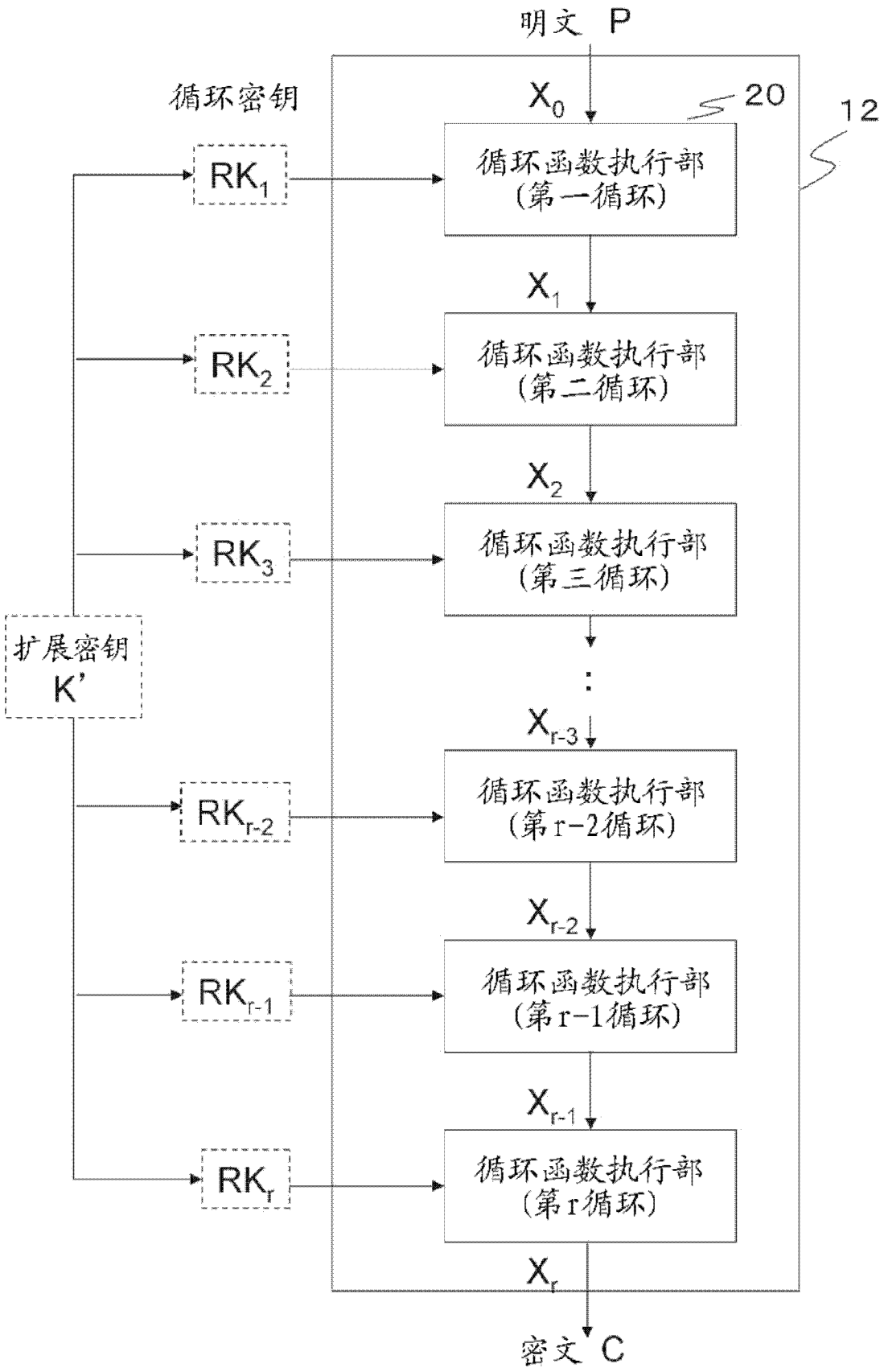

明文 P
循环密钥
X_0
20
12
循环函数执行部
(第一循环)
RK_1
X_1
循环函数执行部
(第二循环)
RK_2
X_2
循环函数执行部
(第三循环)
RK_3
扩展密钥
K'
X_{r-3}
循环函数执行部
(第r-2循环)
RK_{r-2}
X_{r-2}
循环函数执行部
(第r-1循环)
RK_{r-1}
X_{r-1}
循环函数执行部
(第r循环)
RK_r
X_r
密文 C

图 3

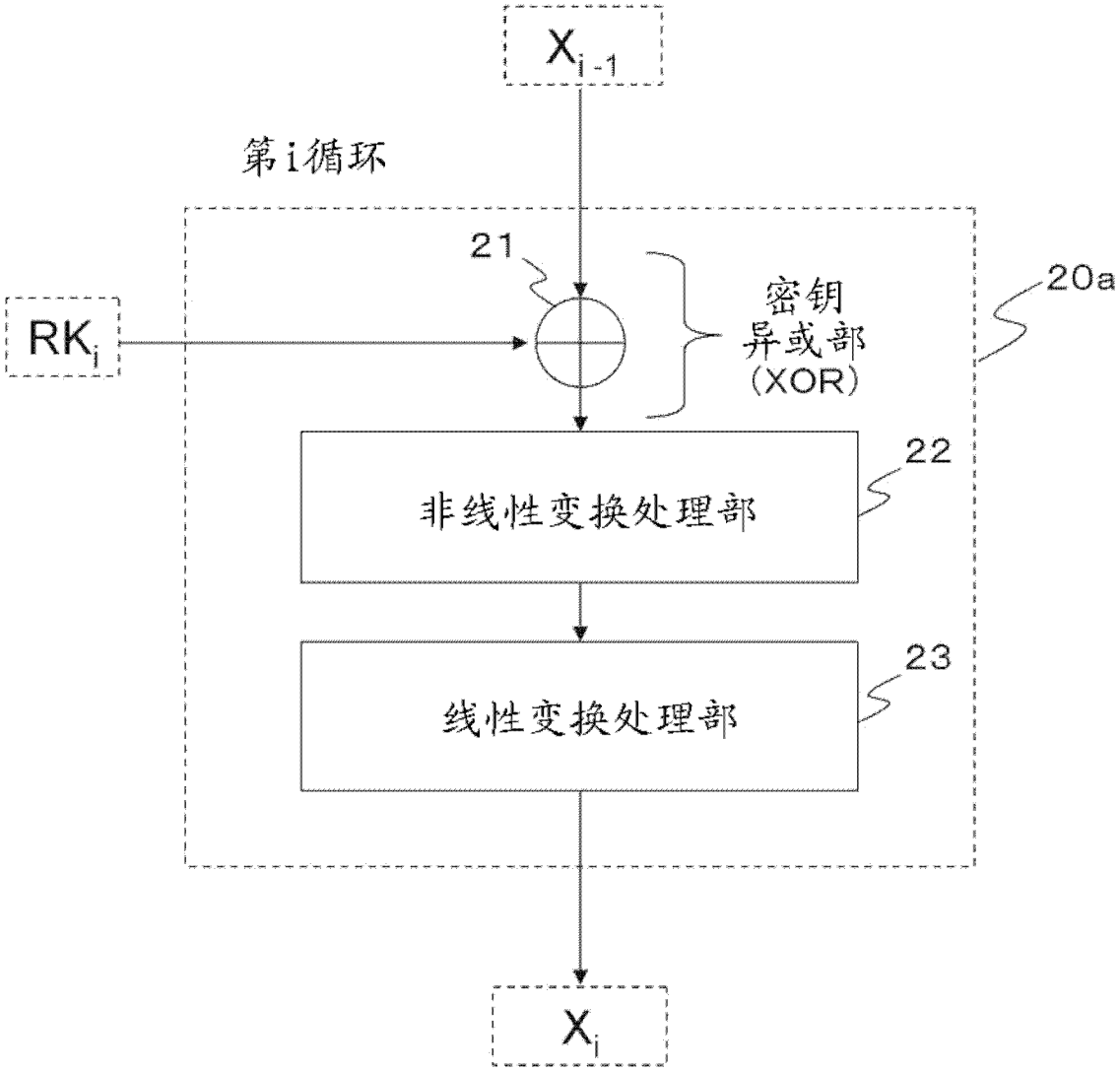


图 4

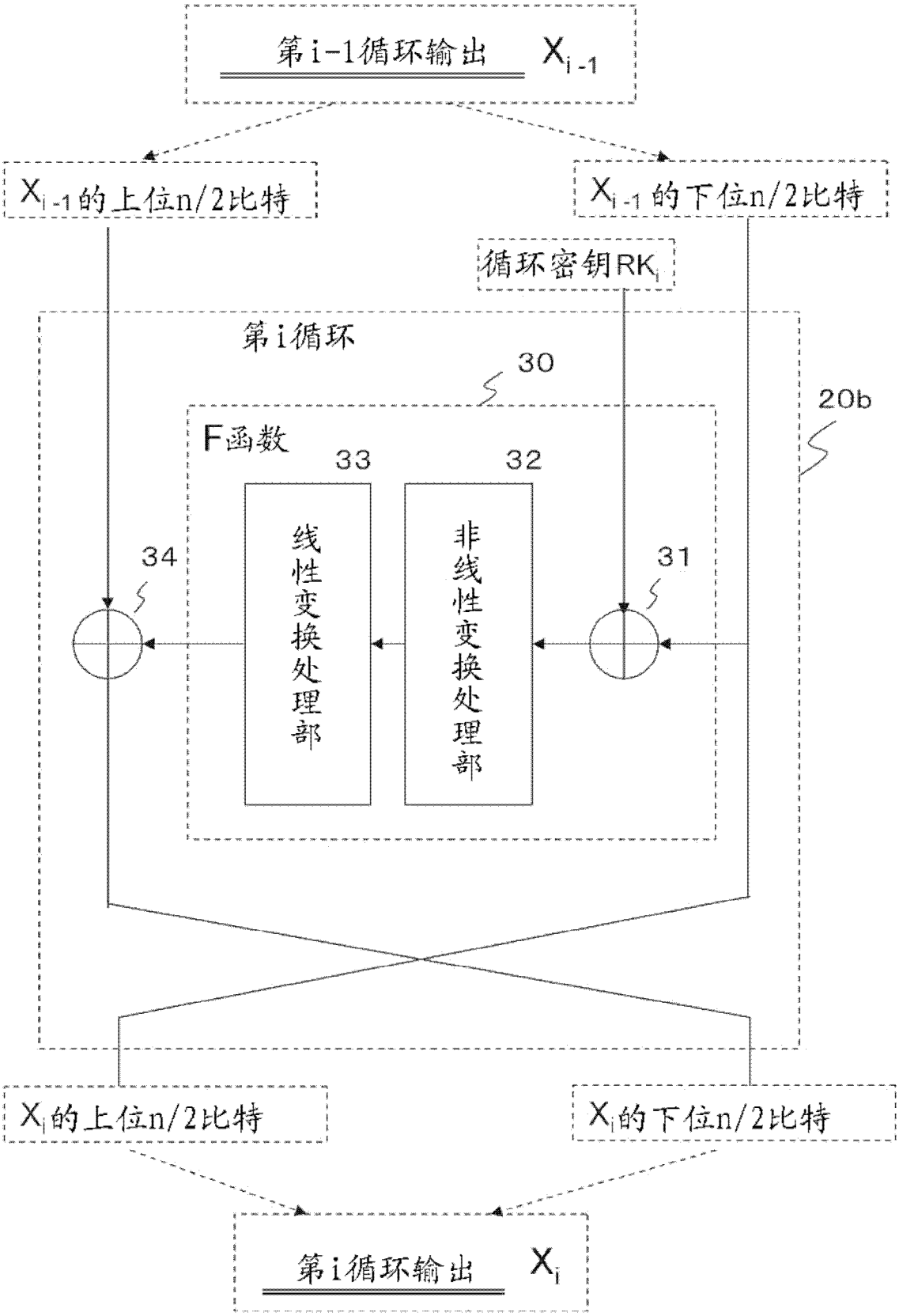

第i-1循环输出 X_{i-1}
X_{i-1}的上位n/2比特
X_{i-1}的下位n/2比特
循环密钥RK_i
第i循环
30
20b
F函数
33
32
34
31
线性变换处理部
非线性变换处理部
X_i的上位n/2比特
X_i的下位n/2比特
第i循环输出 X_i

图 5

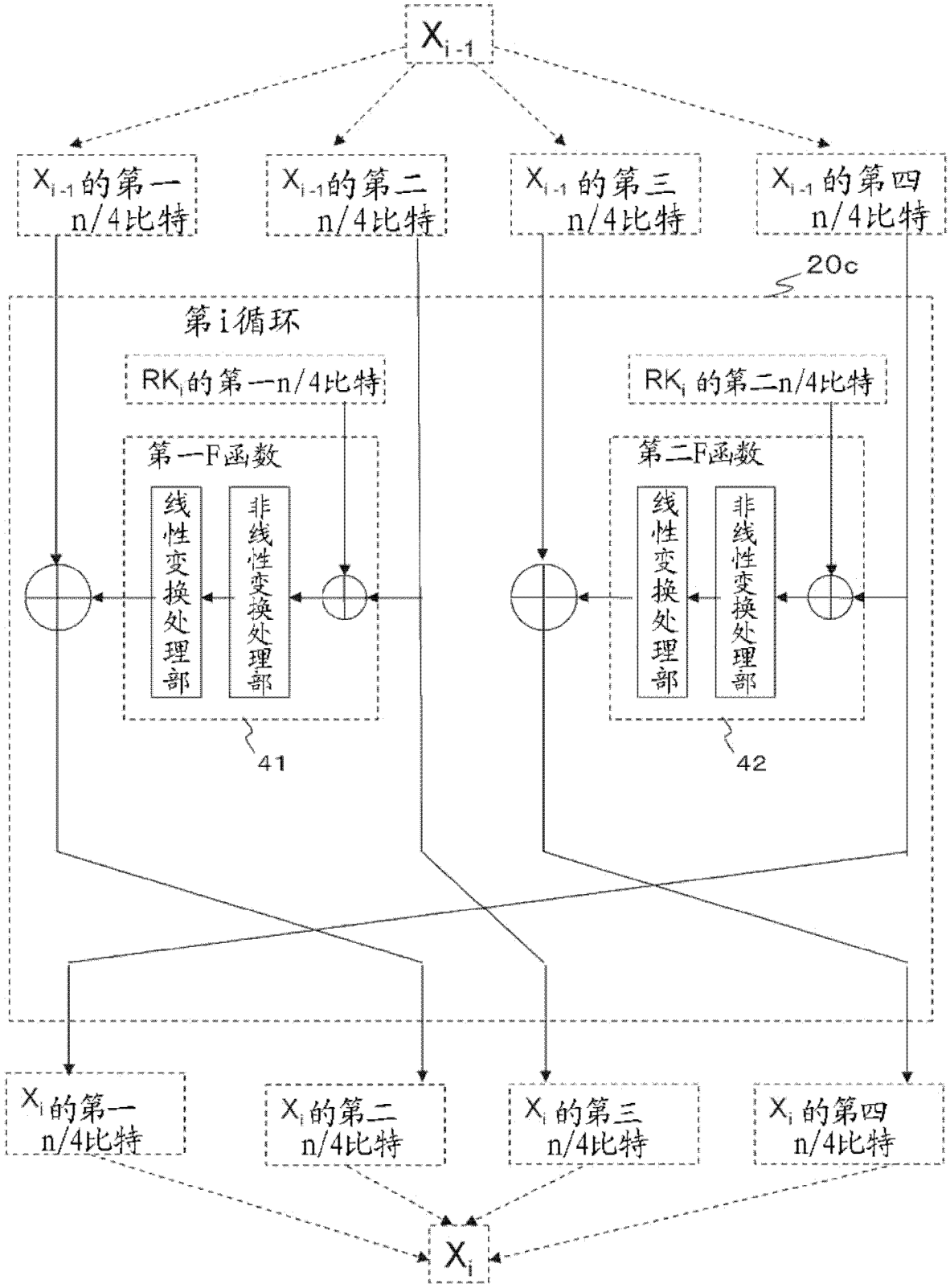

X_{i-1}
X_{i-1}的第一 n/4比特
X_{i-1}的第二 n/4比特
X_{i-1}的第三 n/4比特
X_{i-1}的第四 n/4比特
20c
第i循环
RK_i的第一n/4比特
RK_i的第二n/4比特
第一F函数
第二F函数
线性变换处理部
非线性变换处理部
线性变换处理部
非线性变换处理部
41
42
X_i的第一 n/4比特
X_i的第二 n/4比特
X_i的第三 n/4比特
X_i的第四 n/4比特
X_i

图 6

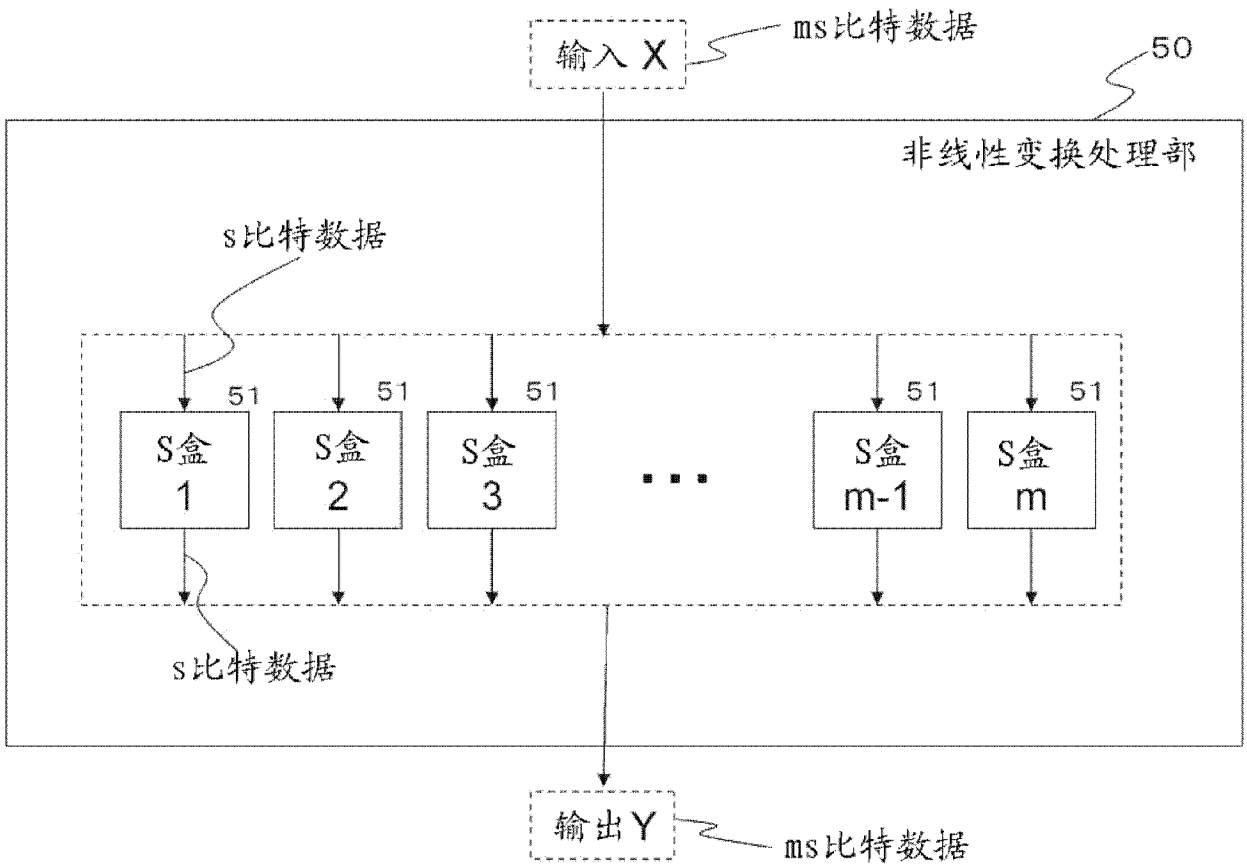

输入 X
ms比特数据
50
非线性变换处理部
s比特数据
51
S盒 1
S盒 2
S盒 3
S盒 m-1
S盒 m
s比特数据
输出Y
ms比特数据

图 7

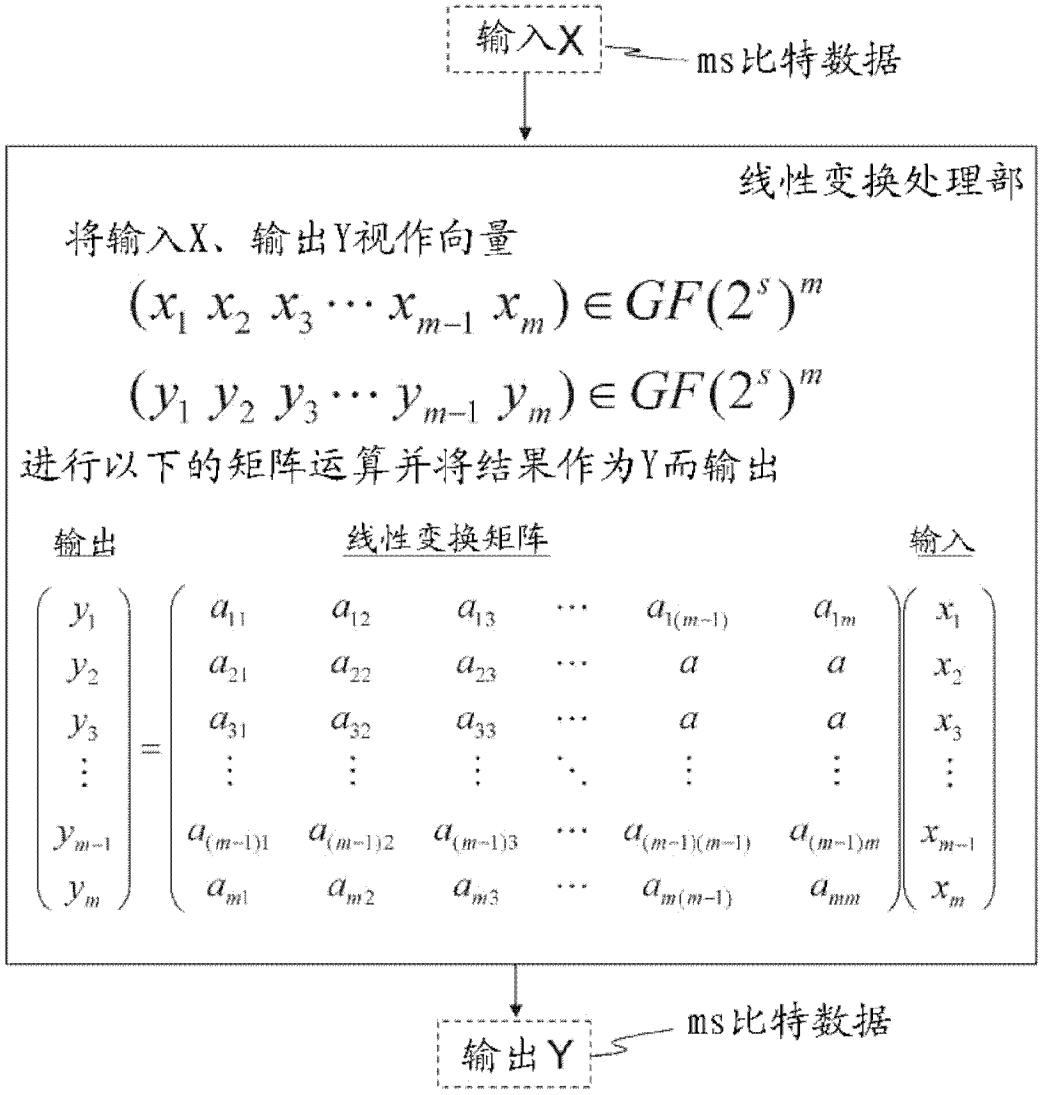

输入X
ms比特数据
线性变换处理部
将输入X、输出Y视作向量
$(x_1\ x_2\ x_3 \cdots x_{m-1}\ x_m) \in GF(2^s)^m$
$(y_1\ y_2\ y_3 \cdots y_{m-1}\ y_m) \in GF(2^s)^m$
进行以下的矩阵运算并将结果作为Y而输出
输出
线性变换矩阵
输入
$\begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ \vdots \\ y_{m-1} \\ y_m \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1(m-1)} & a_{1m} \\ a_{21} & a_{22} & a_{23} & \cdots & a & a \\ a_{31} & a_{32} & a_{33} & \cdots & a & a \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{(m-1)1} & a_{(m-1)2} & a_{(m-1)3} & \cdots & a_{(m-1)(m-1)} & a_{(m-1)m} \\ a_{m1} & a_{m2} & a_{m3} & \cdots & a_{m(m-1)} & a_{mm} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_{m-1} \\ x_m \end{pmatrix}$
输出Y
ms比特数据

图 8

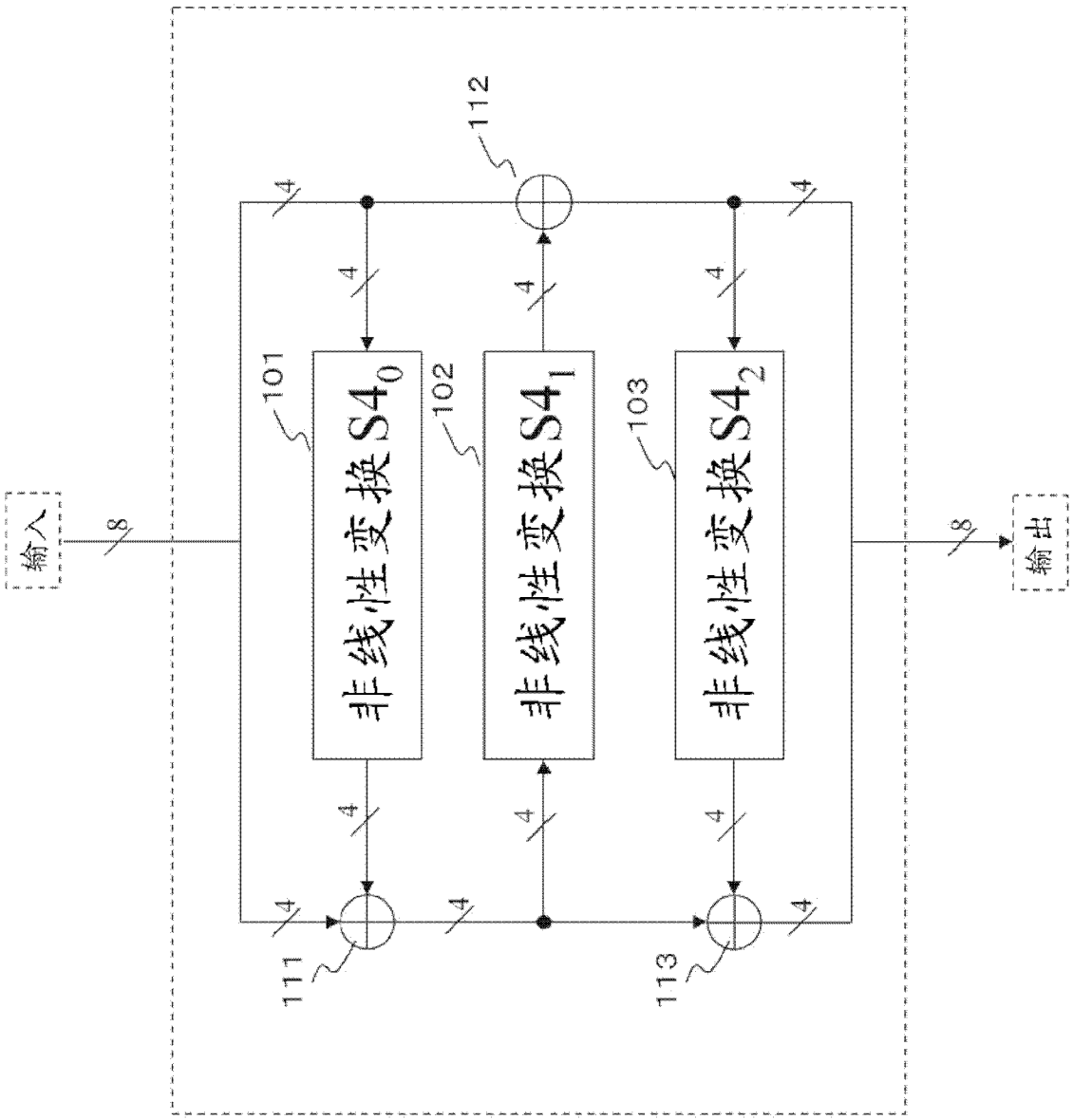


图 9

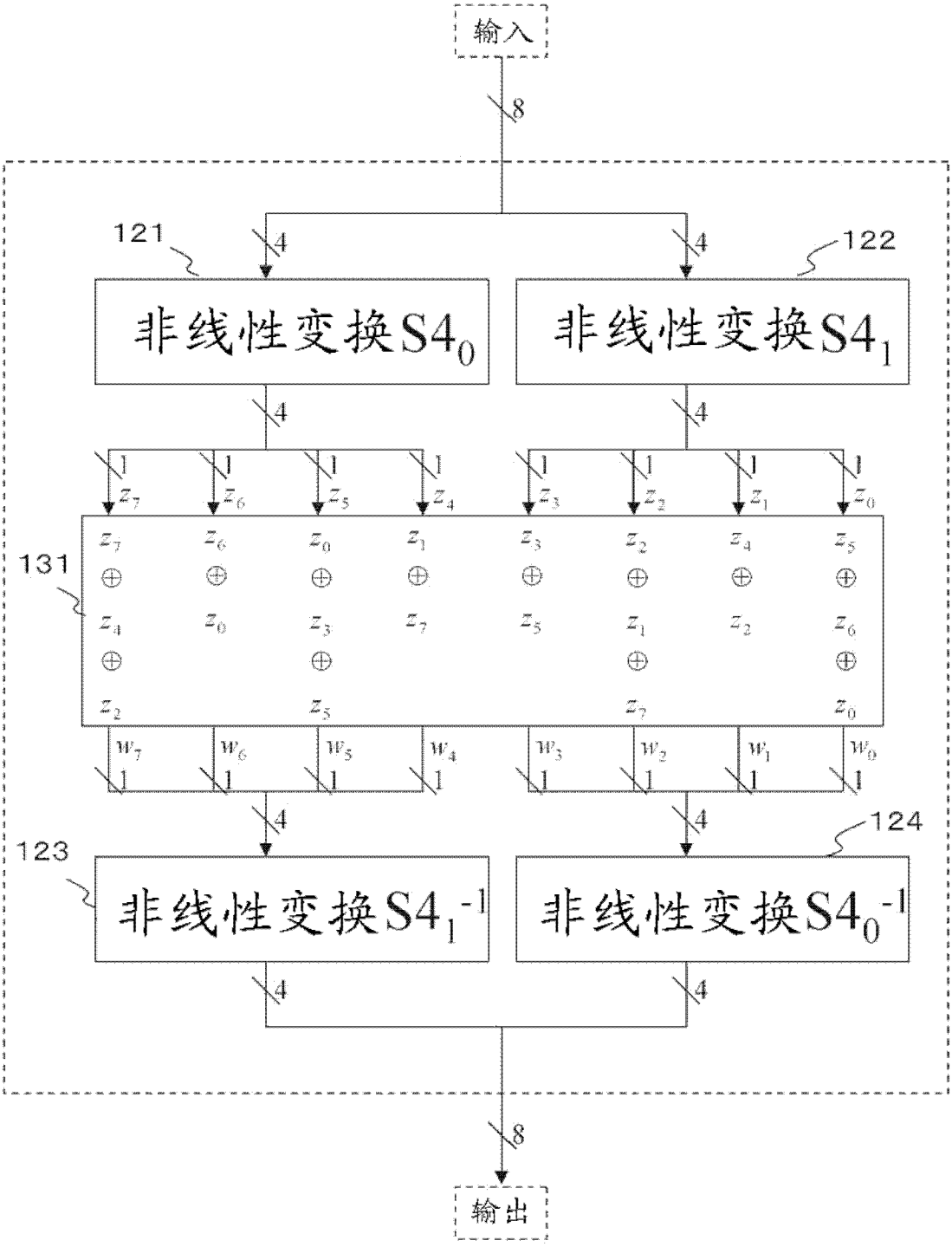

输入
8
121
122
4
非线性变换S4$_0$
非线性变换S4$_1$
131
123
124
非线性变换S4$_1^{-1}$
非线性变换S4$_0^{-1}$
输出

图 10

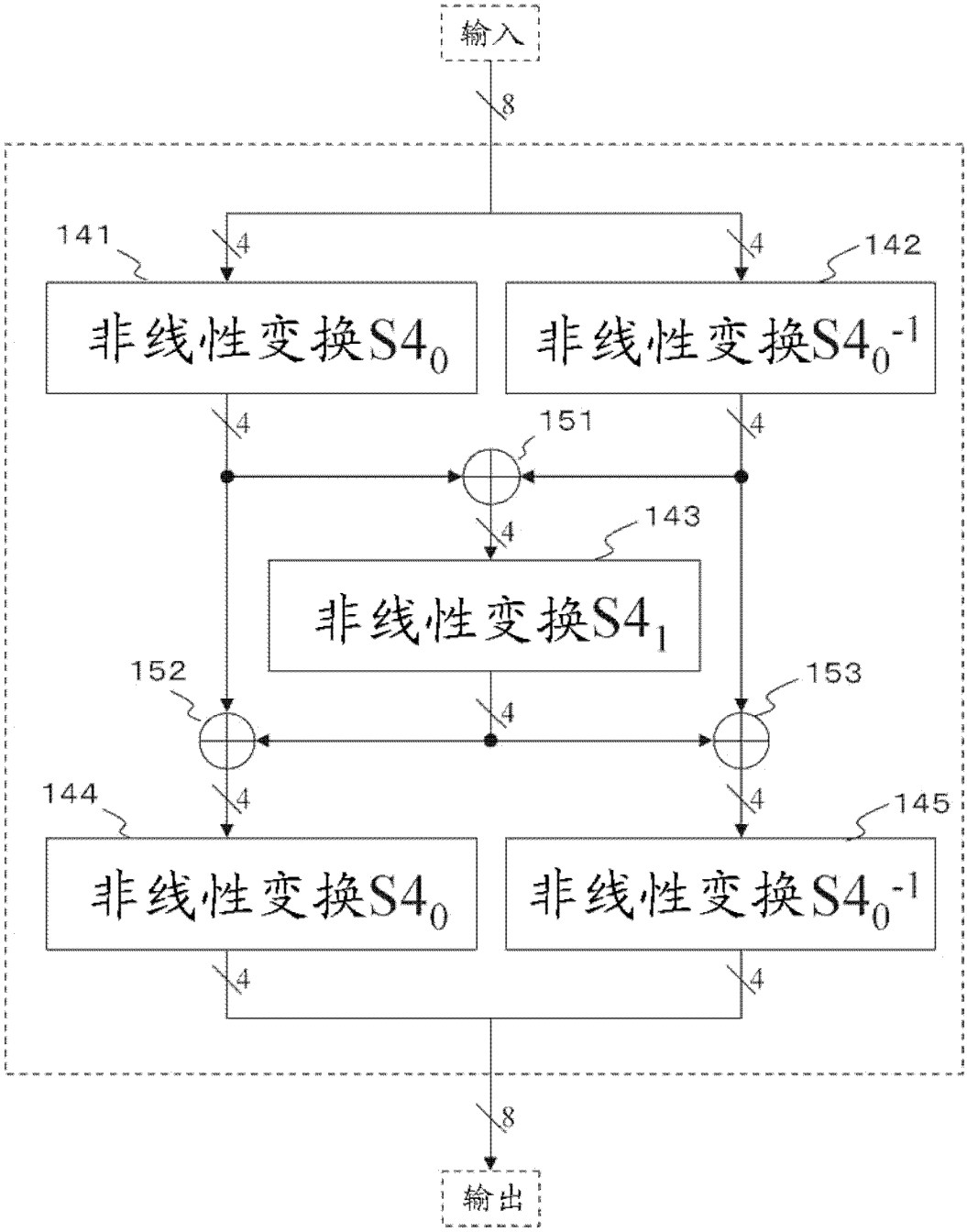

输入
8
141
4
4
142
非线性变换S4$_0$
非线性变换S4$_0^{-1}$
4
151
4
143
4
非线性变换S4$_1$
152
153
4
144
4
4
145
非线性变换S4$_0$
非线性变换S4$_0^{-1}$
4
4
8
输出

图 11

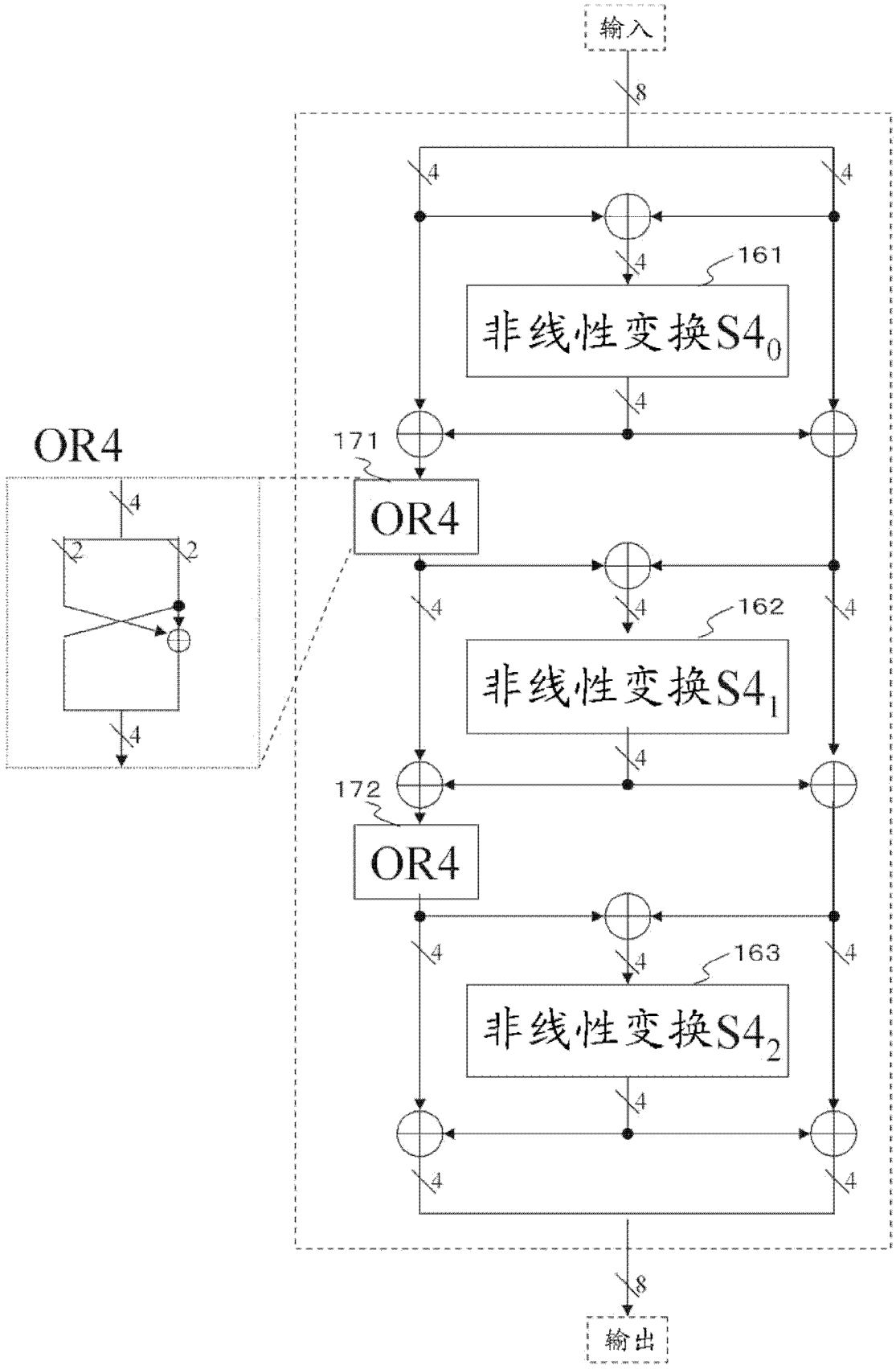

输入
8
4
4
4
161
非线性变换S4$_0$
4
OR4
171
OR4
4
2
2
4
4
4
4
162
非线性变换S4$_1$
4
172
OR4
4
4
4
163
非线性变换S4$_2$
4
4
4
4
8
输出

图 12

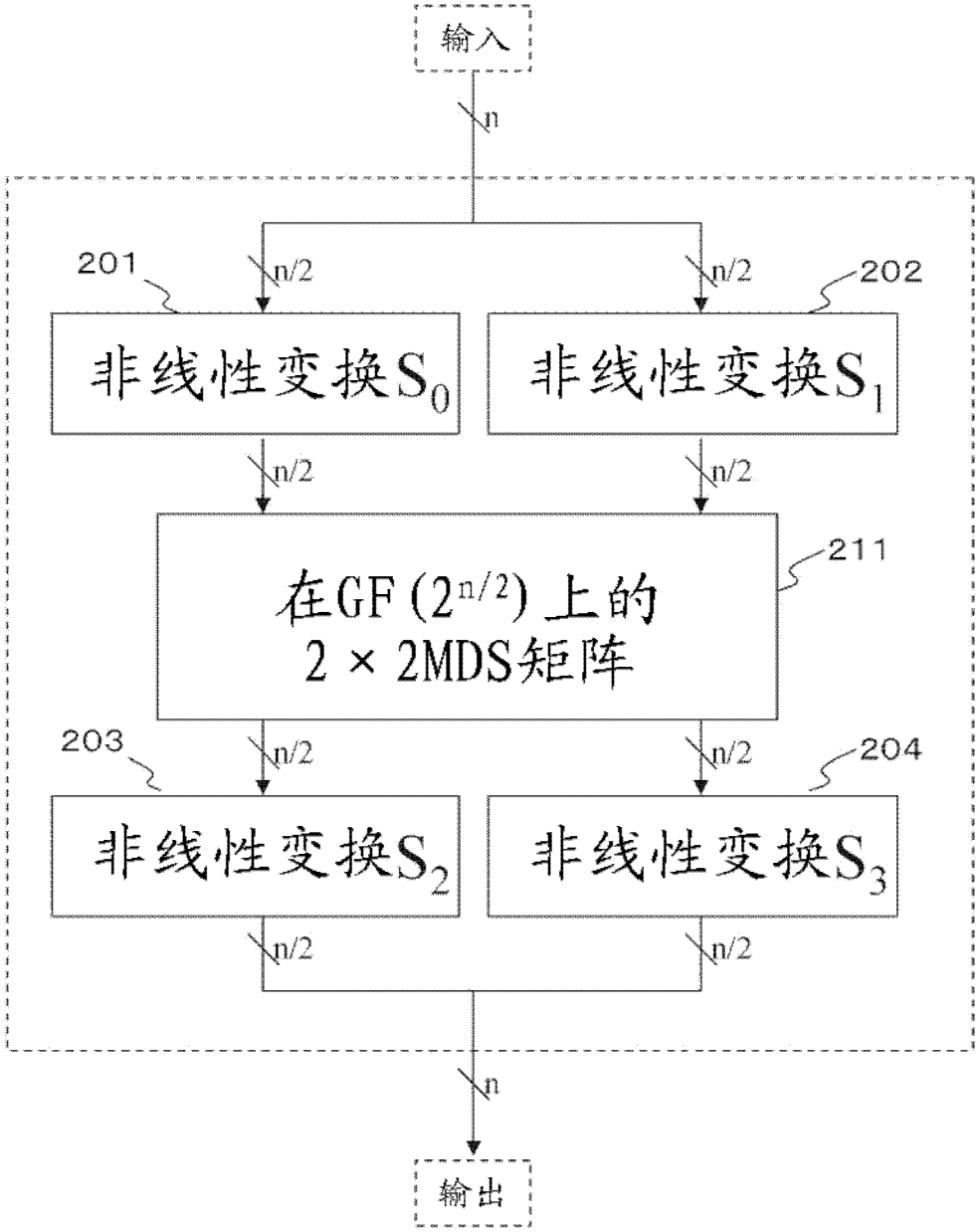
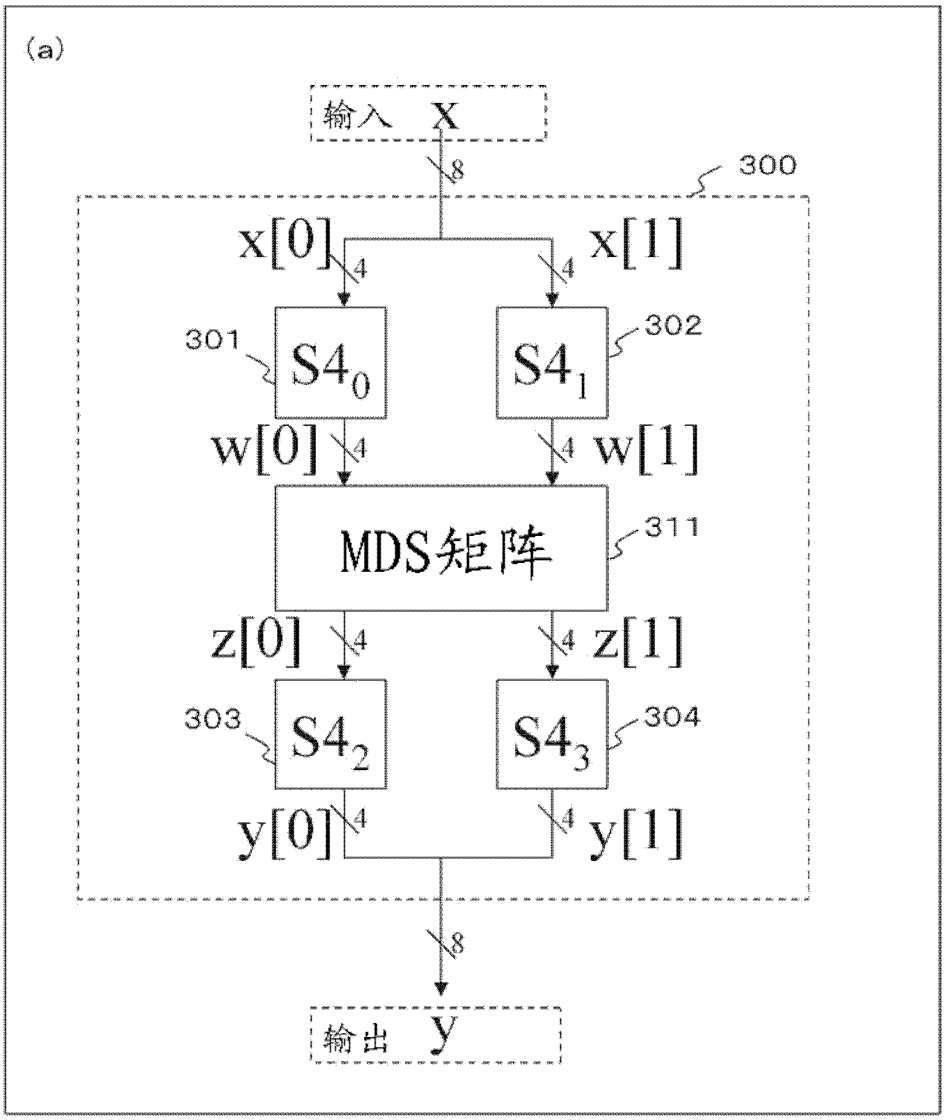

输入
n
201
n/2
n/2
202
非线性变换S_0
非线性变换S_1
n/2
n/2
211
在GF($2^{n/2}$)上的
2 × 2MDS矩阵
203
n/2
n/2
204
非线性变换S_2
非线性变换S_3
n/2
n/2
n
输出

图 13



(b)

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

图 14

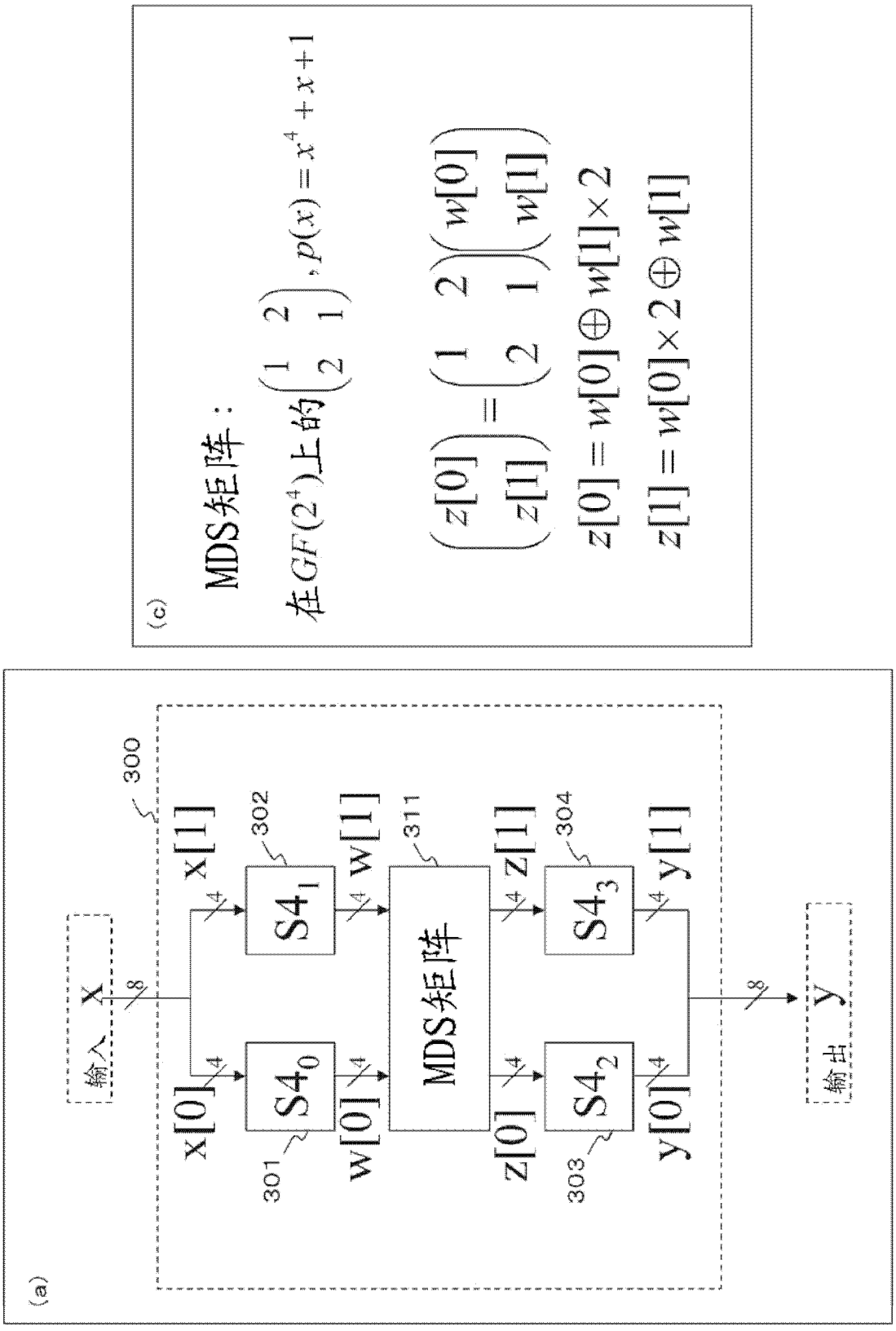
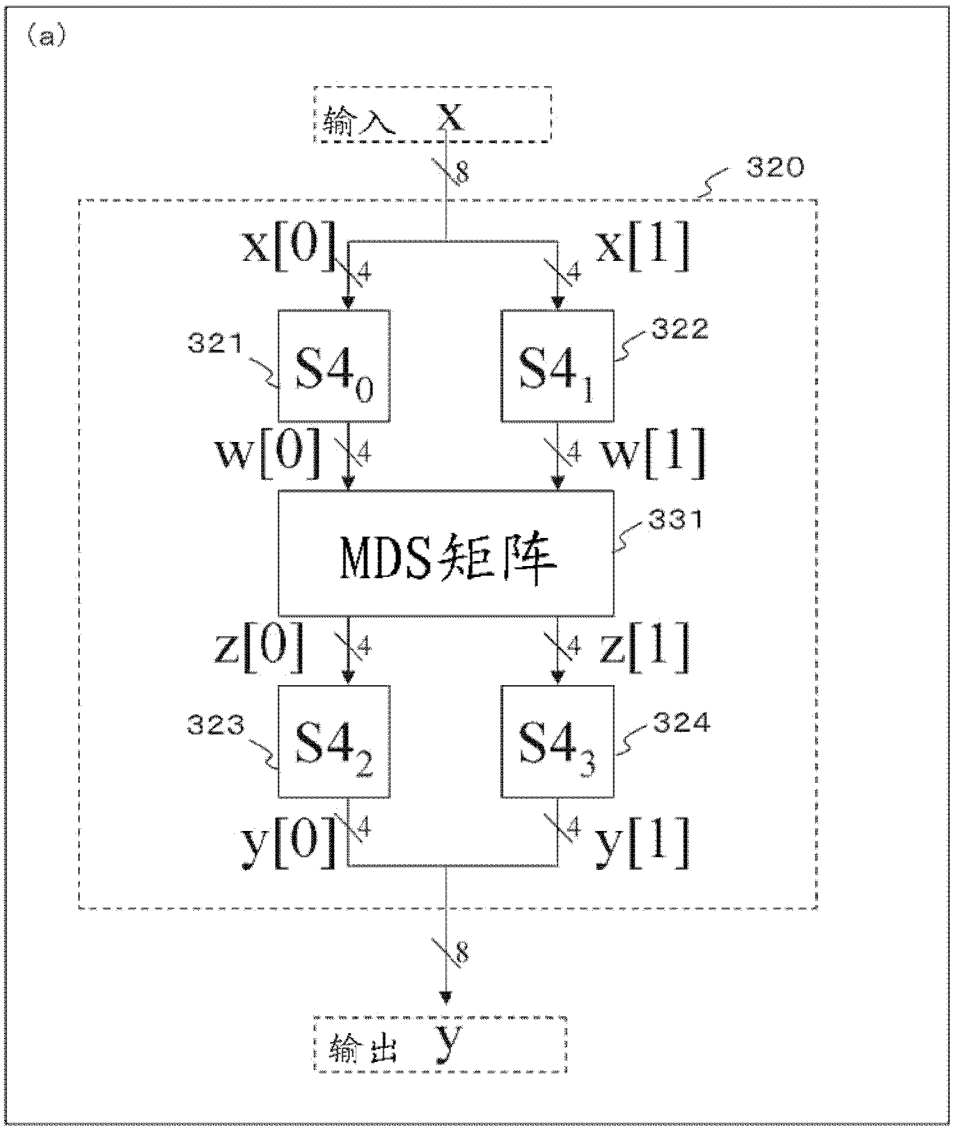

(c)
MDS矩阵：
在$GF(2^4)$上的$\begin{pmatrix}1 & 2\\ 2 & 1\end{pmatrix}$，$p(x)=x^4+x+1$
$\begin{pmatrix}z[0]\\ z[1]\end{pmatrix}=\begin{pmatrix}1 & 2\\ 2 & 1\end{pmatrix}\begin{pmatrix}w[0]\\ w[1]\end{pmatrix}$
$z[0]=w[0]\oplus w[1]\times 2$
$z[1]=w[0]\times 2\oplus w[1]$
(a)
300
输入 X
8
x[0]
x[1]
4
S4$_0$
S4$_1$
301
302
w[0]
w[1]
MDS矩阵
311
z[0]
z[1]
S4$_2$
S4$_3$
303
304
y[0]
y[1]
输出 Y

图 15



(b)

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

图 16

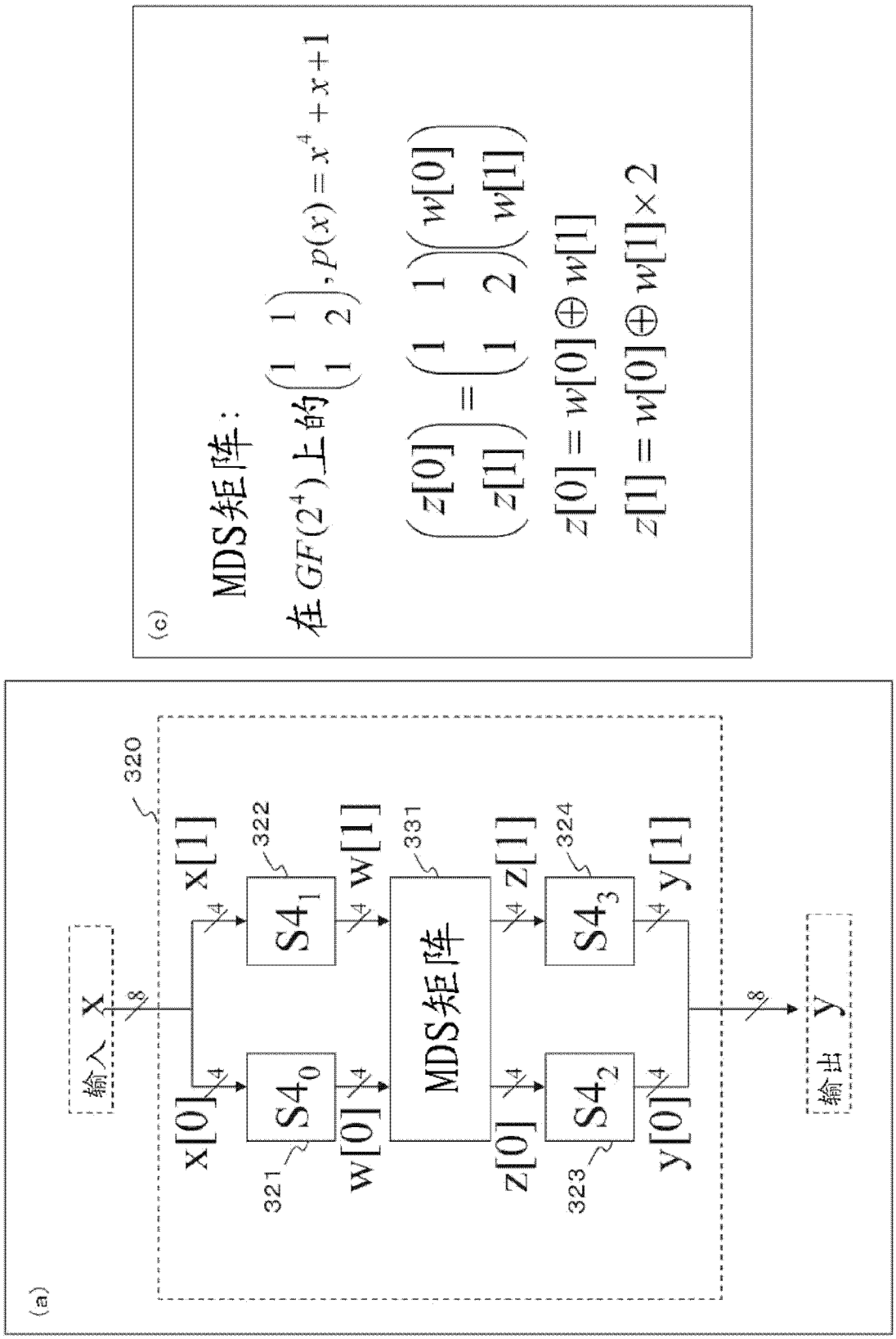

(c)
MDS矩阵：
在 $GF(2^4)$ 上的 $\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$，$p(x) = x^4 + x + 1$
$\begin{pmatrix} z[0] \\ z[1] \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} w[0] \\ w[1] \end{pmatrix}$
$z[0] = w[0] \oplus w[1]$
$z[1] = w[0] \oplus w[1] \times 2$
(a)
输入 X
8
320
x[0]
x[1]
4
S4$_0$
S4$_1$
321
322
w[0]
w[1]
MDS矩阵
331
z[0]
z[1]
S4$_2$
S4$_3$
323
324
y[0]
y[1]
输出 Y

图 17

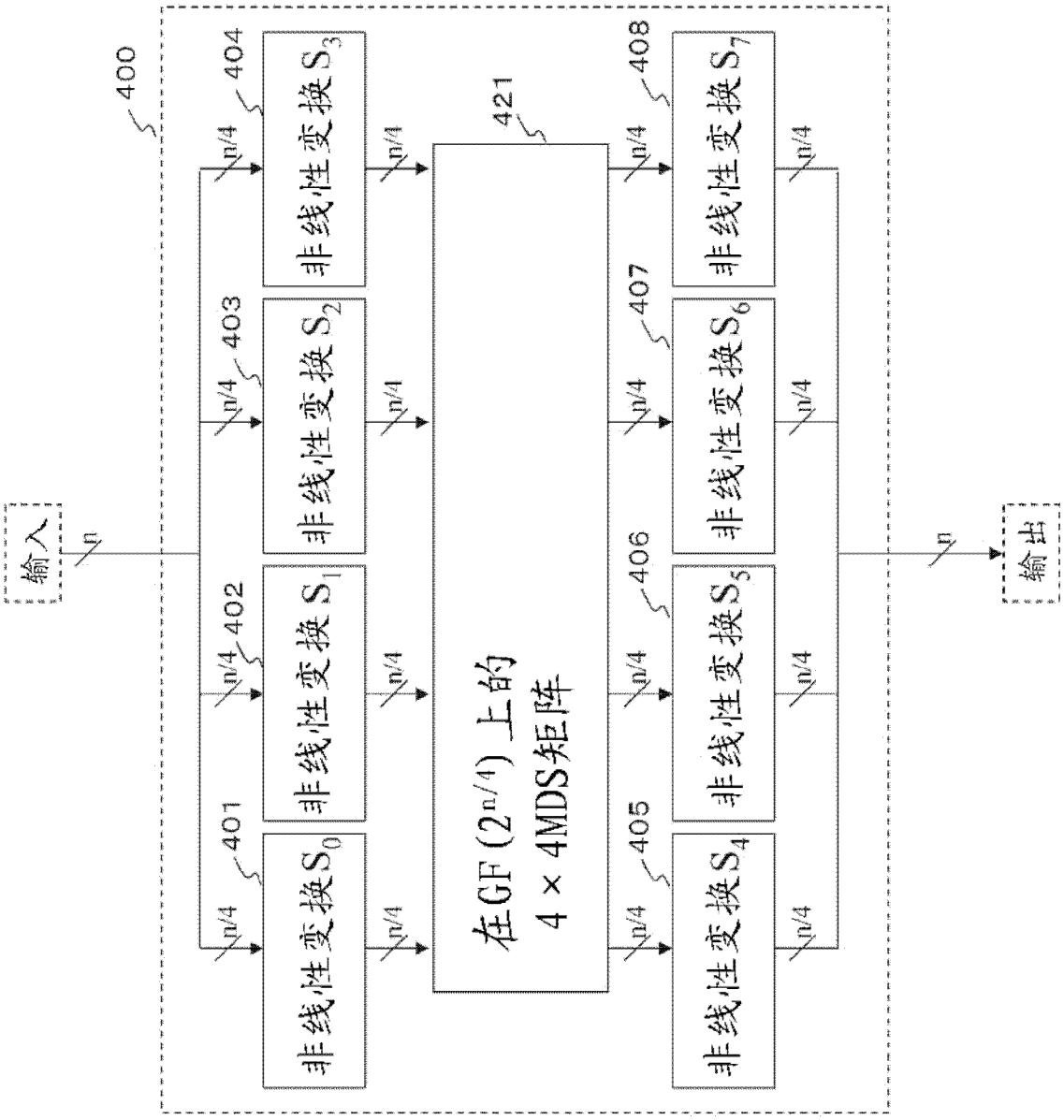

400
输入
n
非线性变换 S_0
非线性变换 S_1
非线性变换 S_2
非线性变换 S_3
非线性变换 S_4
非线性变换 S_5
非线性变换 S_6
非线性变换 S_7
401
402
403
404
405
406
407
408
n/4
421
在GF $(2^{n/4})$ 上的
4 × 4MDS矩阵
n
输出

图 18

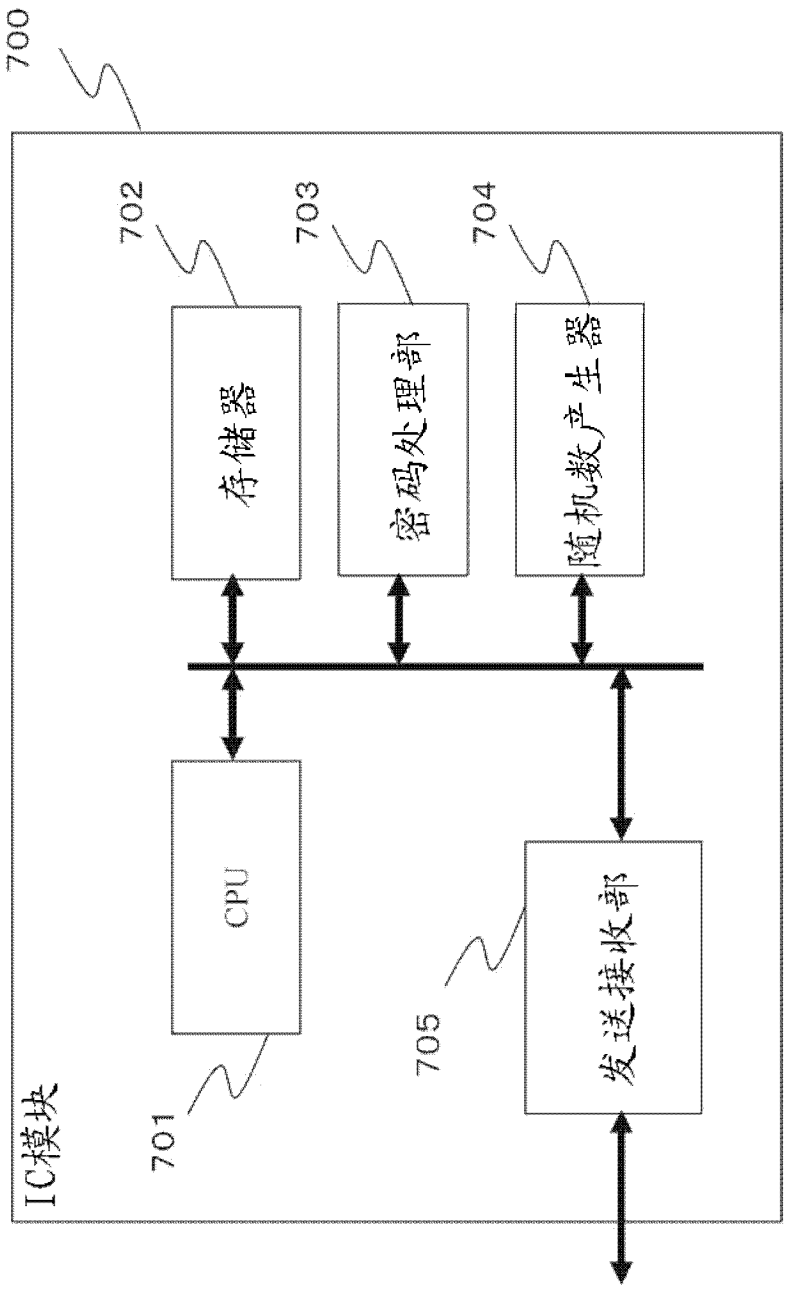


图 19