[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G09C 1/00 (2006.01)

[12] 发明专利说明书

专利号 ZL 200510096622.X

[45] 授权公告日 2010 年 1 月 20 日

[11] 授权公告号 CN 100583192C

[22] 申请日 2001.3.8
[21] 申请号 200510096622.X
分案原申请号 01800470.9
[30] 优先权
[32] 2000. 3. 9 [33] JP [31] 64614/00
[73] 专利权人 三菱电机株式会社
地址 日本东京都
共同专利权人 日本电信电话株式会社
[72] 发明人 松井充 时田俊雄 中岛纯子
神田雅透 盛合志帆 青木和麻吕
[56] 参考文献
JP9 - 269727A 1997.10.14
CN1199969A 1998.11.25
WO9709705A1 1997.3.13
审查员 吴 娟

[74] 专利代理机构 中国专利代理(香港)有限公司
代理人 刘宗杰

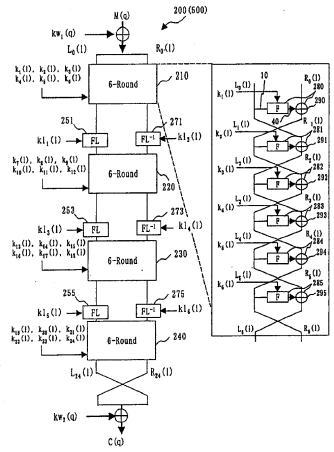
权利要求书 2 页 说明书 33 页 附图 47 页

[54] 发明名称

数据变换装置和数据变换方法

[57] 摘要

可将加密部 200 和解密部 500 兼用同一电路。以非线性数据变换部 200 为中心而将数据正变换部(FL)251 与数据逆变换部(FL^{-1})273 设置成点对称位置，并且通过以非线性数据变换部 220 为中心而将数据正变换部(FL)251 与数据逆变换部(FL^{-1})273 设置成点对称位置而可将加密部 200 和解密部 500 以同一电路来加以构成。



1. 一种数据变换装置，包括：密钥产生部，根据输入密钥数据 K 产生输出密钥数据；及数据处理部，根据上述输出密钥数据至少执行数据的加密和数据的解密中的一种，

其特征在于：

上述密钥产生部包括：

第一 G 位密钥变换部，将基于所述输入密钥数据 K 而生成的 G 位密钥数据变换成 G 位的第一 G 位密钥数据；及

第二 G 位密钥变换部，被输入所述第一 G 位密钥数据，将所述第一 G 位密钥数据变换成 G 位的第二 G 位密钥数据；并且

在上述密钥产生部，当输入密钥数据 K 为 G 位的情况下，通过由上述第一 G 位密钥变换部对上述 G 位的密钥数据进行变换，由此生成第一 G 位密钥数据 K_1，而将上述第一 G 位密钥数据 K_1 作为输出密钥数据输出；

在输入密钥数据 K 为 2G 位的情况下，由上述第一 G 位密钥变换部对上述 G 位的密钥数据进行变换，由此，生成第一 G 位密钥数据 K_1，通过由上述第二 G 位密钥变换部对上述第一 G 位密钥数据 K_1 进行变换，生成 G 位的第二密钥数据 K_2，将上述第一 G 位密钥数据 K_1 和上述第二 G 位密钥数据 K_2 予以连结，以将上述连结后的 2G 位的密钥数据作为上述输出密钥数据进行输出。

2. 如权利要求 1 所述的数据变换装置，其特征在于，

上述第一 G 位密钥变换部包括：

2 段非线性数据变换部，将 G 位密钥数据做非线性变换；及

逻辑运算部，执行自 2 段非线性数据变换部所输出的变换途中的 G 位密钥数据与输入到上述第一 G 位变换部的密钥数据 K 的逻辑运算。

3. 如权利要求 1 所述的数据变换装置，其特征在于，

上述密钥产生部进而包括：位长度变换部，在输入 Q 位的密钥数据的情况下，将 Q 位的密钥数据变换成 2G 位的密钥数据，其中 Q 为 $G < Q < 2G$。

4. 一种数据变换方法，包括：密钥产生步骤，根据输入密钥数据

K产生输出密钥数据；及数据处理步骤，根据上述输出密钥数据至少执行数据的加密和数据的解密中的一种，

其特征在于：

上述密钥产生步骤包括：

第一G位密钥变换步骤，将根据所述输入密钥数据K生成的G位密钥数据变换成G位的第一G位密钥数据；及

第二G位密钥变换步骤，输入上述第一G位密钥数据，将所述第一G位密钥数据变换成G位的第二G位密钥数据；并且

在上述密钥产生步骤，当输入密钥数据K为G位的情况下，通过由上述第一G位密钥变换步骤对上述G位密钥数据进行变换，由此生成第一G位密钥数据K_1，而将上述第一G位密钥数据K_1作为上述输出密钥数据输出；

在输入密钥数据K为2G位的情况下，由上述第一G位密钥变换步骤对上述G位密钥数据进行变换，由此，生成第一G位密钥数据K_1，通过由上述第二G位密钥变换步骤对上述第一G位密钥数据K_1进行变换，生成G位的第二G位密钥数据K_2，将上述第一G位密钥数据K_1和上述第二G位密钥数据K_2予以连结，以将上述连结后的2G位的密钥数据作为上述输出密钥数据进行输出。

数据变换装置和数据变换方法

本申请是下述申请的分案申请：
发明名称：数据变换装置和数据变换方法以及记录用以在计算机上执行数据变换方法的程序的计算机可读取存储媒体
申请号：01800470.9
国际申请号：PCT/JP01/01796
国际申请申请日：2001 年 3 月 8 日
最早的优先权日：2000 年 3 月 9 日

技术领域

本发明是在信息通信等，有关于做为保护数字信息的加密及解密及数据扩散等的数据变换装置和数据变换方法以及记录数据变换方法的记录媒体。

背景技术

图 25 是显示使用在记载于“现代暗号理论”（社团法人电子情报通信学会、平成 9 年 11 月 15 日发行、46 页）的现有的 DES 加密的加密函数的图。

如图 25 所示，设置有 8 个 S 盒。该 8 个 S 盒是分别为不同的表。各表是从 6 位的输入数据来输出 4 位的输出数据。

图 26 是显示记载于“Specification of E2 - a 128 - bit Block Cipher”（Nippon Telegraph and Telephone Corporation, June 14, 1998、10 页）的非线性变换函数的图。

如图 26 所示，于各 S 函数部是设置有 8 个 S 盒。

在现有的加密装置中，是设置多个 S 盒。因为在某一加密是准备分别为不同的表，所以存储容量为比起使用 1 个 S 盒的场合更为加大，而又因为在另外的加密只使用 1 个 S 盒，所以会有所谓安全性降低的问题。

而且，于如图 7 所示，在设置数据正变换部（FL）250 于加密部

的场合时，若无设置数据逆变换部（FL^{-1}）270 于解密部则无法解密。一般，因为数据正变换部（FL）250 与数据逆变换部（FL^{-1}）270 为不同的电路，所以会有所谓无法将加密部与解密部做成同一构成的课题。

而且，在产生扩展密钥的场合时，为了产生安全性更高的扩展密钥而需要复杂的操作。而且，当产生扩展密钥时，会有所谓以做为初期值被输入的密钥数据的位数必需为一定值的课题。

本发明是以提供可将加密用和解密用的电路做成同一个，而且在用以消减使用做为非线性函数计算的电路规模、程序大小、及存储器容量，来产生扩展密钥的场合时，可以简单的构成就可产生的系统做为目的。

发明的概述

本发明的数据变换装置包括：数据处理部，输入密钥数据而至少执行数据的加密和数据的解密的任一种的数据变换，其特征在于：上述数据处理部是将执行数据变换的数据分割为第一数据（L）和第二数据（R）而做数据变换；而且，上述数据处理部是包括：数据正变换部（FL），变换第一数据（L）；及数据逆变换部（FL^{-1}），将第二数据（R）做与上述数据正变换部（FL）的变换相反的变换。

其中，上述数据处理部具有：第一输入和第二输入；及第一输出和第二输出；上述数据正变换部（FL）将变换后的数据输出至数据处理部的第一输入；上述数据逆变换部（FL^{-1}）变换从数据处理部的第二输出所输出的数据予以输出。

其中，上述数据处理部具有：第一输入和第二输入；及第一输出和第二输出，上述数据正变换部（FL）将变换后的数据输出至数据处理部的第二输入，上述数据逆变换部（FL^{-1}）变换从数据处理部的第一输出所输出的数据予以输出。

本发明的数据变换装置包括：数据处理部，输入密钥数据而至少执行数据的加密和数据的解密的任一种的数据变换，其特征于：上述数据处理部包括：非线性变换部，将数据做非线性变换；非线性变换部是包括：第一变换部（s_1），将欲变换的数据的一部分数据输入做为第一部分数据，以使用可将输入后的数据的值变换成其他的值予以输

出的变换表 T 来变换第一部分数据，而输出变换后的数据；及第二变换部（s_2），将欲变换的数据的至少其他的一部分数据输入做为第二部分数据，以使用可使用上述变换表 T 的变换与第二部分用运算来变换第二部分数据，而输出变换后的数据。

其中，上述第一变换部（s_1）在变换表 T 输入数据 y_1 并输出数据 $s_1(y_1)$，并将该数据输出做为数据 $z_1 = s_1(y_1)$，上述第二变换部（s_2）在变换表 T 输入数据 y_2 并输出数据 $s_1(y_2)$，将以循环移位处理数据 $s_1(y_2)$ 的数据（rot （$s_1(y_2)$））输出做为数据 $z_2 = rot(s_1(y_2))$。

其中，上述数据处理部进而包括：第三变换部（s_3）和第四变换部（s_4），与欲变换的数据的第一部分数据和第二部分数据不同的一部分数据输入做为第三部分数据，并将与第一部分数据和第二部分数据和第三部分数据不同的一部分数据分别输入做为第四部分数据，而通过使用上述变换表 T 的变换及分别与第二变换部（s_2）的第二部分用运算不同的第三部分用运算和第四部分用运算，来分别变换第三部分数据和第四部分数据，而输出变换后的数据。

本发明的数据变换装置包括：数据处理部，输入密钥数据而至少执行数据的加密和数据的解密的任一种的数据变换，其特征在于：上述数据处理部包括：有限域变换部，输入欲变换的数据，将所输入的数据视为某一域（field）的元，而使用已使用其有限域的逆元电路加以变换，而输出变换后数据；及 GF(2)上的向量空间 $CF(2)^n$ 的仿射变换部，将欲变换成上述有限域变换部的前段和后段的至少任何一方的 $CF(2^n)$上的数据视为自然的对应 $CF(2)^n$ 的元。

其中，上述有限域变换部只具有：多个 N/2 位运算器，将 N（N 为偶数）位的数据 X 以成为 $X = X_0 + \beta X_1$（X_0、X_1：有限域的元，β：原来的域的元）的高 N/2 位数据 X_1 与低 N/2 位数据 X_0 予以等分，并将成为 $Y = Y_0 + \beta Y_1 = 1/(X_0 + \beta X_1)$（X = 0 时 Y = 0）的高 N/2 位数据 Y_1 与低 N/2 位数据 Y_0 分别以 N/2 位单位来运算而求得数据 Y。

本发明的数据变换装置包括：数据处理部，输入密钥数据而至少执行数据的加密和数据的解密的任一种的数据变换；及密钥产生部，产生上述数据处理部所使用的密钥数据而供应至数据处理部，其特征在于：上述数据处理部具有：多段非线性数据变换部，在每一段输入

扩展密钥并被以多段连接来做非线性变换；上述密钥产生部是包括：密钥移位部，对于上述多段非线性数据变换部的每一段而当产生欲供应的扩展密钥，则输入密钥数据与依存于从密钥数据所产生的密钥数据的至少任一数据而仅以预先所决定的位数 Z_1、Z_2、…、Z_m（在此，i、j、k是做为 1～m 中的任何一个值，$Z_k - Z_j = I \times (Z_{i+1} - Z_i) = I \times B$（I 为整数，$B = Z_{i+1} - Z_i$））做循环移位，而从该循环移位后的密钥数据来产生各段的非线性数据变换部的扩展密钥，而且上述密钥移位部包括：循环移位寄存器，在 1 次动作里做（$Z_{i+1} - Z_i$）位（B 位）的循环移位；及控制部，对于已做 Z_i 位循环移位的密钥数据通过使循环移位寄存器动作一次并使执行（$Z_{i+1} - Z_i$）位（B 位）的循环移位，而在循环移位寄存器使产生做 Z_{i+1} 位循环移位的密钥数据，并对于已做 Z_{i+1} 位循环移位的密钥数据通过使循环移位寄存器动作一次并使执行 $I \times (Z_{i+1} - Z_i)$ 位（$I \times B$ 位）的循环移位，而在循环移位寄存器使产生做 Z_{i+2} 位循环移位的密钥数据。

其中，上述循环移位寄存器是在为了使循环移位寄存器动作而被供应的动作时钟的 1 时钟机器周期里做 $Z_{i+1} - Z_i$ 位（B 位）的循环移位的电路。

其中，上述循环移位电路包括：选择器，以做为（$Z_{i+1} - Z_i$）位（B 位）的值，而选择 $B_1 = 8 \times J_1 + 1$（$J_1 = 0$ 以上的整数）位与 $B_2 = 8 \times J_2 - 1$（$J_2 = 1$ 以上的整数，而 J_1 和 J_2 无关系，即 $J_1 \neq J_2$ 或 $J_1 = J_2$）位的任一值。

本发明的数据变换装置包括：数据处理部，输入密钥数据而至少执行数据的加密和数据的解密的任一种的数据变换；及密钥产生部，产生上述数据处理部所使用的密钥数据而供应至数据处理部，其特征在于：上述数据处理部具有：多段非线性数据变换部，在每一段输入扩展密钥并被以多段连接来做非线性变换，上述密钥产生部是包括：密钥移位部，对于上述多段非线性数据变换部的每一段而当产生欲供应的扩展密钥，则仅以预先决定某一密钥数据的位数（B 位）的顺序来做循环移位，而从该循环移位后的密钥数据来产生供应至各段的非线性数据变换部的扩展密钥，而且上述密钥移位部在仅以 B 位顺序做循环移位的数据里，可无视一部分的数据而不产生扩展密钥，而后从

剩余的其他数据来产生扩展密钥.

本发明的数据变换装置是包括：数据处理部，输入密钥数据而至少执行数据的加密和数据的解密的任一种的数据变换；及密钥产生部，产生上述数据处理部所使用的密钥数据而供应至数据处理部，其特征在于：上述密钥产生部包括：第一 G 位密钥变换部，输入并变换 G 位的 G 位密钥数据，而输出 G 位的第一 G 位变换密钥数据；及第二 G 位密钥变换部，输入从上述第一 G 位变换密钥变换部所输出的第一 G 位密钥数据，进而予以变换而输出 G 位的第二 G 位变换密钥数据；而在上述密钥产生部输入 G 位密钥数据 K 的场合时，是将 G 位密钥数据 K 输入到第一 G 位密钥变换部并予以变换，而将由第一 G 位密钥变换部所输出的第一 G 位变换密钥数据 K_1 予以输出做为 G 位密钥数据；在上述密钥产生部输入 2G 位密钥数据 K 的场合时，将从 2G 位密钥数据 K 产生 G 位密钥数据所产生的 G 位密钥数据予以输入到第一 G 位密钥变换部并变换后输出第一 G 位变换密钥数据 K_1，而将第一 G 位变换密钥数据 K_1 输入到第二 G 位密钥变换部予以变换而输出第二 G 位变换密钥数据 K_2，将由第一 G 位密钥变换部所输出的第一 G 位变换密钥数据 K_1 与由第二 G 位密钥变换部所输出的第二 G 位变换密钥数据 K_2 予以连结，而输出做为变换后的 2G 位密钥数据（K_1、K_2）.

其中，上述第一 G 位密钥变换部是包括：2 段非线性数据变换部，将 G 位密钥数据做非线性变换；及逻辑运算部，执行自 2 段非线性数据变换部所输出的变换途中的 G 位密钥数据与第一 G 位密钥变换部所输入的 G 位密钥数据做逻辑运算.

其中，上述密钥产生部进而包括：位长度变换部，于输入 Q 位（$G < Q < 2G$）的密钥数据的场合时，将 Q 位的密钥数据做成 2G 位的密钥数据.

本发明的数据变换装置是包括：数据处理部，输入密钥数据而至少执行数据的加密和数据的解密的任一种的数据变换；及密钥产生部，产生上述数据处理部所使用的密钥数据而供应至数据处理部，其特征在于：包括非线性函数部（F），其包括：密钥函数部，将执行数据变换的数据与密钥数据做逻辑运算；S 函数部，将执行数据变换的数据

予以置换变换成其他数据；及 P 函数部，在执行数据变换的数据间做逻辑运算；非线性函数部（F）将密钥函数部配置于 S 函数部与 P 函数部之间。

本发明的数据变换装置是包括：数据处理部，输入密钥数据而至少执行数据的加密和数据的解密的任一种的数据变换；及密钥产生部，产生上述数据处理部所使用的密钥数据而供应至数据处理部，其特征在于：包括非线性函数部（F），其包括：密钥函数部，将执行数据变换的数据与密钥数据做逻辑运算；S 函数部，将执行数据变换的数据予以置换变换成其他数据；及 P 函数部，在执行数据变换的数据间做逻辑运算；非线性函数部（F）将密钥函数部配置于 S 函数部与 P 函数部两者之前及两者之后的任一者。

其中，上述 S 函数部包括：第一变换部（s_1），输入欲变换的数据的一部分数据做为第一部分数据，而使用可将输入后的数据的值变换成其他的值并予以输出的变换表 T，来变换第一部分数据而输出变换后的数据；及第二变换部（s_2），输入欲变换的数据的至少其他的一部分数据做为第二部分数据，而使用已使用上述变换表 T 的变换及第二部分用运算，来变换第二部分数据而输出变换后的数据。

本发明的数据变换装置包括至少执行数据的加密和数据的解密的任一种的数据变换的数据处理部，还包括非线性函数部（F），其包括：P 函数部，在执行数据变换的数据间做逻辑运算，上述 P 函数输入 z_1、z_2、…、z_8 的 8 个 4n（n 是 1 以上的整数）位数据，并包括：于上述 z_1、z_2、z_3、z_4 的 4 个数据里，执行至少 2 个以上的数据的异或逻辑运算而得到 4n 位的结果的 U_1 电路；于上述 z_5、z_6、z_7、z_8 的 4 个数据里，执行至少 2 个以上的数据的异或逻辑运算而得到 4n 位的结果的 U_2 电路；执行 U_1 与 U_2 的异或逻辑运算而得到 4n 位的结果的 U_3 电路；对于 U_1 做循环移位的循环电路；及执行上述循环电路的输出与 U_3 的异或逻辑运算而得到 4n 位的结果的 U_4 电路；将上述 U_3、U_4 分别分割成 4 个而做为 z'_1、z'_2、…、z'_8 的 8 个 n 位数据而输出。

本发明的数据变换方法是以实行输入密钥数据而至少执行数据的加密和数据的解密的任一种的数据变换的数据处理，其特征在于：上述数据处理将执行数据变换的数据分割为第一数据（L）和第二数据

（R）；而且上述数据处理包括：数据正变换处理（FL），变换第一数据（L）；及数据逆变换处理（FL^{-1}），将第二数据（R）做与上述数据正变换处理（FL）的变换相反的变换。

本发明的数据变换方法是以实行输入密钥数据而至少执行数据的加密和数据的解密的任一种的数据变换的数据处理，其特征在于：上述数据处理包括：非线性变换处理，将数据做非线性变换；非线性变换处理包括：第一变换处理（s_1），将欲变换的数据的一部分数据输入做为第一部分数据，使用可将输入后的数据的值变换成其他的值予以输出的变换表 T 来变换第一部分数据，而输出变换后的数据；及第二变换处理（s_2），将欲变换的数据的至少其他的一部分数据输入做为第二部分数据，使用可使用上述变换表 T 的变换与第二部分用运算来变换第二部分数据，而输出变换后的数据。

本发明的数据变换方法是以实行输入密钥数据而至少执行数据的加密和数据的解密的任一种的数据变换的数据处理，其特征在于：上述数据处理包括：有限域变换处理，输入欲变换的数据，将所输入的数据视为某一域（field）的元，而使用已使用其有限域的逆元电路加以变换，而输出变换后的数据；及 GF(2)上的向量空间 $CF(2)^n$ 的仿射变换处理，将欲变换成上述有限域变换部的前段和后段的至少任何一方的 $CF(2^n)$上的数据视为自然的对应 $CF(2)^n$ 的元。

本发明的数据变换方法实行：数据处理，输入密钥数据而至少执行数据的加密和数据的解密的任一种的数据变换；及密钥产生处理，产生上述数据处理所使用的密钥数据而供应做为数据处理，其特征在于：上述数据处理具有：多段非线性数据变换处理，于每一段输入扩展密钥并被以多段连接来做非线性变换，上述密钥产生处理包括：密钥移位处理，对于上述多段非线性数据变换处理的每一段而当产生欲供应的扩展密钥，则输入密钥数据与依存于从密钥数据所产生的密钥数据的至少任一数据而仅以预先所决定的位数 Z_1、Z_2、…、Z_m（在此，i、j、k 是做为 1～m 中的任何一个值，$Z_k - Z_j = I \times (Z_{i+1} - Z_i) = I \times B$（I 为整数，$B = Z_{i+1} - Z_i$））做循环移位，而从该循环移位后的密钥数据来产生各段的非线性数据变换处理的扩展密钥，而且上述密钥移位处理包括：循环移位处理，在 1 次动作里做（$Z_{i+1} - Z_i$）位（B 位）

的循环移位；及控制处理，对于已做 Z_i 位循环移位的密钥数据通过循环移位处理动作一次并执行（$Z_{i+1}-Z_i$）位（B 位）的循环移位，而通过循环移位处理产生做 Z_{i+1} 位循环移位的密钥数据，并对于已做 Z_{i+1} 位循环移位的密钥数据通过循环移位处理动作 I 次并执行 $I\times(Z_{i+1}-Z_i)$ 位（$I\times B$ 位）的循环移位，而通过循环移位处理产生做 Z_{i+2} 位循环移位的密钥数据。

本发明的数据变换方法实行：数据处理，输入密钥数据而至少执行数据的加密和数据的解密的任一种的变换；及密钥产生处理，产生上述数据处理所使用的密钥数据而供应做为数据处理，其特征在于：上述数据处理具有：多段非线性数据变换处理，于每一段输入扩展密钥并被以多段连接来做非线性变换，上述密钥产生处理包括：密钥移位处理，对于上述多段非线性数据变换部的每一段而当产生欲供应的扩展密钥，则仅以预先决定某一密钥数据的位数（B 位）顺序来做循环移位，而从该循环移位后的密钥数据来产生供应做各段的非线性数据变换处理的扩展密钥，而且上述密钥移位处理在仅以 B 位顺序做循环移位的数据里，可无视一部分的数据而不产生扩展密钥，而从剩余的其他数据来产生扩展密钥。

本发明的数据变换方法实行：数据处理，输入密钥数据而至少执行数据的加密和数据的解密的任一种的数据变换；及密钥产生处理，产生上述数据处理所使用的密钥数据而供应做为数据处理，其特征在于：上述密钥产生处理包括：第一 G 位密钥变换处理，输入并变换 G 位的 G 位密钥数据，而输出 G 位的第一 G 位变换密钥数据；及第二 G 位密钥变换处理，输入从上述第一 G 位密钥变换处理所输出的第一 G 位密钥数据，进而予以变换而输出 G 位的第二 G 位变换密钥数据；而在上述密钥产生部输入 G 位密钥数据 K 的场合时，将 G 位密钥数据 K 输入到第一 G 位密钥变换部并予以变换，而将由第一 G 位密钥变换处理所输出的第一 G 位密钥数据 K_1 予以输出做为 G 位密钥数据，在上述密钥产生部输入 2G 位密钥数据 K 的场合时，将从 2G 位密钥数据 K 产生 G 位密钥数据所产生的 G 位密钥数据予以输入到第一 G 位密钥变换部并变换后输出第一 G 位变换密钥数据 K_1，而将第一 G 位变换密钥数据 K_1 输入做第二 G 位密钥变换处理予以变换而输出第二

G 位变换密钥数据 K_2，将由第一 G 位密钥变换处理所输出的第一 G 位变换密钥数据 K_1 与由第二 G 位密钥变换处理所输出的第二 G 位变换密钥数据 K_2 予以连结，而输出做为变换后的 2G 位密钥数据（K_1、K_2）。

本发明的数据变换方法实行：数据处理，输入密钥数据而至少执行数据的加密和数据的解密的任一种的数据变换；及密钥产生处理，产生上述数据处理所使用的密钥数据而供应做为数据处理，其特征在于：包括非线性函数处理（F），其包括：密钥函数处理，将执行数据变换的数据与密钥数据做逻辑运算；S 函数处理，将执行数据变换的数据予以置换变换成其他数据；及 P 函数处理，在执行数据变换的数据间做逻辑运算；非线性函数处理（F）使密钥函数动作在 S 函数处理与 P 函数处理之间。

本发明的数据变换方法实行：数据处理，输入密钥数据而至少执行数据的加密和数据的解密的任一种的数据变换；及密钥产生处理，产生上述数据处理所使用的密钥数据而供应做为数据处理，其特征在于：包括非线性函数处理（F），其包括：密钥函数处理，将执行数据变换的数据与密钥数据做逻辑运算；S 函数处理，将执行数据变换的数据予以置换变换成其他数据；及 P 函数处理，在执行数据变换的数据间做逻辑运算；非线性函数处理（F）使密钥函数动作在 S 函数处理与 P 函数处理两者之前及两者之后的任一者。

本发明的数据变换装置包括：数据处理部，输入密钥数据而至少执行数据的加密和数据的解密的任一种的数据变换，其特征在于：上述数据处理部包括：第一输入部；第二输入部；第一输出部；第二输出部；非线性变换部，将数据的加密与数据的解密用同一算法执行；第一输入数据正变换部，变换输入于第一输入部的数据；及第二输出数据逆变换部，输入从第二输出部所输出的数据而做与上述第一输入数据正变换部的变换相反的变换。

其中，上述非线性变换部包括：算法处理部，为从第一输入部输入第一输入数据；从第二输入部输入第二输入数据；使用加密用密钥数据来非线性变换第一输入数据和第二输入数据，而产生第一变换数据和第二变换数据；从第一输出部输出第一变换数据；从第二输出部

输出第二变换数据；从第二输入部输入上述第一变换数据，并从第一输入部输入上述第二变换数据，而使用解密用密钥数据来非线性变换第一变换数据和第二变换数据，以产生第一输出数据和第二输出数据；在从第二输出部输出第一输出数据、从第一输出部输出第二输出数据时，使第一输入数据与第二输出数据为同一，第二输入数据与第一输出数据为同一。

其中，上述数据处理部进而包括：第二输入数据正变换部，变换输入于第二输入部的数据；及第一输出数据逆变换部，输入从第一输出部所输出的数据，而做与上述第二输入数据正变换部的变换相反的变换。

本发明的数据变换装置包括：数据处理部，输入密钥数据而至少执行数据的加密和数据的解密的任一种的数据变换；及密钥产生部，产生上述数据处理部所使用的密钥数据而供应至数据处理部，其特征在于：上述数据处理部包括：非线性函数部（F），将执行数据变换的数据做非线性变换，上述密钥产生部加工供应至非线性函数部（F）的密钥数据，而将加工后的密钥数据供应至数据处理部的非线性函数部（F）以外的部分并与数据做运算。

本发明的数据变换方法实行：数据处理，输入密钥数据而至少执行数据的加密和数据的解密的任一种的数据变换；及密钥产生处理，产生上述数据处理所使用的密钥数据而供应做为数据处理，其特征在于：上述数据处理包括：非线性函数处理（F），将执行数据变换的数据做非线性变换，上述密钥产生处理加工供应到非线性函数处理（F）的密钥数据，而将加工后的密钥数据供应至数据处理的非线性函数处理（F）以外的处理并与数据做运算。

而且，该发明的特征是为记录用以在计算机上执行上述数据变换方法的程序的计算机可读取存储记录媒体。

而且，该发明的特征是用以在计算机上执行上述数据变换方法的程序。

附图的简单说明

图 1 是显示加密用数据变换装置 100 和解密用数据变换装置 400

的图。

图 2 是码及符号的说明图。

图 3 是加密部 200 或解密部 500 的构成图。

图 4 是加密部 200 或解密部 500 的其他构成图。

图 5 是数据正变换部（FL）251 的构成图。

图 6 是数据逆变换部（FL^{-1}）271 的构成图。

图 7 是显示现有的加密部和解密部的一部。

图 8 是显示加密部 200 或解密部 500 的一部分的图。

图 9 是显示置于点对称的数据正变换部（FL）251 和数据逆变换部（FL^{-1}）271 的图。

图 10 是显示成为点对称的数据正变换部（FL）251 和数据逆变换部（FL^{-1}）271 的图。

图 11 是显示非线性函数 F 的图。

图 12 是 S 盒第一变换部 13 和 S 盒第二变换部 14 的构成图。

图 13 是 S 盒变换部 21 的构成图。

图 14 是线性变换部 85 的构成图。

图 15 是线性变换部 87 的构成图。

图 16 是密钥产生部 300 或密钥产生部 600 的构成图。

图 17 是位长度变换部 310 的动作说明图。

图 18 是移位寄存器 A341 的构成图。

图 19 是移位控制部 345 的控制表的构成图。

图 20 是移位寄存器 A341 和移位寄存器 B342 的动作说明图。

图 21 是移位寄存器 A341 和移位寄存器 B342 与扩展密钥的对应图。

图 22 是移位寄存器 A341～移位寄存器 D344 的动作说明图。

图 23 是移位寄存器 A341～移位寄存器 D344 与扩展密钥的对应图。

图 24 是显示实装加密用数据变换装置 100 和解密用数据变换装置 400 的计算机的图。

图 25 是现有的 DES 的加密函数的构成图。

图 26 是显示现有的 128 位块加密 E2 的非线性函数的图。

图 27 是显示 S 盒变换部的其他的例的图。

图 28 是显示使用 S 盒第一～第四变换部的非线性函数部 F 的图。

图 29 是变更密钥函数部 25 的配置的图。

图 30 是变更密钥函数部 25 的其他的图。

图 31 是 P 函数部 30 的其他的构成图。

图 32 是 P 函数部 30 的其他的构成图。

图 33 是显示图 31 的 S1～S4 的构成的图。

图 34 是等价密钥的非存在证明的说明图。

图 35 是等价密钥的非存在证明的说明图。

图 36 是加密部 200 或解密部 500 的其他的构成图。

图 37 是加密部 200 或解密部 500 的其他的构成图。

图 38 是加密部 200 或解密部 500 的其他的构成图。

图 39 是加密部 200 或解密部 500 的其他的构成图。

图 40 是加密部 200 或解密部 500 的其他的构成图。

图 41 是加密部 200 或解密部 500 的其他的构成图。

图 42 是合并图 39 和图 40 的场合的图。

图 43 是对于图 3 所示的加密部 200 或解密部 500 而使用图 28 所示的非线性函数部 F 的场合的构成图。

图 44 是显示使用从图 43 所示的非线性函数部 F 来删除密钥函数部 25 的非线性函数部 F′的场合的图。

图 45 是显示对于图 44 的构成更进而与扩展密钥一起执行白扩展密钥的运算的场合的图。

图 46 是显示于非线性函数部 F 取得如图 29 所示那样的构成的场合时，从非线性函数部 F 来删除密钥函数部 25，代以将扩展密钥 k 供应至 XOR 电路 298 的图。

图 47 是显示于非线性函数部 F 取得如图 30 所示那样的构成的场合时，从非线性函数部 F 来删除密钥函数部 25，代以将被非线性变换的扩展密钥 k′供应至 XOR 电路 298 的图。

实施形态一

图 1 是显示该实施形态的加密用数据变换装置 100 和解密用数据

变换装置 400 的图。

加密用数据变换装置 100 是输入例如为 128 位的明文，而输出 128 位的密文的加密装置。解密用数据变换装置 400 是输入 128 位的密文，而输出 128 位的明文的解密装置。加密用数据变换装置 100 是由加密部 200 及密钥产生部 300 所构成。密钥产生部 300 是输入 128 位或 192 位或 256 位的密钥数据，以使用常数 V_i 来产生多（n 个）的 64 位或 128 位的扩展密钥来供应加密部 200。解密用数据变换装置 400 包括解密部 500 及密钥产生部 600。解密部 500 是输入密文，而执行密文的解密的解密用数据处理部。密钥产生部 600 是与前述的密钥产生部 300 相同或相像。而且，加密部 200 及解密部 500 可使用同一结构，在图中，虽以图显示分为加密部 200 及解密部 500，但可兼用 1 个电路或 1 个程序。同样地，密钥产生部 300 及密钥产生部 600 也可兼用 1 个电路或 1 个程序。即，加密用数据变换装置 100 及解密用数据变换装置 400 是可兼用同一电路或同一程序。

图 2 是显示使用在以下的图及说明中的符号的意思。

以下，在图 3 以后的各图中，是将左侧数据称为左数据 L，在图中，将右侧数据称为右数据 R。而且，将输入至非线性数据变换部 210、220、230、240 称为输入数据，将非线性数据变换部 210、220、230、240 称为中间数据，从非线性数据变换部 210、220、230、240 所输出的数据称为输出数据。

图 3 是显示加密部 200 或解密部 500 之一例的图。

图 3 是显示 6 段非线性数据变换部 210 和 6 段非线性数据变换部 220 和 6 段非线性数据变换部 230 成为纵向连接的情形。于 6 段非线性数据变换部 210 与 6 段非线性数据变换部 220 之间是设置数据正变换部（FL）251 及数据变换部（FL^{-1}）271。而且，于 6 段非线性数据变换部 220 与 6 段非线性数据变换部 230 之间是设置数据正变换部（FL）253 及数据逆变换部（FL^{-1}）273。于 6 段非线性数据变换部 210 之中是设置 6 段非线性数据变换部。例如 1 个非线性数据变换部 280 是由非线性函数部 F 和 XOR（异或逻辑）电路 290 所构成。如此而来，在图 3 中是设置全部 18 段的 6 段非线性数据变换部。

非线性数据变换部 210 包括：第一个非线性数据变换部 280，对

于任意 2 个右输入数据 R_0 和左输入数据 L_0，将上述左输入数据 L_0 以使用第一个扩展密钥 k_1 做第一个非线性变换，而将该第一个做非线性变换的输出数据与上述右输入数据 R_0 的异或逻辑以做为第一个左中间数据 L_1 加以输出，并将上述左输入数据 L_0 以做为第一个右中间数据 R_1 加以输出；及第二个非线性数据变换部 281，将上述第一个左中间数据 R_1 以使用第二个扩展密钥 k_2 做第二个非线性变换，而将该第二个做非线性变换的输出数据与上述第一个右中间数据 R_1 的异或逻辑以做为第二个左中间数据 L_2 加以输出，并将上述第一个左中间数据 L_1 以做为第二个右中间数据 R_2 加以输出；而从第一个非线性数据变换部 280 以纵向连接第六个非线性数据变换部 285，将最终的右中间数据 R_6 和左中间数据 L_6 做为变换后的输出数据。

图 4 是显示对于图 3 的加密部 200 还追加数据正变换部（FL）255 和数据逆变换部（FL^{-1}）275 和 6 段非线性数据变换部 240，而通过全部 24 段非线性数据变换部来执行变换的情形。

图 5 是显示数据正变换部（FL）251 的图。

在图 5 中，是显示将数据正变换部（FL）251 的输入数据分为左输入数据 51 和右输入数据 52，于执行逻辑运算后，通过左输入数据 60 和右输出数据 61 而做成输出数据的情形。左输入数据 51 是在 AND 电路 54 中，与扩展密钥 53 做逻辑积运算，其后，在 1 位循环左移位部中，执行向左的 1 位循环移位（也称为循环移位）。移位后是由 XOR 电路 56 来与右输入数据 52 做异或逻辑运算。XOR 电路 56 的输出成为右输出数据 61，同时在 OR 电路 58 中，与扩展密钥 57 做逻辑和运算，其结果为，进而在 XOR 电路中执行与左输入数据 51 的异或逻辑的运算，而成为左输出数据 60。

图 6 是显示数据逆变换部（FL^{-1}）271 的图。

在图 6 中，将输入数据分为左输入数据 71 和右输入数据 72，于执行逻辑运算后，通过左输出数据 80 和右输出数据 81 而做成输出数据的情形。

右输入数据 72 是在 OR 电路 74 中，做与扩展密钥 73 的 OR 逻辑运算，进而，在 XOR 电路 75 中，做与左输入数据 71 的异或逻辑运算。其结果为，来自 XOR 电路 75 的输出成为左输出数据 80，同时在 AND

电路 757 中，做与扩展密钥 76 的 AND 逻辑运算，并在 1 位循环左移位部 78 中，执行向左方向的 1 位循环左移位，其结果为，进而，在 XOR 电路 79 中与右输入数据 72 做异或逻辑运算，而成为右输出数据 81。

图 5 所示的数据正变换部（FL）251 与图 6 所示的数据逆变换部（FL^{-1}）271 是做正逆相反的操作。因而，在同一的扩展密钥之下通过将图 5 的输出数据 Y 做成图 6 的输出数据 Y，可以做为图 6 的输出数据 X 而可得到图 5 的输入数据 X。

如此而来，通过将一方的输出数据做成他方的输入数据，而将以做为他方的输出数据而可得到一方的输入数据的关系称为处在正变换和逆变换的关系。数据正变换部（FL）251 与数据逆变换部（FL^{-1}）271 是执行如此的正变换与逆变换的电路。

还有，图 5 的 1 位循环左移位部 55 与图 6 的 1 位循环左移位部 78 虽是一起向左移位，但两方也可一起执行向右移位。而且，假如数据正变换部（FL）251 与数据逆变换部（FL^{-1}）271 是执行正变换与逆变换，则也可为其他构成。例如，也可改变循环的移位数。而且，更进而可附加含有 not 的 AND 电路、not 的 OR 电路、及含有 not 的 XOR 电路。即，于分别将含有 not 的 AND 电路、not 的 OR 电路、及含有 not 的 XOR 电路表示为 andn、orn、xorn 的场合时，定义以下。

x andn y: （not x）and y

x orn y: （not x）or y

x xorn y: （not x）and y

在最近的几个 CPU，具有也含有 not 的 and、or、xor 命令。这些的命令是可以与 and、or、xor 命令同样的成本来执行。

图 7 是显示现有的加密部 201 和现有的解密部 501。

在现有的加密部 201 中，设置 2 个数据正变换部 FL。因此，为了做该逆操作，而必需于解密部放置 2 个数据逆变换部 FL^{-1}。因而，一般加密部与解密部的构成是不同的，而无法将加密部和解密部做成同一电路。

一方面，如图 8 所示，在该实施形态中，在加密部 200，因为将数据正变换部（FL）251 和数据逆变换部（FL^{-1}）271 相邻配置，所以即使在解密部 500 也可以完全相同的构成来执行解密。例如，在在数

据正变换部（FL）251 变换右数据 R 而得到左数据 L′，在数据逆变换部（FL^{-1}）271 变换左数据 L 而得到右数据 R′的场合时，通过使左数据 L′输入于数据逆变换部（FL^{-1}）271 而可得到右数据 R，并通过使右数据 R′输入于数据正变换部（FL）251 而可得到左数据 L。

如此而来，加密部 200 和解密部 500 是可以完全相同的构成来实现，而可兼用加密部 200 和解密部 500 来使用。

图 9 是显示在以非线性数据变换部 280 为中心而数据正变换部（FL）251 与数据逆变换部（FL^{-1}）271 成为点对称的位置的情形。

因此，在以非线性数据变换部 280 为中心而将数据正变换部（FL）251 与数据逆变换部（FL^{-1}）271 置于点对称的位置的情形时，可以通过同一构成而执行加密和解密。

图 10 是显示置于点对称的位置的数据正变换部（FL）与数据逆变换部（FL^{-1}）的对应。

如图 10 所示，在图 3 中显示数据正变换部（FL）251 与数据逆变换部（FL^{-1}）273 配置于以 6 段非线性数据变换部 220 做为中心的点对称的位置。

还有，在图 3、图 4、图 8、及图 9 中，数据正变换部（FL）与数据逆变换部（FL^{-1}）的位置也可相反。而且，在图 3、图 4、图 8、及图 9 中，右数据 R 与左数据 L 也可相反。

图 36 是显示使用 6 段非线性数据变换部 210 与 6 段非线性数据变换部 220 与 6 段非线性数据变换部 230 而构成加密部 200 的情形。

6 段非线性数据变换部 210 与 6 段非线性数据变换部 220 与 6 段非线性数据变换部 230 是可使用于加密和解密两方的电路。

在此，通过 6 段非线性数据变换部 210 与数据正变换部（FL）250 与数据逆变换部（FL^{-1}）271 而构成正逆数据变换部 211。在此，所谓正逆数据变换部是指可使用于加密和解密两方的电路。即，正逆数据变换部是执行通过将一方的输出数据做成他方的输入数据，并可以他方的输出数据来取得一方的输入数据的正变换和逆变换的 1 个电路。

而且，通过 6 段非线性数据变换部 220 与数据正变换部（FL）251 与数据逆变换部（FL^{-1}）273 而构成正逆数据变换部 221。

而且，通过 6 段非线性数据变换部 230 与数据正变换部（FL）253

与数据逆变换部（FL^{-1}）275 而构成正逆数据变换部 231。

将这些正逆数据变换部 211 与正逆数据变换部 221 与正逆数据变换部 231 以纵列连接而构成加密部 200。因而，该加密部 200 即使做为解密部 500 也可使用。

而且，假如将 6 段非线性数据变换部 210 与 6 段非线性数据变换部 220 与数据正变换部（FL）251 与数据逆变换部（FL^{-1}）271 视为非线性数据变换部 1210，则非线性数据变换部 1210 是可使用于加密和解密两方的电路。在此，通过非线性数据变换部 1210 与数据正变换部（FL）250 与数据逆变换部（FL^{-1}）273 而构成正逆数据变换部 1211。

而且，6 段非线性数据变换部 220 与 6 段非线性数据变换部 230 与数据正变换部（FL）253 与数据逆变换部（FL^{-1}）273 视为非线性数据变换部 1220，则通过非线性数据变换部 1220 与数据正变换部（FL）251 与数据逆变换部（FL^{-1}）275 而构成正逆数据变换部 1221。

所谓正逆数据变换部 1211 和正逆数据变换部 1221 均可使用于解密部 500。

而且，假如将从 6 段非线性数据变换部 210 至 6 段非线性数据变换部 230 止视为非线性数据变换部 2210，则非线性数据变换部 2210 为可使用于加密和解密两方的电路。

在此，通过非线性数据变换部 2210 与数据正变换部（FL）250 与数据逆变换部（FL^{-1}）275 而构成正逆数据变换部 2211。

正逆数据变换部 2211 即使解密部 500 也可使用。

如以上所述，加密部 200 或解密部 500 通过将正逆数据变换部多纵向连接而构成。

而且，加密部 200 或解密部 500 通过使正逆数据变换部含于正逆数据变换部之中，可将正逆数据变换部做成阶层化而构成。

图 37 是显示包括 6 段非线性数据变换部 210 的加密部 200 与解密部 500 成为同一构成的例。

图 37 的 6 段非线性数据变换部 210 是如图 3、及图 4 的所示，具有偶数段的非线性数据变换部 280。数据 A 成为第一个输入数据正变换部 256 所变换的数据 A′，被输入于第一输入部 261，而从第一输入部 261 所输入的数据 A′从第一输出部 263 做为数据 A_1' 而被输出。而且，

从第二输入部 262 所输入的数据 B 从第二输出部 264 做为数据 B_1 而被输出。从第二输出部 264 所输出的数据 B_1 做为由第二输出数据逆变换部 279 所变换的数据 B_1' 而被输出。

从加密部 200 的第一个输出部 263 所输出的数据 A′做为数据 A′而被输入于解密部 500 的第二输入部 262。从加密部 200 的第二输出数据逆变换部 279 所输出的数据 B_1' 做为数据 B_1' 而被输入于解密部 500 的第一输入数据正变换部 256，并做为数据 B_1 而被输出。

非线性数据变换部 210 输入数据 B_1 而输出数据 B。而且，非线性数据变换部 210 输入数据 A_1' 而输出数据 A′。第二输出数据逆变换部 279 是输入数据 A′而输出数据 A。

在图 38，是奇数段的非线性数据变换部 219 含有奇数段的非线性数据变换部 280。因而，从第一输入部 261 所输入的数据 A′从第二输出部 264 做为数据 A_1' 而被输出，并被第二输出数据逆变换部 279 所变换，做为数据 A″而被输出。而且，从第二输入部 262 所输入的数据 B 从第一输出部 263 做为数据 B_1 而被输出。

从加密部 200 的第一输出部 263 所输出的数据 B_1 做为数据 B_1 而被输入于解密部 500 的第二输入部 262。从解密部 500 的第二输出数据逆变换部 279 所输出的数据 A_1'' 做为解密部 500 的数据 A_1''，而被输入于第一输入数据正变换部 256。

图 37、及图 38 的场合是加密部 200 与解密部 500 均为同一构成，而可做加密、及解密。

图 39 是显示于第二输入部 262 设置第二输入数据正变换部 257、及于第一输出部 263 设置第一输出数据逆变换部 278 的情形。

图 40 是显示于第一输入部 261 设置第一输入数据逆变换部 276、及于第二输出部 264 设置第二输出数据正变换部 259 的情形。

图 41 是显示于左侧的输入输出部 261、263 设置数据正变换部 256、258、及于右侧的输入输出部 262、264 设置数据逆变换部 277、279 的情形。

图 42 是显示合并图 39 与图 40 的情形。

虽未加以图示，但也可合并图 37 与图 39。而且，也可合并图 38 与图 39。而且，虽未加以图示，但也可从图 39 来将图 42 的 6 段（偶

数段）的非线性数据变换部 210 做为奇数段的非线性数据变换部 219。从图 39 到图 42 的场合也可以加密部 200 和解密部 500 的同一构成来实现。

实施形态 2

图 11 是非线性数据变换部 280 的非线性函数部 F 的构成图。

非线性函数部 F 输入 F 函数输入数据 10，而执行非线性变换来输出 F 函数输出数据 40。64 位的 F 函数输入数据 10 可分为 8 个数据，而以做为 8 位数据加以处理。各 8 位数据输入于密钥函数部 25 的 8 个 XOR 电路 12，并与扩展密钥 11 做异或逻辑运算，在 S 函数部 20 中，接受使用置换的非线性变换。其后，在 P 函数部 30 中，在 8 位数据间通过如图所示的 16 个 XOR 电路 815 而执行运算，并输出 64 位的 F 函数输出数据 40。在 S 函数部 20 设置 4 个 S 盒第一变换部 13 及 4 个 S 盒第二变换部 14。

图 12 是显示 S 盒第一变换部 13 及 S 盒第二变换部 14 的实现例。

在 S 盒第一变换部 13 的内部设置变换表 T。变换表 T 是对于 0～255 的值来预先存储使任意（随机）对应的 0～255 的值，而输入 0～255 的值，来输出对应于各值（0～255 的值）的表。例如，在输入 1 的场合时，从变换表 T 来输出 7。变换表 T 执行已考虑到是否为全单射、及最大差分机率为充分小等的安全性的非线性变换。

S 盒第二变换部 14 含有 S 盒第一变换部 13，同时具有 1 位循环左移位部 22（图的“<<< 1”的“<<<”是表示循环左移位，而“1”是表示 1 位）。1 位循环左移位部 22 是对于 S 盒第一变换部 13 的输出来执行 1 位的循环左移位。例如，在输入 1 的场合时，从 S 盒第一变换部 13 来输出 7，并从 1 位循环左移位部 22 来输出 14。

只要以如图 12 般地来构成 S 盒第一变换部 13 及 S 盒第二变换部 14，则尽管不需要具有 2 种类变换表 T，但可得到与设置 2 种类变换表 T 的场合相同的效果。通过只具有 1 个变换表 T，而可减少存储变换表 T 的存储器容量，而使整体电路变小。

而且，如图 27 的所示，取代 1 位循环左移位部 22，或者通过在 1 位循环左移位部 22 之外设置 1 位循环右移位部（图 27 的 S 盒第三变

换部 15 的“>>> 1”），而可得到与设置更加不同的变换表 T 的场合相同的效果。而且，对于被输入的数据 y 来设置 1 位循环左移位部（图 27 的 S 盒第四变换部 16 的“<<< 1”），也可先移位被输入的数据 y 后再根据变换表 T 做变换。在图 27 中，虽显示 s（y）、s（y）<<< 1、s（y）>>> 1、s（y <<< 1）的情形，但 s（y >>> 1）也可，s（y <<< 1）<<< 1、s（y <<< 1）>>> 1、s（y >>> 1）<<< 1、s（y >>> 1）>>> 1 的情形也可。通过移位量做为 1 位，例如，在只具有 1 位移位命令的 CPU 等，也可通过做 3 位和 5 位移位，而执行高速处理等。而且，即使在使用只可做 1 位移位的硬件来执行该移位处理的场合时，同样地具有可适用高速处理的场合。进而，不只 1 位移位，即使为 2 位、3 位等的任意位的移位也可，通过执行任意位的移位，而具有与附加不同种类的表相同的效果的场合。

图 28 是显示使用图 27 所示的 4 个 S 盒第一～第四变换部 13、14、15、16 的 S 函数部 20 的图。

而且，将 P 函数部 30 的其他构成显示于图 31。

从 8 位的输入数据 y_1、y_2、y_3、y_4，而分别参考 S1、S2、S3、S4 来求得 32 位的数据 Z_1、Z_2、Z_3、Z_4，并以电路 913 来求得这些异或逻辑运算结果，而且，从 8 位的输入数据 y_5、y_6、y_7、y_8，而分别参考 S2、S3、S4、S1 来求得 32 位的数据 Z_5、Z_6、Z_7、Z_8，并以电路 916 来求得这些异或逻辑运算结果，在电路 917 取得这些异或逻辑运算结果 U_2 与前述异或逻辑运算结果 U_1 的异或逻辑运算而做为 z'_1、z'_2、z'_3、z'_4 予以输出，而且，对于根据电路 913 的异或逻辑运算结果 U_1，向左 1 位循环移位（在该图 31 中，是显示“<<< 1”并非为 1 位，而是 1 字节循环移位）为以电路 918 来执行，以电路 917 的输出与电路 919 来执行异或逻辑运算而得到 z'_5、z'_6、z'_7、z'_8。

在此，如图 33 的（a）～（d）的所示，是以 S1 为使用 S 盒第一变换部 13、S2 为使用 S 盒第二变换部 14、S3 为使用 S 盒第三变换部 15、S4 为使用 S 盒第四变换部 16 而构成，并复制 4 个来自各个变换部的 8 位输出数据而成为 32 位数据，进而，以只输出其中 3 个数据（24 位）那样地，予以屏蔽而输出 32 位数据。

还有，上述电路 918 的 1 位的循环移位是以 S 盒所处理的位长度

（8位＝1字节）单位来移位。

图32虽是与图31为等价的构成，但却显示实装方法不同的P函数部30。

从8位的输入数据 y_1、y_2、y_3、y_4，而分别参考S5、S6、S7、S8来求得32位的数据 Z_1、Z_2、Z_3、Z_4，而这些是以电路933来执行异或逻辑运算，其运算结果A从电路933被输出。而且，从8位的输入数据 y_5、y_6、y_7、y_8，而分别参考S9、SA、SB、SC来输出32位的数据 Z_5、Z_6、Z_7、Z_8，这些为以电路936来执行异或逻辑运算，其运算结果B从电路936被输出。运算结果B是由电路937向右做1位循环移位（在该图32中，是与图31相同，并非为1位单位，而是做S盒所处理的位长度单位（1字节单位）的移位），同时在电路938与运算结果A做异或逻辑运算。该运算结果C是由电路939向上（左）做1位循环，同时在电路940与电路937的输出做异或逻辑运算。其运算结果D是由电路941向上（左）做2位循环，同时在电路942与电路939的输出做异或逻辑运算。其运算结果E是由电路943向（右）做1位循环，同时在电路944与电路941的输出做异或逻辑运算。电路944的输出F做为 z'_1、z'_2、z'_3、z'_4、且电路943的输出做为 z'_5、z'_6、z'_7、z'_8 而被输出。

在此，是以S5、SC为使用S盒第一变换部13与逻辑移位、S6、S9为使用S盒第二变换部14与逻辑移位、S7、SA为使用S盒第三变换部15与逻辑移位、S8、SB为使用S盒第四变换部16与逻辑移位而构成。逻辑移位是为了将来自各变换部的8位输出数据输出于32位输出数据中的预定位置而被利用，以在S5、SA为0字节、在S6、SB为1字节、在S7、SC为2字节、在S8、S9为3字节向左移位般地加以设定。即，只要将在变换部的8位输出做为z，则32位的输出变成在S5、SA为[0、0、0、z]（0是表示8个各个位为0），在S6、SB为[0、0、z、0]，在S8、S9为[z、0、0、0]。

还有，实装也可是以将直接预定的输出送出般地来计算的8位输入，也可先准备32位输出的置换表。

图31、及图32的场合时是可提供以成为比在图26所示的现有的E2加密所使用的置换处理更为高速、且更柔软的实装的装置。

在图 11 中，在将处于 S 函数部 20 的 S 盒以与全种类不同的 S 盒予以构成的场合时，对于需要 8 个变换表 T，以通过做成如图 12 的构成，而可将存储变换表 T 的整体存储容量做成 1/2。

而且，对于图 12 所示的 S 盒第一变换部 13、及 S 盒第二变换部 14 通过以分时输入 8 个 8 位数据，而可只以图 12 所示的 S 盒第一变换部 13、及 S 盒第二变换部 14 来代替现有的个别的 8 个 S 盒。

图 13 是显示 S 函数部 20 的 S 盒的其他例子的图。

关于具体的构成，详细叙述于松井、及樱井所著“伽罗瓦域除法电路及乘除法共同电路”（专利证书登录号码 2641285[H9. 5. 2]）。

在 S 盒变换部 21 输入 8 位数据，并输出 8 位数据，S 盒变换部 21 是由 N（在此是 N = 8）位线性变换部 17 与有限域变换部 18 与 N 位线性变换部 19 所构成。N 位线性变换部 17 执行 8 位操作。有限域变换部 18 只进行为伽罗瓦域 $GF(2^4)$的元的仅 4 位的操作。N 位线性变换部 19 执行 8 位操作。N 位线性变换部 17 的线性变换部 85 是执行图 14 所示的线性变换的电路。而且，线性变换部 87 是执行图 15 所示的线性变换的电路。

还有，也可以使用执行仿射变换（还有，线性变换是可考虑为仿射变换的一态样）的电路来代替线性变换部 85。或者是，也可使用执行仿射变换的电路来代替线性变换部 87。线性变换部 85 是在 8 位的数据（X）来执行变换，而将所得到的 8 位的数据（X′）视为伽罗瓦域 $GF(2^8)$的元，并从 X′来将高 4 位和低 4 位的数据（X_1 和 X_0）分别视为有限域 $GF(2^4)$的元，而输出到有限域变换部 18。在此，例如将 $GF(2^8)$的元β做为有限多项式 $X^8 + X^6 + X^5 + X^3 + 1 = 0$ 的元，只要一做为 $\alpha = \beta^{238}$，则有限域 $GF(2^4)$的基底表示为[1、α、α^2、α^3]，只要一使用此来表示 $GF(2^4)$的元 X_0、X_1，则成为所谓 $X' = X_0 + \beta X_1$ 的关系（详细请参考“伽罗瓦域除法电路及乘除法共同电路”（专利证书登录号码 2641285[H9. 5. 2]））。有限域变换部 18 是只以执行 4 位的运算的运算器来构成。

在此，做为“有限域”的取法是考虑对于 $GF(2^n)$，为 n = 2m 的有限域 $GF(2^m)$，在此的例是 n = 8、m = 4。

有限域变换部 18 是使用以“伽罗瓦域除法电路及乘除法共同电路”（专利证书登录号码 2641285[H9. 5. 2]）中所示的 n = 8、m = 4 时

的电路为基础而构成的有限域的逆元电路。做为该逆元电路的运算结果，各个视为 $GF(2^4)$的元的高 4 位的数据和低 4 位的数据（Y_1 和 Y_0）为做为 $GF(2^8)$上的元的 8 位的数据 Y 而被输出于线性变换部 87。在此，是 $Y = Y_0 + \beta Y_1$。根据以上，该逆元电路是运算 $Y_0 = Y + \beta Y_1 = 1/(X_0 + \beta X_1)$ 的电路。而且，在该逆元电路的“有限域”的元的表示法（基底的取法）是如所谓“多项式基底”和“正规基底”那样地，可考虑几个“基底”的取法。

在图 13 的 S 盒变换部 21 中成为特征的点，是以为了执行非线性变换而被输入的数据的位宽度（8 位）的一半的位宽度（4 位）来运算的点。即，在逆元电路中，是只执行 4 位操作的点为其特征。

如此而来，通过执行只 4 位的操作而有可能使运算速度变慢，但电路整体的规模具有所谓远比使用 8 位的运算元件还来得小的优点。

因而，S 盒变换部 21 的其次的特征是于前述有限域变换部 18 的两侧设置 N 位线性变换部 17 与 N 位线性变换部 19 之点。只要一使用有限域变换部 18 来实现 S 盒变换部 21，则比起以使用存储随机的值的变换表 T 的场合，虽具有所谓整体电路的规模变小，或构造简单的优点，但相反地却有安全性降低的可能性。在此，在有限域变换部 18 的两侧执行线性变换或仿射变换，而可消除因为采用有限域变换部 18 所导致的安全性的降低的问题。

还有，在图 13 中，虽在有限域变换部 18 的两侧执行线性变换，但也可只设置一侧。或者是，也可在一侧做线性变换，而在另一侧执行仿射变换。

图 29 是将图 11 所示的密钥函数部 25、即处于 S 函数部 20 与 P 函数部 30 之前的密钥函数部 25 予以配置于 S 函数部 20 与 P 函数部 30 之后。

而且，图 30 是将密钥函数部 25 配置于 S 函数部 20 与 P 函数部 30 之间。

通过如图 29 或图 30 般的构成，比起图 11 所示的构成，可得到所谓实装上高速成为较多的效果。进而，通过修正扩展密钥的产生，在图 29 或图 30 的构成中，从相同的输入可得到与图 11 的构成相同的输出。在图 26 所示的现有的 F 函数中，具有 2 个 S 函数，分别于最初执

行扩展密钥的运算，其次，根据 S 函数执行运算。对于此，图 29 所示的场合是将一个密钥函数部 25 配置于 F 函数的最后。而且，图 30 的场合时，是将一个密钥函数部 25 配置于 S 函数部 20 与 P 函数部 30 之间。

图 43 是对于图 3 所示的加密部 200 或解密部 500 而使用图 28 所示的非线性函数部 F 的场合的构成图。

以做为 F 函数输入数据 10 而将左数据输入于非线性函数部 F，并输出 F 函数输出数据 40。F 函数输出数据 40 与右数据做异或逻辑运算，其结果成为次段的左数据。而且，左数据做为 F 函数输入数据 10 而被输入于非线性函数部 F，同时做为次段的右数据而被使用。在图 43 所示的构成中，因为在非线性函数部 F 之中执行密钥函数部 25 和 S 函数部 20 和 P 函数部 30 的运算，所以在非线性函数部 F 的运算负荷变成很大。对于通过执行使在该非线性函数部 F 的运算负荷分散，而达成处理的高速化的例，以下使用图来说明。

图 44 是显示以使用从图 43 所示的非线性函数部 F 之中删除密钥函数部 25 的非线性函数部 F′的场合。扩展密钥 k_1 在 XOR 电路 891 中与左数据 L_0 做异或逻辑运算。而且，扩展密钥 k_2 在 XOR 电路 297 中与右数据 R_0 做异或逻辑运算。左数据做为 F 函数输入数据 10 而被输入于非线性函数部 F′，并接受 S 函数部 20 与 P 函数部 30 的变换。XOR 电路 297 与 F 函数输出数据 40 在 XOR 电路 290 做异或逻辑运算，而输出左数据 L_1。

一方面，密钥产生部 300、600 与扩展密钥 k_1 和 k_3 做异或逻辑运算，而输出该被加工的扩展密钥 $k_1 + k_3$。XOR 电路 891 的输出 R_1 与扩展密钥 $k_1 + k_3$ 在 XOR 电路 298 做异或逻辑运算，并输出右数据。密钥产生部 300、600 加工扩展密钥，而产生 $k_1 + k_3$、$k_2 + k_4$、$k_3 + k_5$、…、$k_{16} + k_{18}$ 予以输出。密钥产生部 300、600 将被加工的扩展密钥供应至非线性函数部（F）以外的处理而与数据做运算。该结果为，左数据 L_{18} 与右数据 R_{18} 可得到与图 43 的场合相同。

通过将被加工的扩展密钥供应至非线性函数部（F）以外的处理而与数据做运算，而在非线性函数部 F′中，在做 S 函数部 20 与 P 函数部 30 的计算之间，在非线性函数 F′的外部、即 XOR 电路 297、298

可做与密钥数据的计算，而密钥函数部 25 的计算则从非线性函数部 F 消失，于是非线性函数部 F 的负荷被分散，而高速实装成为可能。

图 45 是显示对于图 44 的构成并进而与扩展密钥一起来执行白扩展密钥 kw_1 的运算的情形。在图 45 中，是显示密钥产生部为预先执行白扩展密钥的一部分 $kw_{1\ high}$ 与第一扩展密钥 k_1 的异或逻辑运算（即，密钥产生部为加工扩展密钥），而供应至 XOR 电路 891 的情形。

而且，显示密钥产生部预先执行白扩展密钥的一部分 $kw_{1\ low}$ 与第二扩展密钥 k_2 的异或逻辑运算（即，密钥产生部为加工扩展密钥），而供应至 XOR 电路 297 的情形。

如此而来，可消除图 44 所示的 XOR 电路 293 的运算。而且，图 45 的情形为，密钥产生部执行白扩展密钥 kw_2 的一部分 $kw_{2\ low}$ 与扩展密钥 k_{17} 的异或逻辑运算（即，密钥产生部为加工扩展密钥），而供应至 XOR 电路 299。而且，密钥产生部为执行白扩展密钥 kw_2 的其他部分 $kw_{2\ high}$ 与扩展密钥 k_{18} 的异或逻辑运算（即，密钥产生部为加工扩展密钥），而供应至 XOR 电路 892。

如此而来，可消除图 44 所示的 XOR 电路 296 的运算。

图 46 是显示将在非线性函数部 F 为取得如图 29 的所示的构成的场合时，从非线性函数部 F 删除密钥函数部 25，以密钥产生部将扩展密钥 k 供应至 XOR 电路 298 来取代的情形。

而且，图 47 是显示将在非线性函数部 F 取得如图 30 的所示的构成的场合时，从非线性函数部 F 删除密钥函数部 25，以密钥产生部将非线性变换而成的扩展密钥 $k' = P(k)$ 供应至 XOR 电路 298 来取代的情形。图 47 的场合是显示对于密钥数据施以与依据 P 函数处理的运算相同的运算而产生非线性变换而成的密钥数据，将非线性变换而成的密钥数据做为上述数据处理所使用的密钥数据，而供应至数据处理的非线性函数部（F）以外的处理并使与数据做运算的情形。因为图 46 及图 47 的任一场合均可从非线性函数部 F 来消除密钥函数部 25，所以可减少非线性函数部 F 的运算负荷，因为与非线性函数部 F 的运算平行而可执行处于非线性函数部 F 之外的 XOR 电路的运算，所以可执行高速处理。

实施形态 3

图 16 是图 1 所示的密钥产生部 300（或密钥产生部）600 的构成图。

密钥产生部 300 是由位长度变换部 310 与第一 G 位密钥变换部 320 与第二 G 位密钥变换部 320 与密钥移位部 340 所构成。在密钥产生部 300 输入 128 位或 192 位或 256 位的密钥数据，而产生 128 位的密钥数据 k_1 与 128 位的密钥数据 k_2，并输出多个 64 位的扩展密钥。在位长度变换部 310 中，即使输入与位数不同的密钥数据，也可以使所输出的密钥数据的位长度成为一定般地进行变换。即，位长度变换部 310 是在内部产生高 128 位的密钥数据 SK_{high} 与低 128 位的密钥数据 SK_{low}，而将前者输出于第一 G 位密钥变换部 320 与密钥移位部 340。而且，将后者输出于第二 G 位密钥变换部 320 与密钥移位部 340。而且，将前者与后者做异或逻辑运算的 128 位密钥数据输出于第一 G 位密钥变换部 320。

图 17 是显示位长度变换部 310 的内部动作的图。

在输入 128 位密钥数据于位长度变换部 310 的场合时，其所输入的密钥数据仍做为高 128 位密钥数据 SK_{high} 而被输出。而且，低 128 位密钥数据 SK_{low} 是被设定为 0 而被输出。

其次，在输入 192 位密钥数据于位长度变换部 310 的场合时，其所输入的密钥数据的高 128 位数据仍做为高 128 位密钥数据 SK_{high} 而被输出。而且，被输入的 192 位密钥数据的低 64 位数据与反相其低 64 位的 64 位反相数据连结，而产生低 128 位的密钥数据 SK_{low} 并予以输出。

其次，在输入 256 位密钥数据的场合时，被输入的密钥数据的高 128 位做为 SK_{high}、且低 128 位做为 SK_{low} 而被输出。

在第一 G 位密钥变换部 320 从位长度变换部 310 将 128 位密钥数据 SK_{high} 与 SK_{low} 做异或逻辑运算结果输入，在接受 2 段非线性变换后，与 128 位密钥数据 SK_{high} 做异或逻辑运算，进而接受 2 段非线性变换，输出 128 位密钥数据 k_1。

在输入于位长度变换部 310 的密钥数据长度为 128 位的场合时，使用从第一 G 位密钥变换部 320 所输出的 128 位密钥数据和被输入的

元密钥数据而使密钥移位部 340 产生扩展密钥。而输入于位长度变换部 310 的密钥数据长度为 192 位或 256 位的场合时，进而将第一 G 位密钥变换部 320 所输出的 128 位密钥数据输入于第二 G 位密钥变换部 320，而与低 128 位密钥数据 SK_{low} 做异或，在执行 2 段非线性变换后，输出 128 位密钥数据 k_2。在密钥移位部 340 输出从第一 G 位密钥变换部 320 与第二 G 位密钥变换部 320 两方所输出的 2 个 128 位密钥数据，使用两者与所输入的元密钥数据而使密钥移位部 340 产生扩展密钥。

密钥移位部 340 包括移位寄存器 A 341 与移位寄存器 B 342 与移位寄存器 C 343 与移位寄存器 D 344 与移位控制部 345。从移位控制部 345 输出选择信号 346 到移位寄存器，而控制移位寄存器的动作。

图 18 是显示移位寄存器 A 341 的构成的图。

移位寄存器 A 341 包括：具有 128 位开关群的选择器 A 347；及 128 位的寄存器 A 348。选择信号 346 包括：开关信号，指示将选择器 A 347 的各开关全部同时连接于 A 侧或 B 侧的任一侧。在图中，是显示通过选择信号 346 而选择器 A 347 的开关群为选择 A 的情形，在该场合时，是显示寄存器 A 348 为循环移位于 17 位左侧的情形。而且，显示于开关群连接 B 的场合时，寄存器 A 以 15 位循环移位于左侧。该 15 位移位或 17 位移位是在一时钟机器周期里执行。

还有，循环移位的移位数（15、17）是一例，也可为其他的移位数。

图 19 是显示存储于移位控制部 345 的控制表的一部分的图。

该控制表是在每一时钟存储使寄存器移位几个位的表。例如，在寄存器 A 控制表中，显示在第一时钟移位 15 位。而且，更显示在第二时钟移位 15 位。同样地来显示第三时钟及第四时钟也移位 15 位。第五时钟～第八时钟显示分别移位 17 位。

图 20 是显示在从 128 位密钥数据来产生扩展密钥的场合时，移位控制部 345 使用图 19 所示的表来控制移位寄存器的结果的图。

在移位寄存器 A 341 设定从位长度变换部 310 所输入的高 128 位密钥数据 SK_{high}。在移位寄存器 A 342 设定从第一 G 位密钥变换部 320 所输入的 128 位密钥数据 K_1。在如此状态中，根据图 19 所示的控制表，而动作移位寄存器 A 341 及移位寄存器 A 342。在图 20 中，无视

画斜线的部分，表示不输出。在此以外的未画斜线的部分如图 21 所示，做为扩展密钥而被输出。

图 21 是显示与寄存器的值与扩展密钥的对应的图。

在图 20 中，显示每一时钟以每 15 位做 4 次移位，从第五时钟起每一时钟做 17 位移位的情形。从移位寄存器 A 341 与移位寄存器 A 342 输出或不输出高 64 位及低 64 位做为扩展密钥的判断、或者其输出的顺序号码被记载于未做图示的控制表里，而基于其控制表，通过使输入指示信号含于选择信号 346 而输出到移位寄存器，成为从各移位寄存器可以每 64 位输出扩展密钥。

图 22 是显示从 192 位或 256 位的密钥数据来产生扩展密钥的情形。

即，显示在移位寄存器 A 341 设定位长度变换部 310 所输入的高 128 位密钥数据 SK_{high}，在移位寄存器 A 342 设定低 128 位密钥数据 SK_{low}，在移位寄存器 A 343 设定第一 G 位密钥变换部 320 所输出的 128 位密钥数据 K_1，在移位寄存器 A 344 设定第二 G 位密钥变换部 320 所输出的 128 位密钥数据 K_2 的情形。

斜线部分是显示未使用做为扩展密钥的密钥。

图 23 是显示寄存器的值与扩展密钥的对应的图。

未使用做为扩展密钥的密钥和图 23 所示的寄存器的值与扩展密钥的对应也存储在处于前述控制部的控制表。

图 19 的所示，移位控制部 345 存储移位设定于移位寄存器 A 341 的密钥数据的位数。即，如移位寄存器 A 控制表的所示，通过使设定于移位寄存器 A 341 的密钥数据移动 $Z_0 = 0$ 位、$Z_1 = 15$ 位、$Z_2 = 45$ 位、$Z_3 = 60$ 位、$Z_4 = 77$ 位、$Z_5 = 94$ 位、$Z_6 = 111$ 位、$Z_7 = 128$ 位，而成为一个一个地产生扩展密钥。

各移位数之和成为 $15 + 15 + 15 + 15 + 17 + 17 + 17 + 17 = 128$，通过将 128 位的寄存器做 128 位循环移位，寄存器返回初期状态。

如此而来，将移位数的总和做为 128 位（寄存器的位数）而返回初期状态的理由是在对于初期状态的寄存器而有其次的处理的场合时，仍然可开始其次的处理。而且，即使在执行逆变换处理（解密）的场合时，因为从为了产生扩展密钥的处理的开始为仍然照样地从初

期状态来开始，所以通过设定初期状态，而变换处理（加密）与逆变换处理（解密）均可执行。而且，将移位数的总数不做成比128位（寄存器的位数）更大，原因是因为例如128位（寄存器的位数）以下的2位循环移位与比128位（寄存器的位数）还大的130位循环移位已成为同一值，而做为依据已做为一循环以上的移位（128位以上的移位数）的寄存器内的状态，可防止相同值的发生。寄存器A控制表最好是每当寄存器做一循环，尽可能在其途中来设定成为不规则的移位数的值。然而，为了简单做成移位寄存器的构成，最好以被限制的移位数来移位。在此，将寄存器在1个时钟（1时钟）里可做15位与17位两种类的移位来加以构成，使用该两种类的移位，进而，如以下所述般地，可实现移位不同的位数。

做成所谓$Z_1-Z_0=15$（在此，设$Z_1-Z_0=B_1$），$Z_2-Z_1=30$（即，$Z_2-Z_1=2B_1$），$Z_2-Z_1=2(Z_1-Z_0)$的关系。而且，如移位寄存器B控制表的所示，做成所谓$Z_5-Z_4=34$（在此，设$Z_5-Z_4=2B_2$），$Z_6-Z_5=17$（即，$Z_6-Z_5=B_2$），$Z_5-Z_4=2(Z_6-Z_5)$的关系。即，将移位数的差分做为15位和30位或17位和34位，做成为1次的移位数（15位和17位）的整数倍（2倍=I倍）的移位数（30位或34位）。

如此而来，通过将移位数的差分做成1次的移位数或1次的移位数的2倍以上的整数倍（I倍、I是2以上的整数）的任一种，并通过使移位寄存器A 341动作1次或2次（I次），而可容易地实现存储于控制表的移位数的操作。所谓使动作2次（I次）是意味着为了动作移位寄存器A 341而被供应的动作时钟的2时钟（I时钟）机器周期里移位动作完毕。

在此，使移位I次（2次）的场合时，直至I-1次（2-1=1次）为止的已移位的数据是无视高数据与低数据，而做为扩展密钥不使用。例如，于从图19的$Z_1=15$移位至$Z_2=45$的场合时，成为$I=(Z_2-Z_1)/$（I次的移位数）=（45-15）/15=2，而第I-1次（2-1=第1次）的移位后的数据无视于高数据与低数据，而做为扩展密钥不使用。此在图20中为在key [8]和key [9]画斜线，而表示做为扩展密钥不使用。因而，以使用第I次（第2次）的移位后的高数据与低数据的任一方或两方做为扩展密钥。此是表示在图20中将key [12]和key [13]做为

扩展密钥予以输出。

如此而来，因为执行2以上的整数倍的移位，并不仅为15位或17位的移位，也可执行30（=15×2）位或34（=17×2）位（或45（=15×3））位或51（=17×3）位等的移位，而使移位数变化，因而更提高了安全性。而且，即使是设置前述的做为扩展密钥未使用的场合时，同样地也是为了提高安全性。

做为扩展密钥未使用的数据（在图20和图22中，做为画斜线的扩展密钥未使用的密钥）是最好产生于如硬件的处理、或程序的处理为未连续执行的场合时。例如，在图3中，最好于执行数据正变换部（FL）与数据逆变换部（FL^{-1}）的操作时，或者于其前后，或在程序中调用函数，或在执行副程序或中断处理的场合时的处理的分界线，或在处理的变化时来执行。

而且，图19所示的控制表的特征是指定$B_1 = 8 \times 2 - 1 = 15$（$B_1 = 8 \times J_1 - 1$，在此$J_1$是1以上的整数）位的移位数、及$B_2 = 8 \times 2 + 1 = 17$（$B_2 = 8 \times J_2 + 1$，在此$J_2$是0以上的整数，$J_1 = J_2$或$J_1 \neq J_2$）位的移位数。通过将移位的量做成于8的倍数±1，而成为执行奇数位的移位，所以比起仅以偶数位移位其安全性更加提高。而且因为做为移位量而仅执行于8的倍数±1，所以会有在只具有1位移位命令的CPU等中，比起移位3位和5位，有时更可执行高速处理。而且，即使在使用只可以移位1位的硬件来执行该移位处理的场合时，同样地，也会有可适用高速处理的场合。

在前述位长度变换部310的说明中，虽显示输入3种类的位宽度的密钥数据的场合，但于输入具有128位（G位）和256位（2G位）间的位长度Q（G < Q < 2G）的密钥数据的场合时，也可使用任何算法处理而可以与输入256位的密钥数据的场合同样大小般地来伸长密钥数据。即，在输入具有G位和2G位间的长度Q的密钥数据的场合时，通过位长度变换部310而可将Q位的密钥数据变换成2G位的密钥数据。

其次，使用图34来说明等价密钥的非存在证明。

在以下的图34的说明中，以“+”来意味为异或逻辑运算。

在此，做成输入2个128位的密钥数据SK1和SK2（SK1≠SK2），

并做成位长度变换部 310 为从 SK1 输出 $SK1_{high}$ = SK1 = (SKH1 | SKL1)，且从 SK2 输出 $SK2_{high}$ = SK2 = (SKH2 | SKL2)。在此，SKHi (i = 1、2) 是 Ski 的高 64 位数据，而 SKLi (i = 1、2) 是 Ski 的低 64 位数据。

将 SKH1 与 SKH2 做异或逻辑运算结果做为ΔA，将 SKL1 与 SKL2 做异或逻辑运算结果做为ΔB，因为 SK1 ≠ SK2，所以成立“至少ΔA ≠0 或ΔB ≠0”。

如图 34 的所示，通过该ΔA 与ΔB 接受 2 段非线性变换，而变化成 ΔA + ΔD、及ΔB + ΔC。此是意味着 $SK1_{high}$ 与 $SK2_{high}$ 的异或逻辑运算结果 (ΔA | ΔB) 变化成自接受 2 段非线性变换的数据与自 $SK2_{high}$ 接受 2 段非线性变换的数据做异或逻辑运算的结果(ΔA + ΔD | ΔB + ΔC)。因而，只要接受该 2 段非线性变换的数据在异或逻辑电路 999 分别与 $SK1_{high}$、$SK2_{high}$ 做异或逻辑运算，则该两个数据的异或逻辑运算结果便成为 (ΔD | ΔC)。还有，在此若非线性变换为全单射函数，则对于 ΔX ≠ 0 的输入，因为输出ΔY ≠ 0，所以若为“至少ΔA ≠ 0 或ΔB ≠ 0”，则成为“至少ΔC ≠ 0 或ΔD ≠ 0”。所以，意味着绝无通过 2 段非线性变换而从 $SK1_{high}$ 和 $SK2_{high}$ 输出相同数据的情形，成为等价密钥的非存在证明。

一方面，如图 35 的所示，不仅执行 2 段非线性变换，也可考虑关于 3 段非线性变换的场合。因为成立“至少ΔA ≠ 0 或ΔB ≠ 0”，所以会有ΔA 或ΔB 的任一个为 0 的情形。假如ΔA = 0 则ΔC = 0，而且，通过与上述相同的计论，则 $SK1_{high}$ 与 $SK2_{high}$ 的异或逻辑运算结果 (0 | ΔB) 变化成自 $SK1_{high}$ 接受 3 段非线性变换的数据与自 $SK2_{high}$ 接受 3 段非线性变换的数据做异或逻辑运算的结果 (ΔB + ΔE | ΔD)。因而，只要接受该 3 段非线性变换的数据在异或逻辑电路 999 分别与 $SK1_{high}$、$SK2_{high}$ 做异或逻辑运算，则该两个数据的异或逻辑运算结果便成为 (ΔB + ΔE | ΔB + ΔD)。还有，在此若假定ΔB = ΔD = ΔE ≠ 0 成立，则成为 (ΔB + ΔE | ΔB + ΔD) = (0 | 0)。总之，意味着只要分别与 $SK1_{high}$ 和 $SK2_{high}$ 做异或逻辑运算，则其运算结果为一致。即，意味着从 $SK1_{high}$ 和 $SK2_{high}$ 输出相同数据的情形，即为加密的安全性问题上很多的等价密钥存在着。

不仅以上所述的 3 段非线性变换，即使在一般的非线性变换上也有从不同的 SK1 和 SK2 输出等价的 K_1，即有存在等价密钥的可能性，但可证明若为在本实施形态中所述的 2 段非线性变换则等价密钥即不存在。

而且，附上等价密钥的非存在证明，是因为虽可想到在该 2 段非线性变换之外也有，但在执行 2 段非线性变换的场合时，因为除了可附上等价密钥的非存在证明，且为简单的构成，所以做成 2 段非线性变换的构成最佳。

图 24 是显示实装加密用数据变换装置 100 或解密用数据变换装置 400 的计算机的图。

加密用数据变换装置 100 或/及解密用数据变换装置 400 做成印刷电路板连接于总线。在该印刷电路板包括 CPU、存储器或逻辑电路元件，并通过执行前述说明过的动作将由 CPU 所供应的明文做成密文，再送回 CPU。或者是，将从 CPU 送过来的密文解密成明文，再送回 CPU。

加密用数据变换装置 100 或解密用数据变换装置 400 可全部以使用硬件来加以实现。而且，加密用数据变换装置 100 或解密用数据变换装置 400 也可全部以使用软件而做为数据变换方法来加以实现。即，使用存储于硬盘装置和软盘装置的程序而可使执行前述的动作。或者是，虽未予以图示，但也可组合硬件和软件使实现前述的动作。而且，虽未予以图示，无需以一台计算机来实现前述的动作全部，而也可以如服务器与客户终端、或主计算机与终端计算机那样地，在被分散的系统中来达成前述的动作。

在前述的图 1～图 47 的图中记载有箭头的图其箭头的方向表示动作的流向，在前述的图 1～图 47 的图中记载有箭头的图是数据变换装置的方块图，而且也为流程图。因而，在前述的方块图的记载有“什么部”的部分是通过改成“什么步骤”或“什么处理”，而成为表示数据变换方法的动作流程图或程序流程图。

还有，在前述的实施形态中，虽显示 128 位的明文和密文的场合，但也可为 256 位的明文和密文及其他位的明文和密文的场合。

而且，在前述的实施形态中，虽显示 128、192、256 位的密钥数

据和 64 位的扩展密钥的场合，但也可为其他位数的场合。

在明文和密文和扩展密钥的位长度改变的场合时，不用说以对应其位长度，各部和各步骤和各处理的所处理的位长度也要改变。

产业上的可利用性

若依据该发明的实施形态，则因为加密和解密可在同一处理步骤来执行，包括数据正变换部（FL）251 及数据逆变换部（FL^{-1}）271，所以可兼用加密部 200 和解密部 500 来加以使用。

而且，若依据该发明的实施形态，则因为兼用变换表 T 来构成 S 盒第一变换部 13 及 S 盒第二变换部 14，所以会有所谓构成变为简单的效果。

而且，若依据该发明的实施形态，则因为使用有限域变换部 18，所以构成变为简单，同时因为设置线性变换部 85 及线性变换部 87，所以即使在使用有限域变换部 18 的场合时也可使安全性提高。

而且，若依据该发明的实施形态，则通过移位控制部 345 以整数次动作移位寄存器来执行可使用非仅 15 位和 17 位的一定值的移位数（例如，30 位和 34 位）密钥数据的移位，故可提高安全性。

而且，若依据该发明的实施形态，则因为在移位寄存器设置从被移位的数据做为扩展密钥不使用的场合，所以更可提高安全性。

而且，若依据该发明的实施形态，则因为即使在输入位数不同的密钥数据的场合时，通过位长度变换部 310 变换成一定长度的密钥数据，所以可执行具有柔软性的密钥产生操作。

而且，若依据该发明的实施形态，则通过在第一 G 位密钥变换部 320 使用 2 段非线性变换，而可证明对于 K_1 并不存在等价密钥，而可使安全性提高。

而且，若依据该发明的实施形态，则因为变更密钥函数部 25 的配置位置，所以可行高速处理。

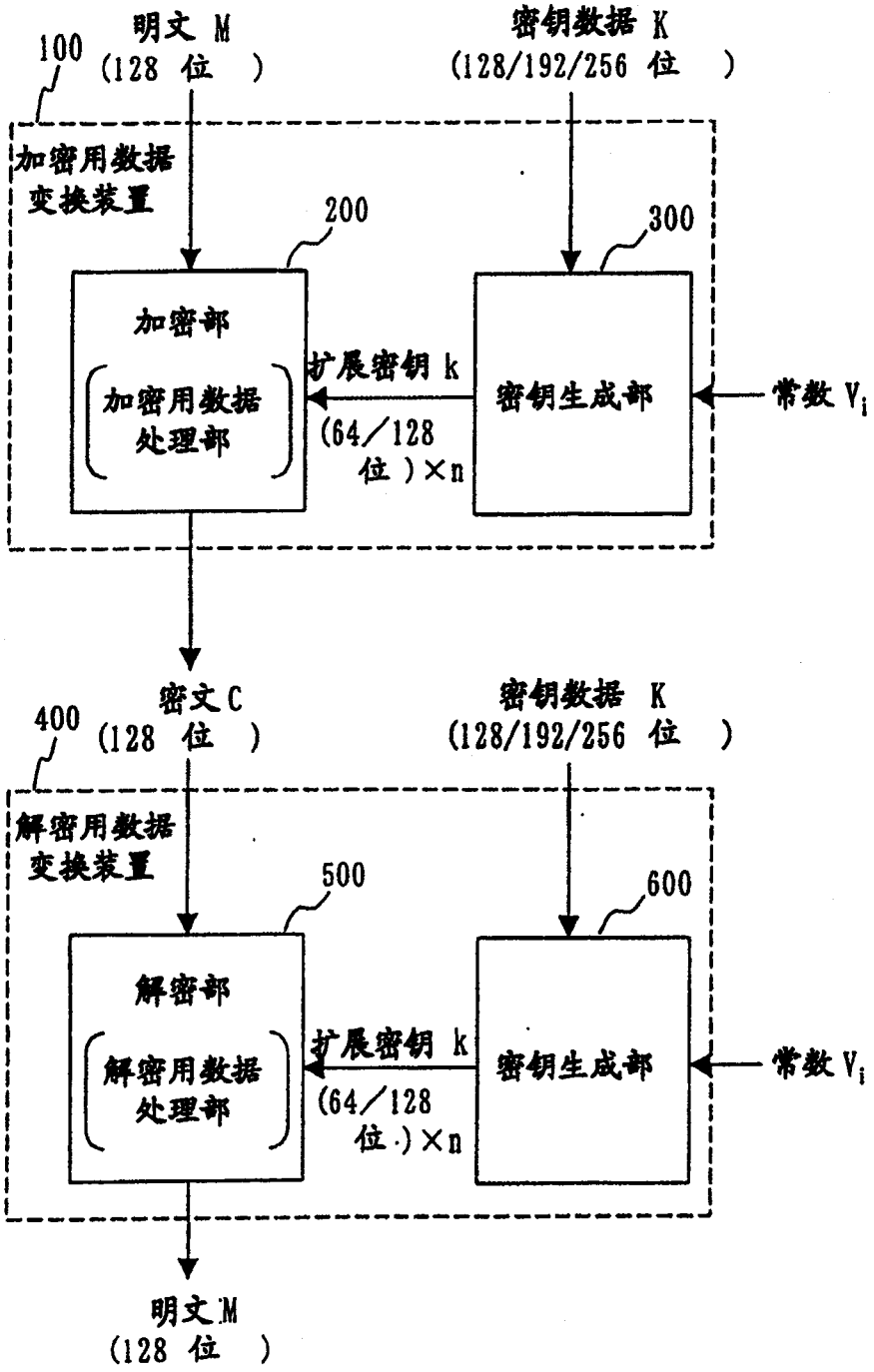

明文 M
(128 位)
100
密钥数据 K
(128/192/256 位)
加密用数据
变换装置
200
300
加密部
加密用数据
处理部
扩展密钥 k
(64／128
位)×n
密钥生成部
常数 V_i
密文 C
(128 位)
400
密钥数据 K
(128/192/256 位)
解密用数据
变换装置
500
600
解密部
解密用数据
处理部
扩展密钥 k
(64／128
位)×n
密钥生成部
常数 V_i
明文 M
(128 位)

图 1

(b)：1 字节 (8 位)
(w)：4 字节 (32 位)
(l)：8 字节 (64 位)
(q)：16 字节 (128 位)

M：
C：
K：
T：

kw_1, kw_2
k_1, k_2, ... , k_{24}
kl_1, kl_2, ... , kl_6

F ：
FL ：
FL^{-1}：

L_0, L_1, ... , L_{24} 左数据
R_0, R_1, ... , R_{24} 右数据
V_1, V_2, ... , V_6

1 M(q)表示16 字节 (128 位)的明文
2 kw_1(q)表示 16 字节 (128位)的扩展密钥
3 k_1(l)表示 8 字节 (64 位)的扩展密钥
4 L_0(l)表示 8 字节 (64 位)的左数据

图 2

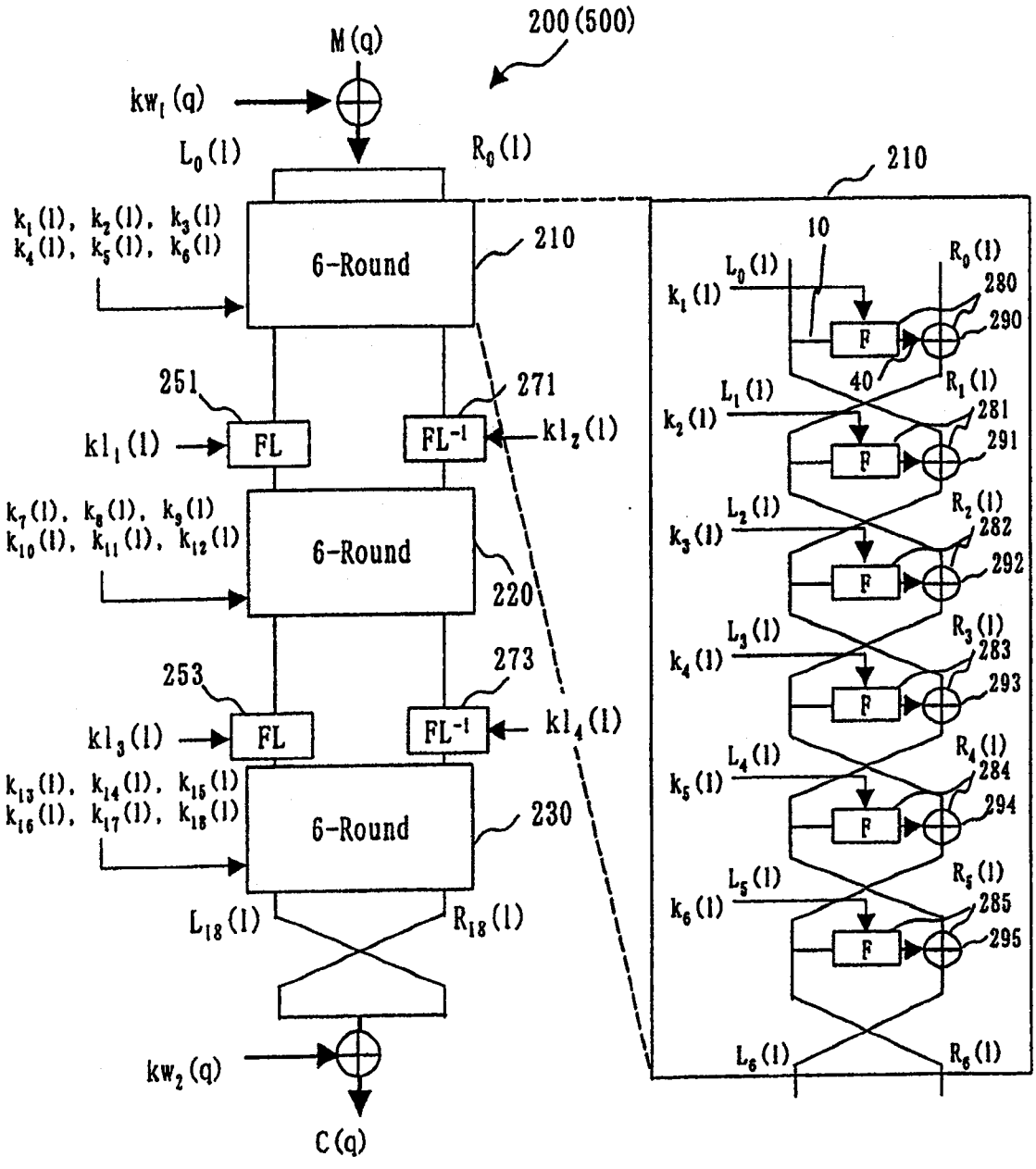

200(500)
M(q)
kw1(q)
L0(1)
R0(1)
210
k1(1), k2(1), k3(1)
k4(1), k5(1), k6(1)
6-Round
251
271
kl1(1)
FL
FL-1
kl2(1)
k7(1), k8(1), k9(1)
k10(1), k11(1), k12(1)
220
253
273
kl3(1)
kl4(1)
k13(1), k14(1), k15(1)
k16(1), k17(1), k18(1)
230
L18(1)
R18(1)
kw2(q)
C(q)
10
F
40
280
290
281
291
282
292
283
293
284
294
285
295
L6(1)
R6(1)

图 3

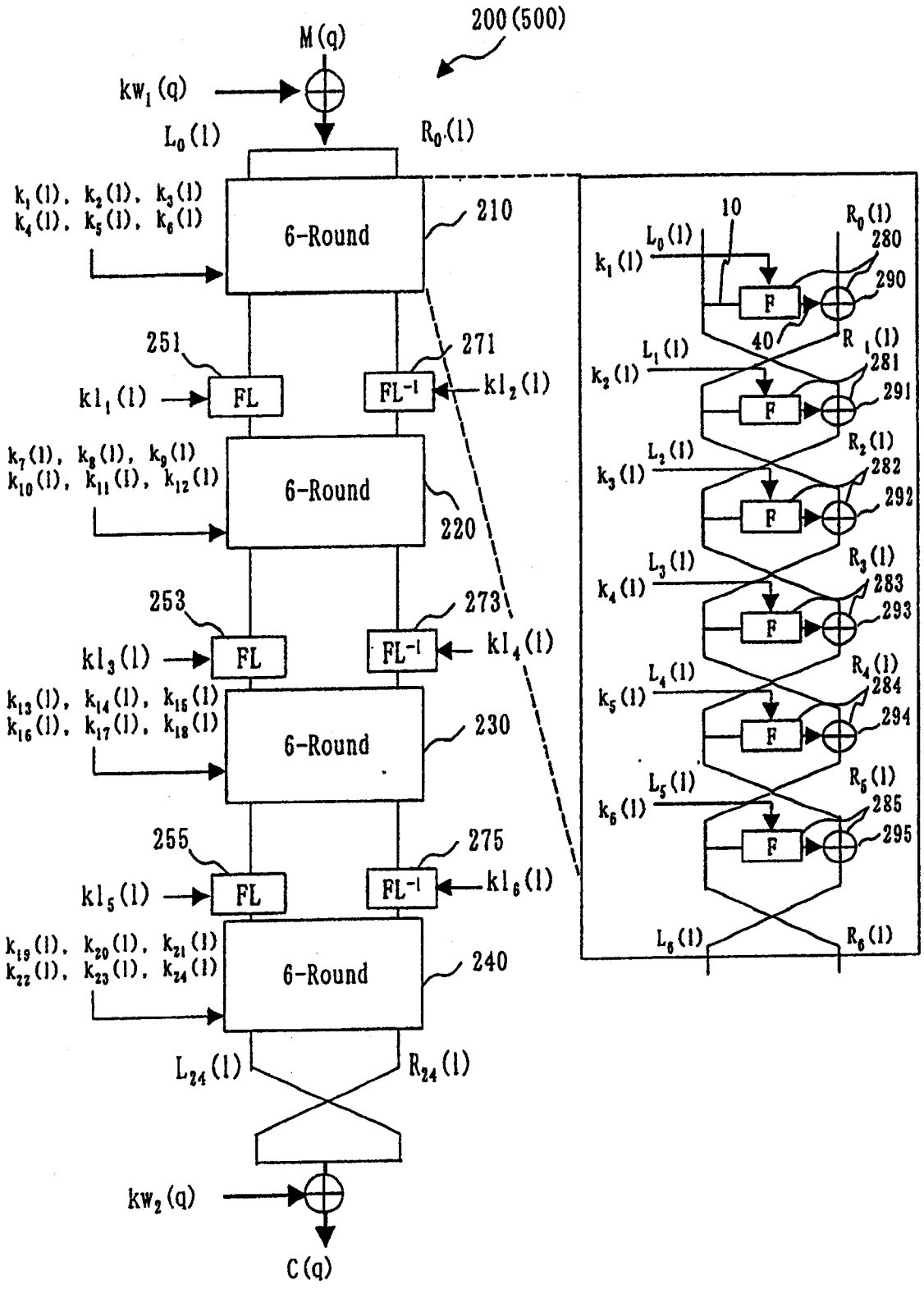

200(500)
M(q)
kw1(q)
L0(1)
R0(1)
k1(1), k2(1), k3(1)
k4(1), k5(1), k6(1)
6-Round
210
251
271
kl1(1)
FL
FL-1
kl2(1)
k7(1), k8(1), k9(1)
k10(1), k11(1), k12(1)
6-Round
220
253
273
kl3(1)
FL
FL-1
kl4(1)
k13(1), k14(1), k15(1)
k16(1), k17(1), k18(1)
6-Round
230
255
275
kl5(1)
FL
FL-1
kl6(1)
k19(1), k20(1), k21(1)
k22(1), k23(1), k24(1)
6-Round
240
L24(1)
R24(1)
kw2(q)
C(q)
10
40
F
280
281
282
283
284
285
290
291
292
293
294
295
L1(1)
L2(1)
L3(1)
L4(1)
L5(1)
L6(1)
R1(1)
R2(1)
R3(1)
R4(1)
R5(1)
R6(1)
k1(1)
k2(1)
k3(1)
k4(1)
k5(1)
k6(1)

图 4

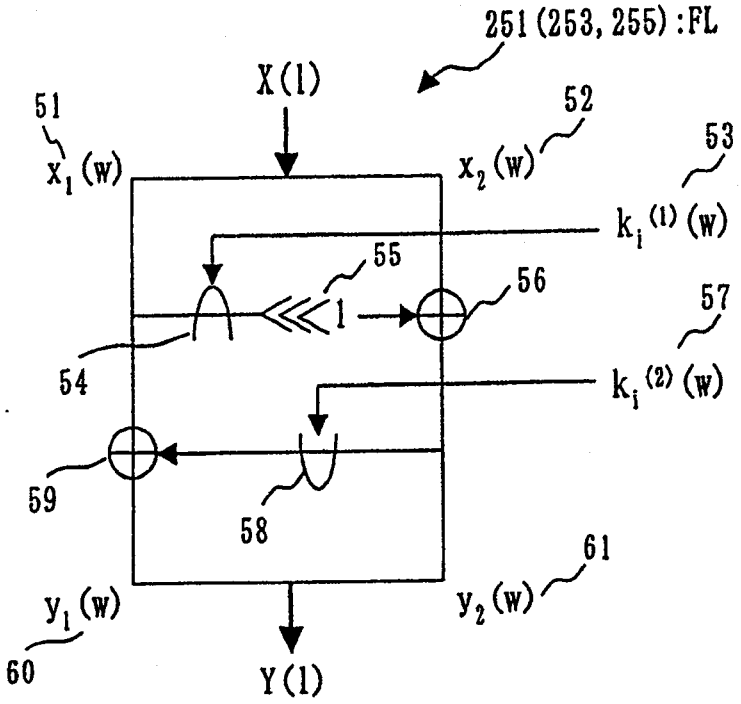

251(253, 255):FL
X(1)
51
$x_1(w)$
52
$x_2(w)$
53
$k_i^{(1)}(w)$
55
1
56
57
54
$k_i^{(2)}(w)$
59
58
61
$y_1(w)$
$y_2(w)$
60
Y(1)

图 5

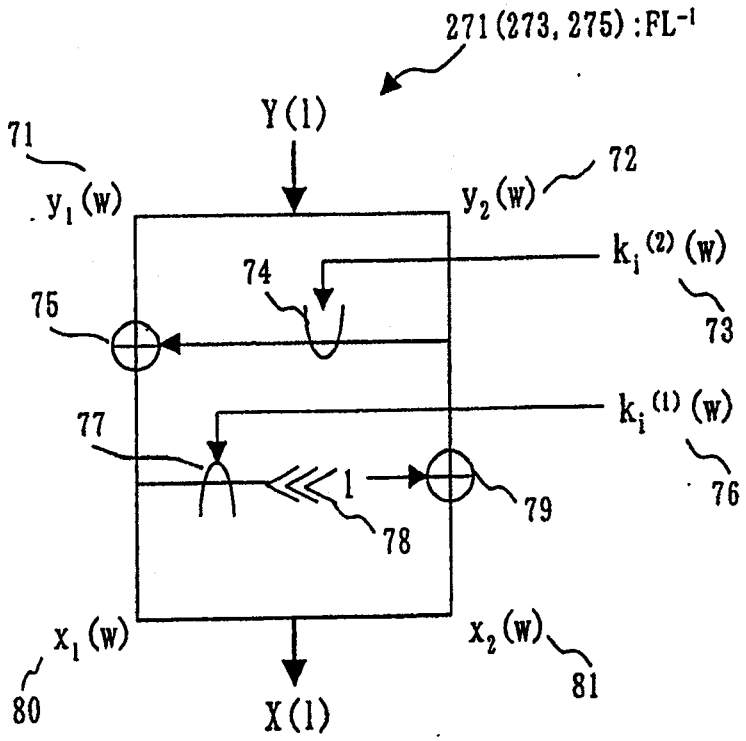

271(273,275):FL-1
Y(1)
71
y1(w)
y2(w)
72
ki(2)(w)
73
74
75
ki(1)(w)
76
77
1
78
79
x1(w)
80
x2(w)
81
X(1)

图 6

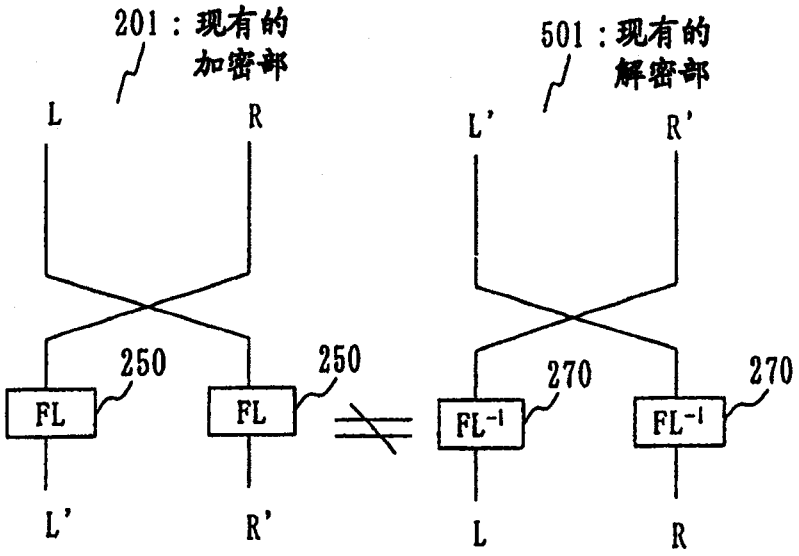


图 7

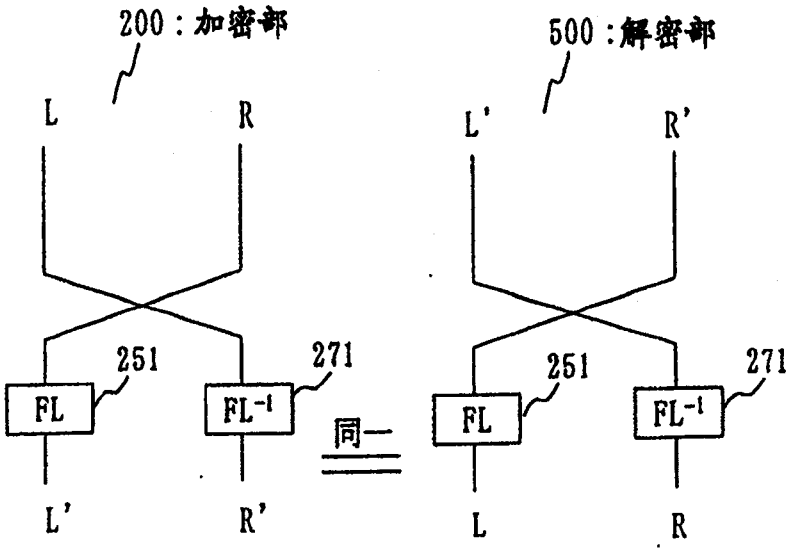


图 8

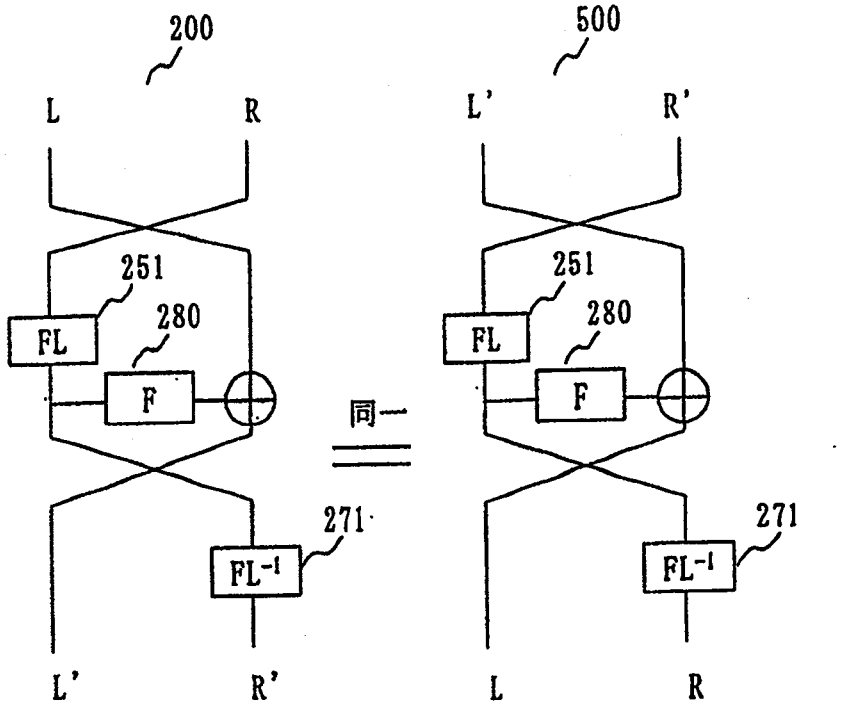


图 9

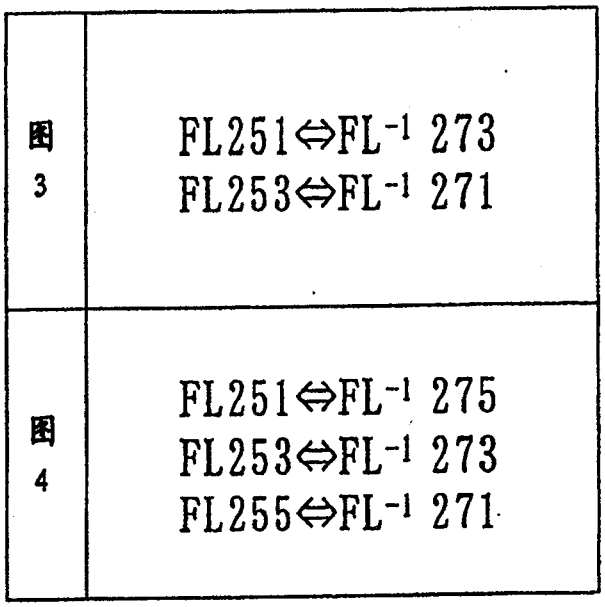


图 3
FL251⇔FL-1 273
FL253⇔FL-1 271
图 4
FL251⇔FL-1 275
FL253⇔FL-1 273
FL255⇔FL-1 271

图 10

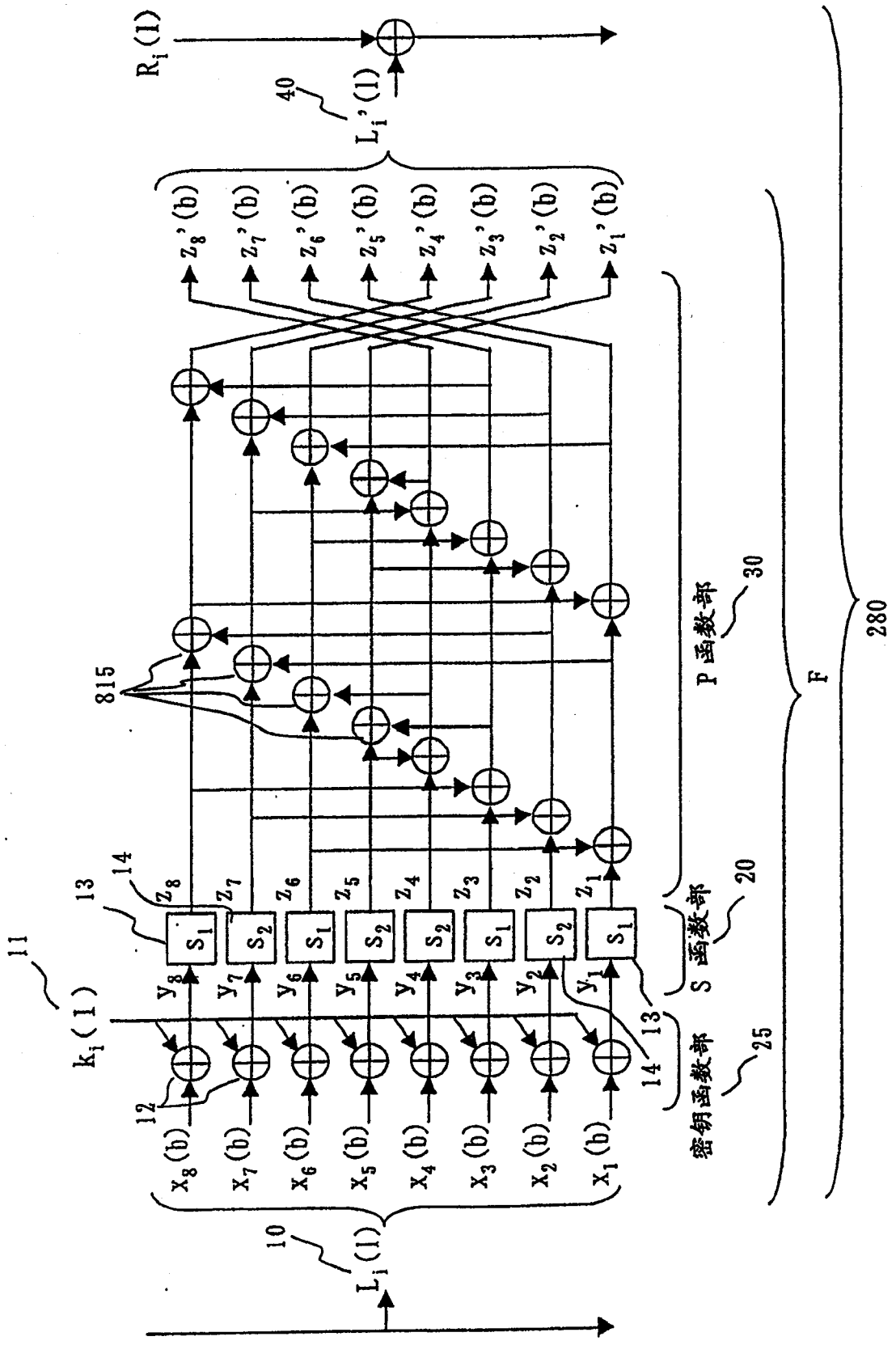

$R_i(l)$
40
$L_i'(l)$
$z_8'(b)$ $z_7'(b)$ $z_6'(b)$ $z_5'(b)$ $z_4'(b)$ $z_3'(b)$ $z_2'(b)$ $z_1'(b)$
815
P函数部
30
F
280
S函数部
20
密钥函数部
25
11
$k_i(l)$
13
14
z_8 z_7 z_6 z_5 z_4 z_3 z_2 z_1
S_1 S_2 S_1 S_2 S_2 S_1 S_2 S_1
y_8 y_7 y_6 y_5 y_4 y_3 y_2 y_1
12
$x_8(b)$ $x_7(b)$ $x_6(b)$ $x_5(b)$ $x_4(b)$ $x_3(b)$ $x_2(b)$ $x_1(b)$
10
$L_i(l)$

图 11

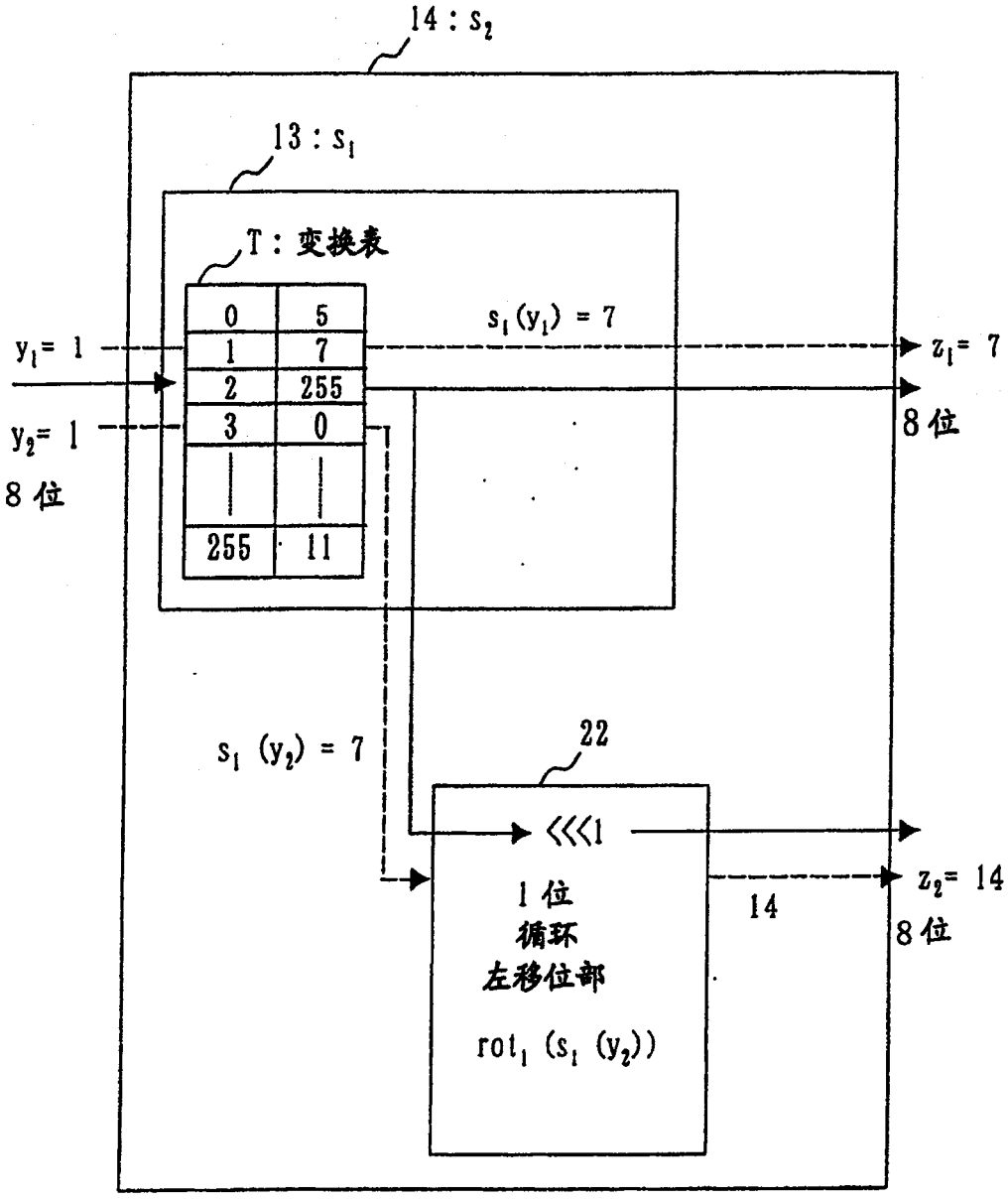
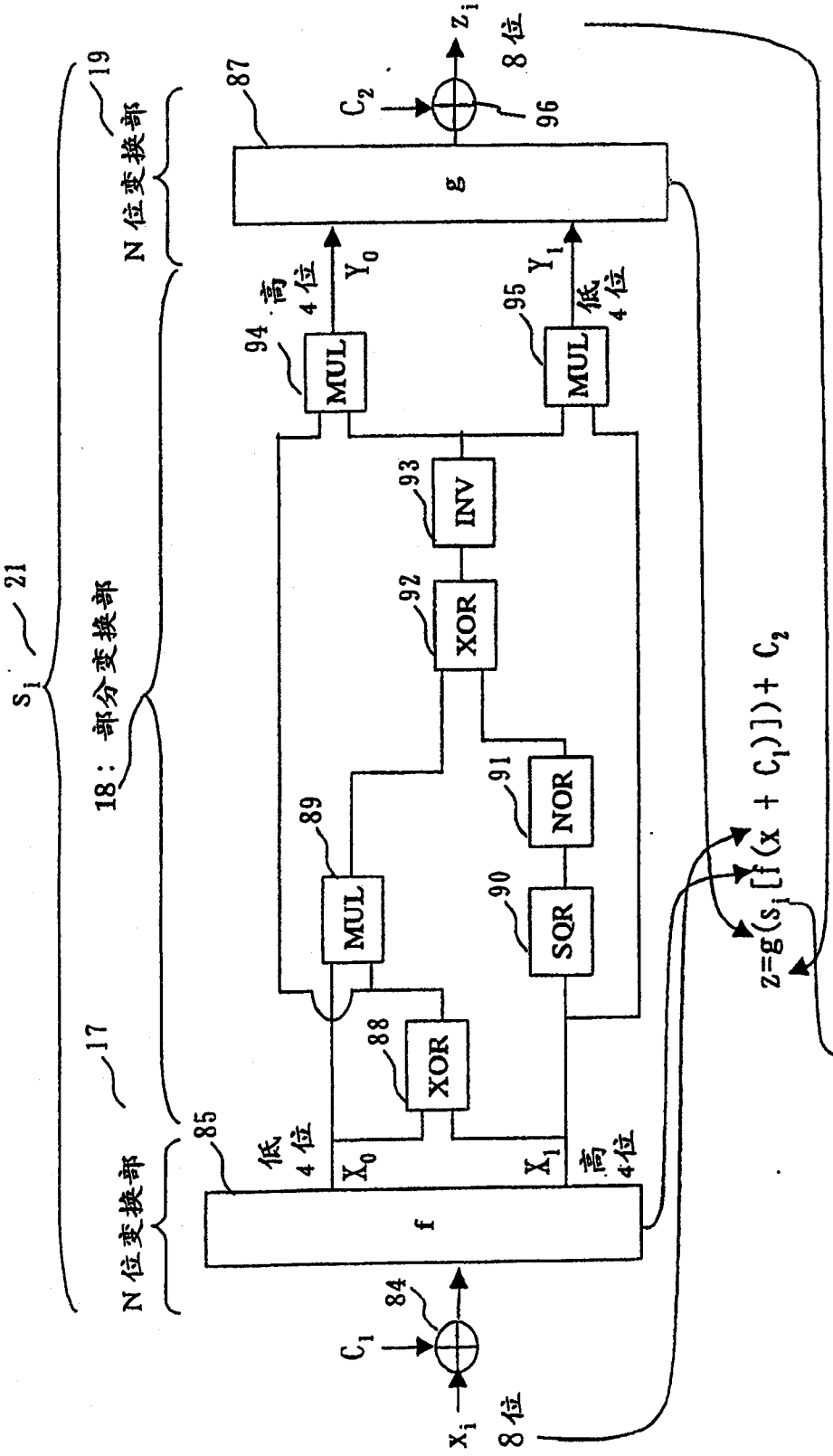

14 : s_2
13 : s_1
T : 变换表
0 5
1 7
2 255
3 0
255 11
y_1= 1
y_2= 1
8 位
$s_1(y_1)$ = 7
z_1= 7
8 位
$s_1(y_2)$ = 7
22
<<<1
1 位
循环
左移位部
$rot_1(s_1(y_2))$
14
z_2= 14
8 位

图 12



$$z=g(s_i[f(x+C_1)])+C_2$$

$$s_i[f(x+C_1)])=Y_0+Y_1\beta$$

$$=1/(X_0+X_1\beta)$$

$$=(X_0+X_1+X_1\beta)/((X_0+X_1)\cdot X_0+X_1\cdot X_1\cdot Nr(\beta))$$

88·94 95 93 88 89 92 90 91

X_0、X_1、Y_0、$Y_1\in GF(16)$

图 13

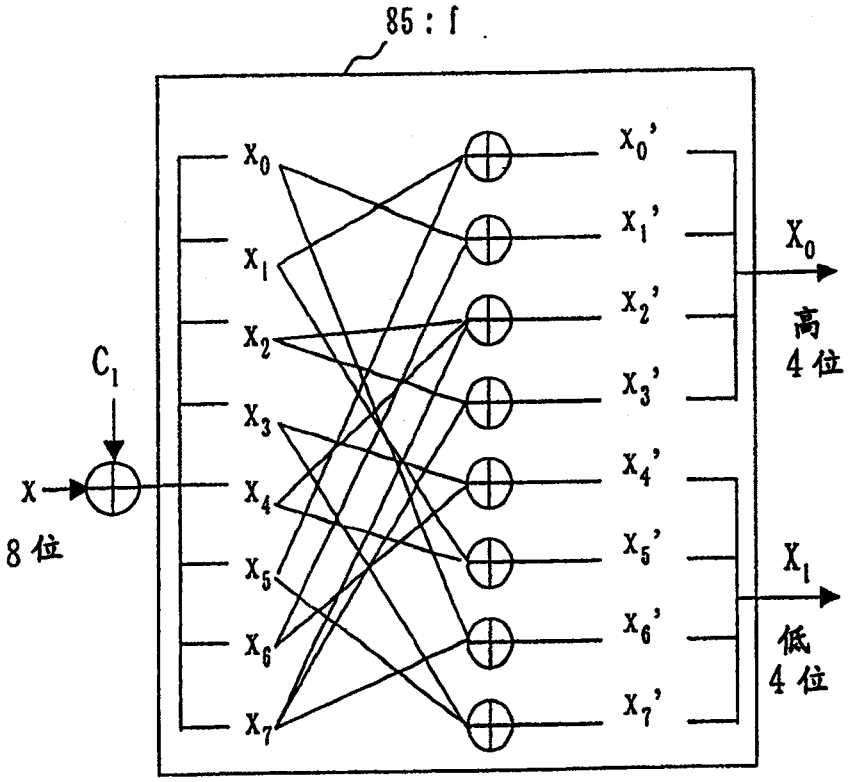

85 : 1
X0
X1
X2
X3
X4
X5
X6
X7
X0'
X1'
X2'
X3'
X4'
X5'
X6'
X7'
C1
X
8 位
X0
高
4 位
X1
低
4 位

图 14

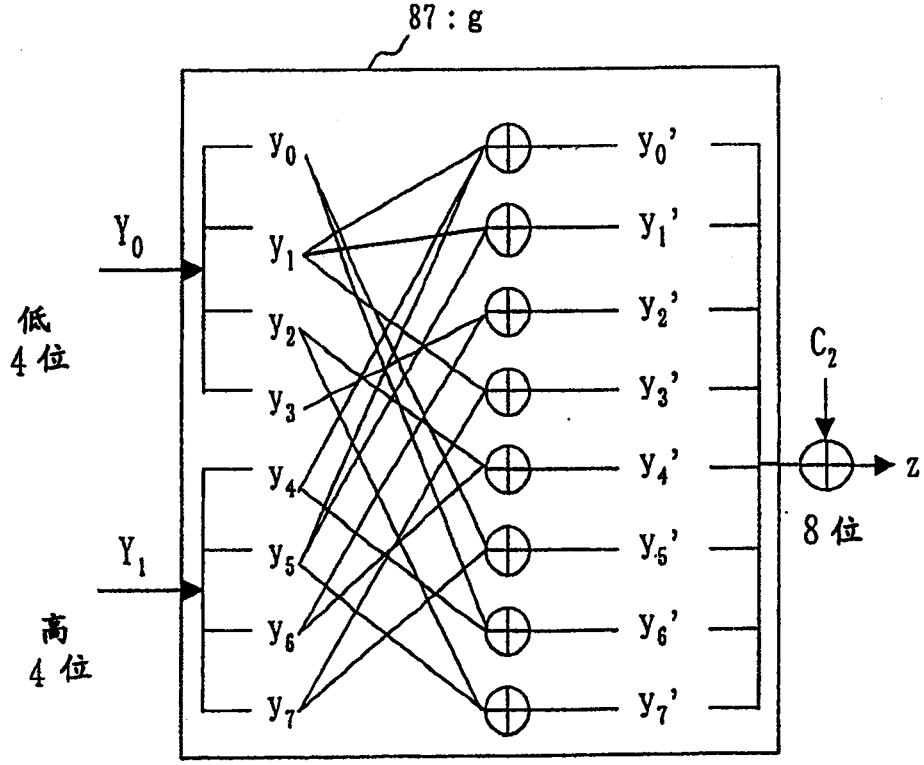

87 : g
Y_0
低
4 位
Y_1
高
4 位
y_0
y_1
y_2
y_3
y_4
y_5
y_6
y_7
y_0'
y_1'
y_2'
y_3'
y_4'
y_5'
y_6'
y_7'
C_2
z
8 位

图 15

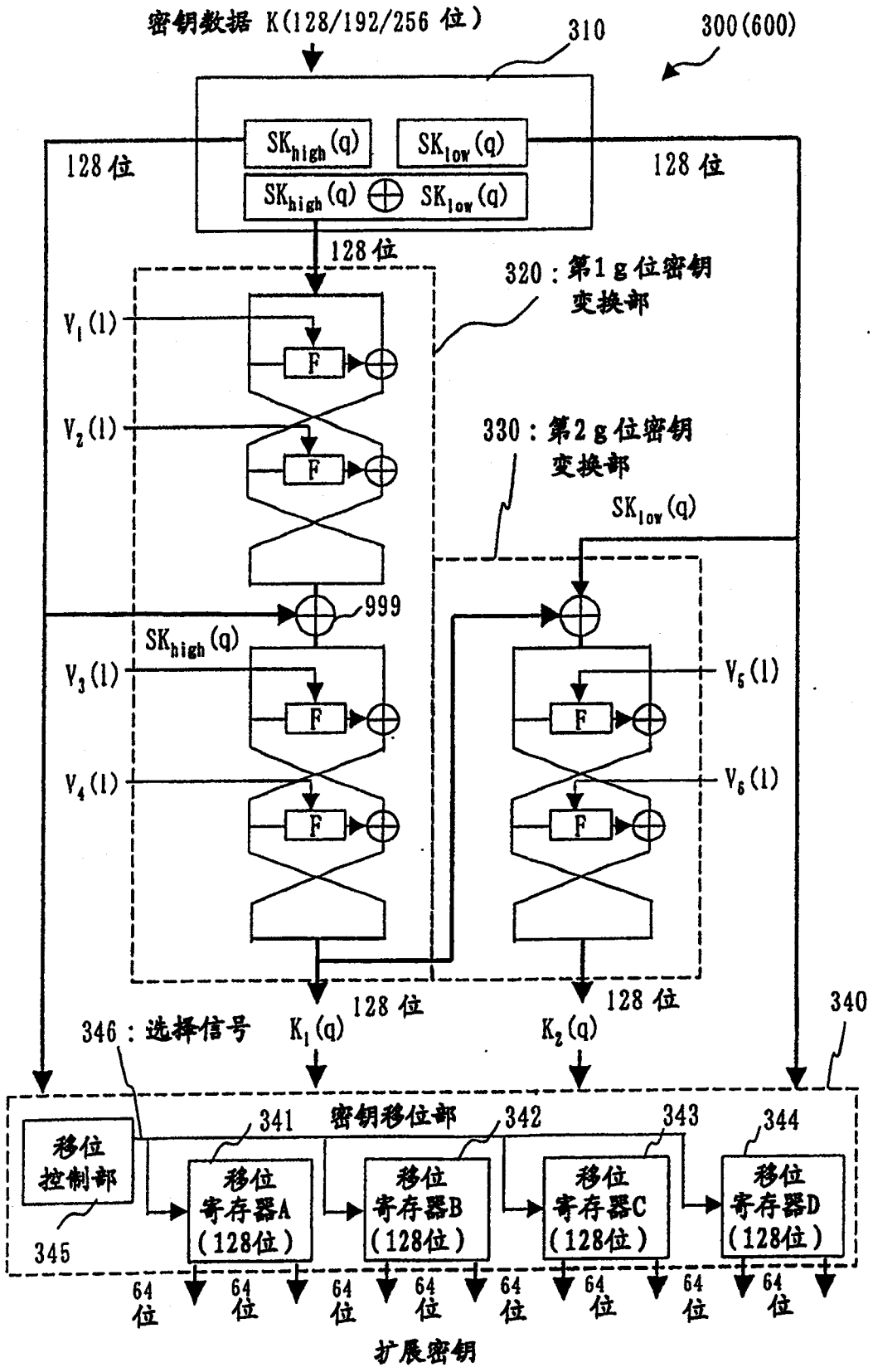

密钥数据 K(128/192/256 位)
310
300(600)
$SK_{high}(q)$
$SK_{low}(q)$
$SK_{high}(q) \oplus SK_{low}(q)$
128 位
128 位
128 位
320：第1 g 位密钥变换部
$V_1(1)$
$V_2(1)$
F
330：第2 g 位密钥变换部
$SK_{low}(q)$
999
$SK_{high}(q)$
$V_3(1)$
$V_4(1)$
$V_5(1)$
$V_6(1)$
128 位
128 位
340
346：选择信号
$K_1(q)$
$K_2(q)$
密钥移位部
341
342
343
344
移位控制部
移位寄存器A (128位)
移位寄存器B (128位)
移位寄存器C (128位)
移位寄存器D (128位)
345
64 位
扩展密钥

图 16

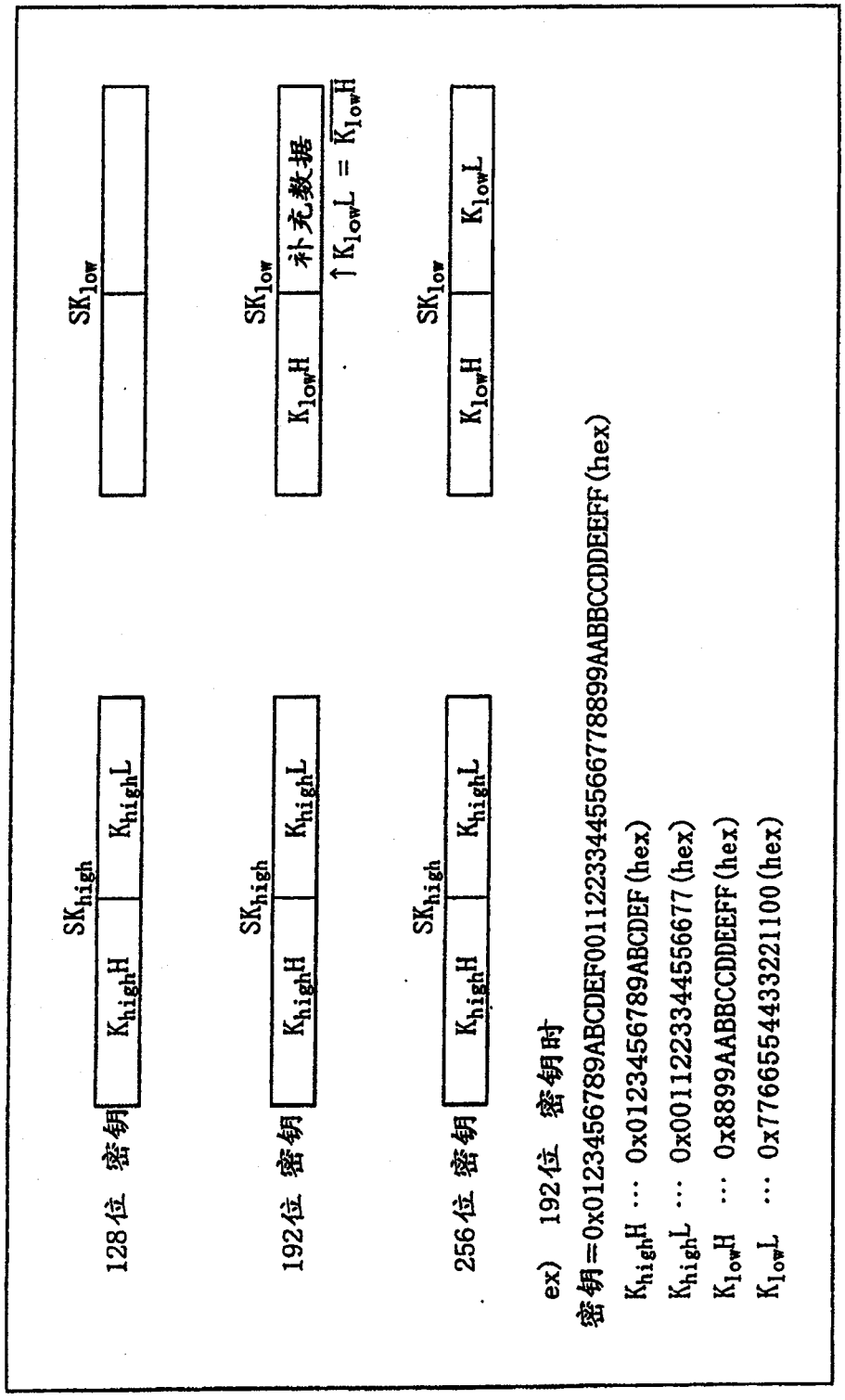

SK_high
SK_low
128位 密钥
K_highH
K_highL
192位 密钥
补充数据
↑K_lowL = ~K_lowH
256位 密钥
K_lowH
K_lowL
ex) 192位 密钥时
密钥=0x0123456789ABCDEF0011223344556677899AABBCCDDEEFF(hex)
K_highH … 0x0123456789ABCDEF(hex)
K_highL … 0x0011223344556677(hex)
K_lowH … 0x8899AABBCCDDEEFF(hex)
K_lowL … 0x7766554433221100(hex)

图 17

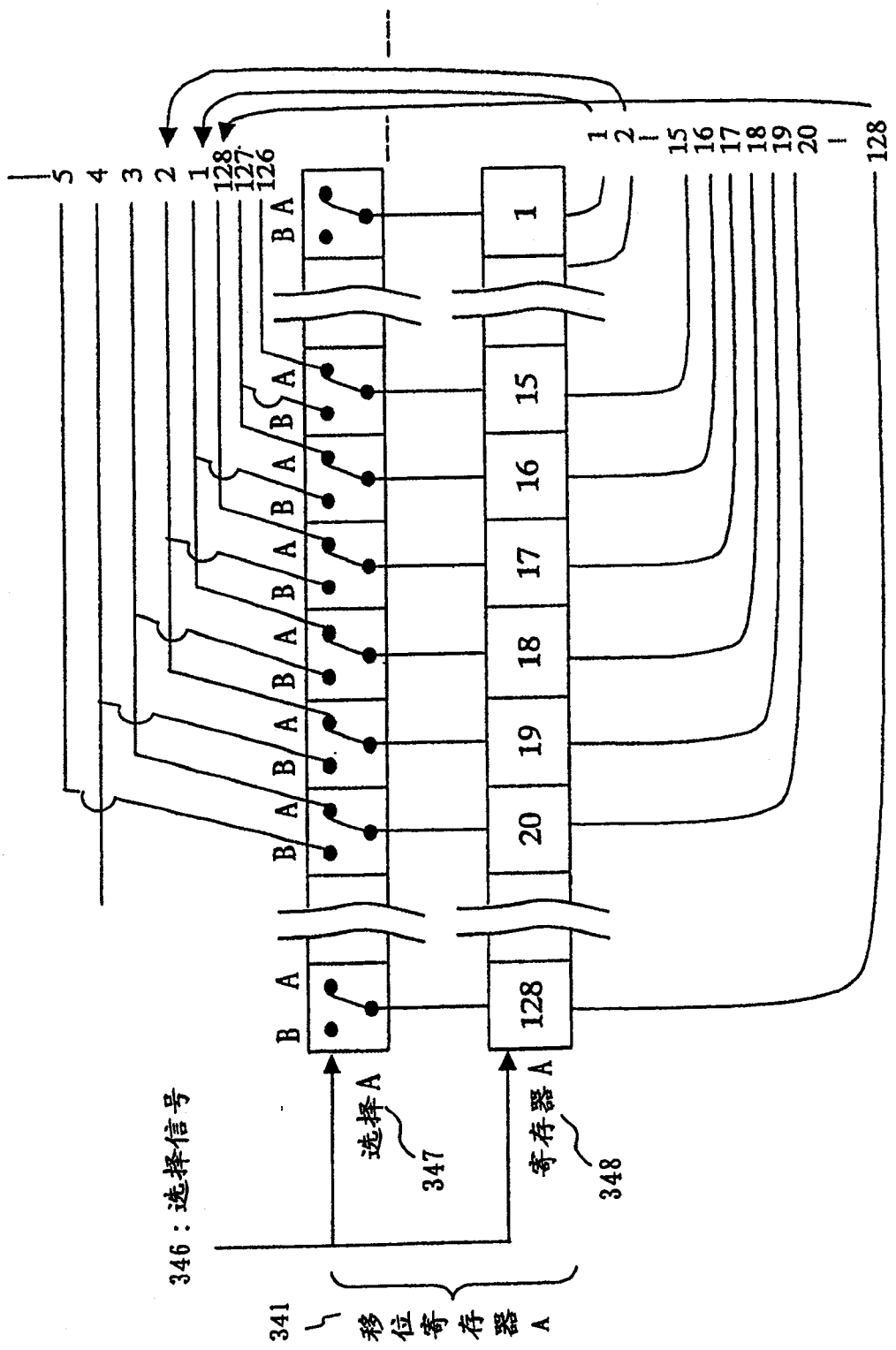
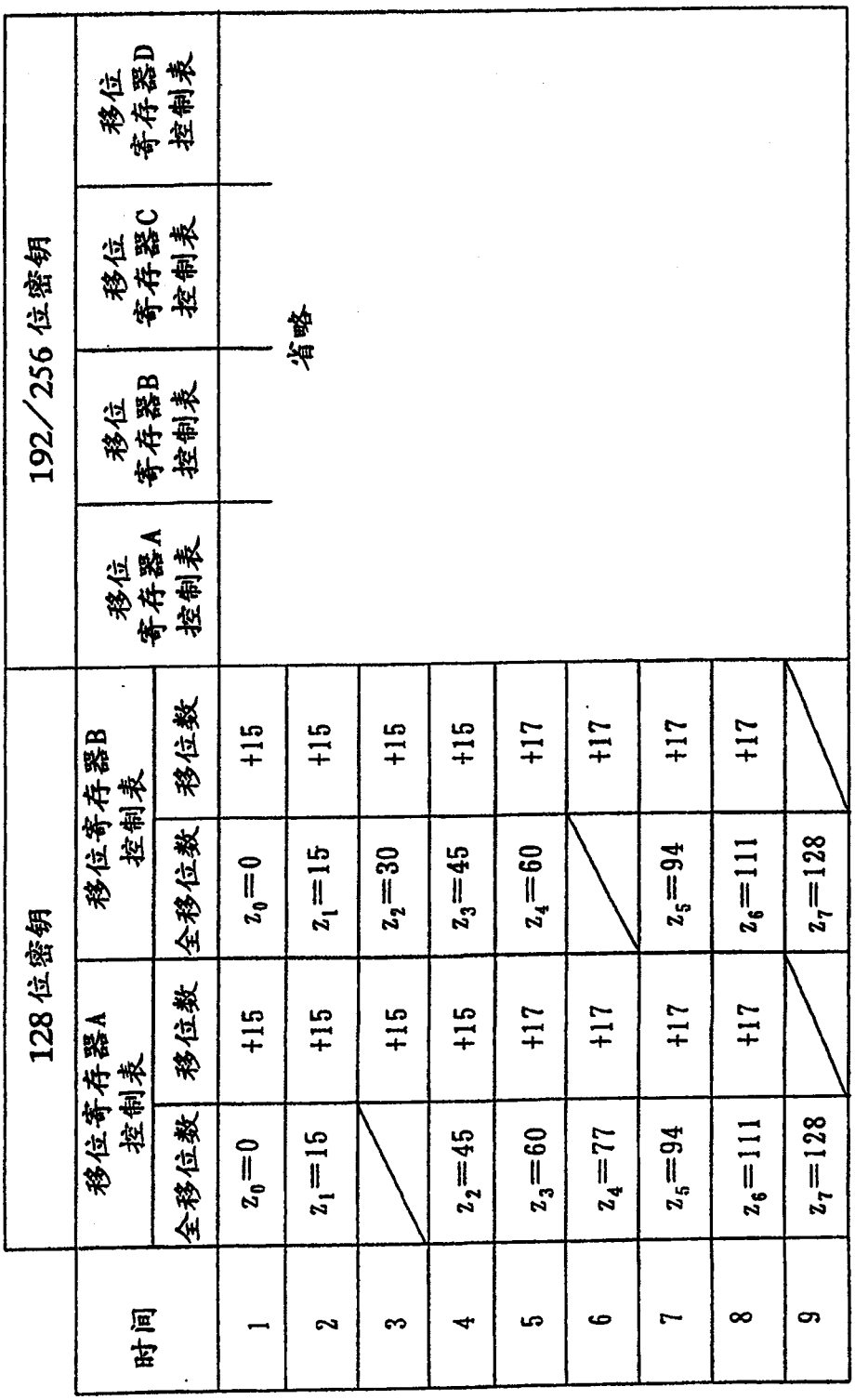

346：选择信号
341
移位寄存器A
选择A
347
寄存器A
348
B A
1
2
15
16
17
18
19
20
128
5
4
3
2
1
128
127
126

图 18



时间	128位密钥				192/256位密钥			
	移位寄存器A控制表		移位寄存器B控制表		移位寄存器A控制表	移位寄存器B控制表	移位寄存器C控制表	移位寄存器D控制表
	全移位数	移位数	全移位数	移位数	省略			
1	$z_0=0$	+15	$z_0=0$	+15				
2	$z_1=15$	+15	$z_1=15$	+15				
3		+15	$z_2=30$	+15				
4	$z_2=45$	+15	$z_3=45$	+15				
5	$z_3=60$	+17	$z_4=60$	+17				
6	$z_4=77$	+17		+17				
7	$z_5=94$	+17	$z_5=94$	+17				
8	$z_6=111$	+17	$z_6=111$	+17				
9	$z_7=128$		$z_7=128$					

图 19

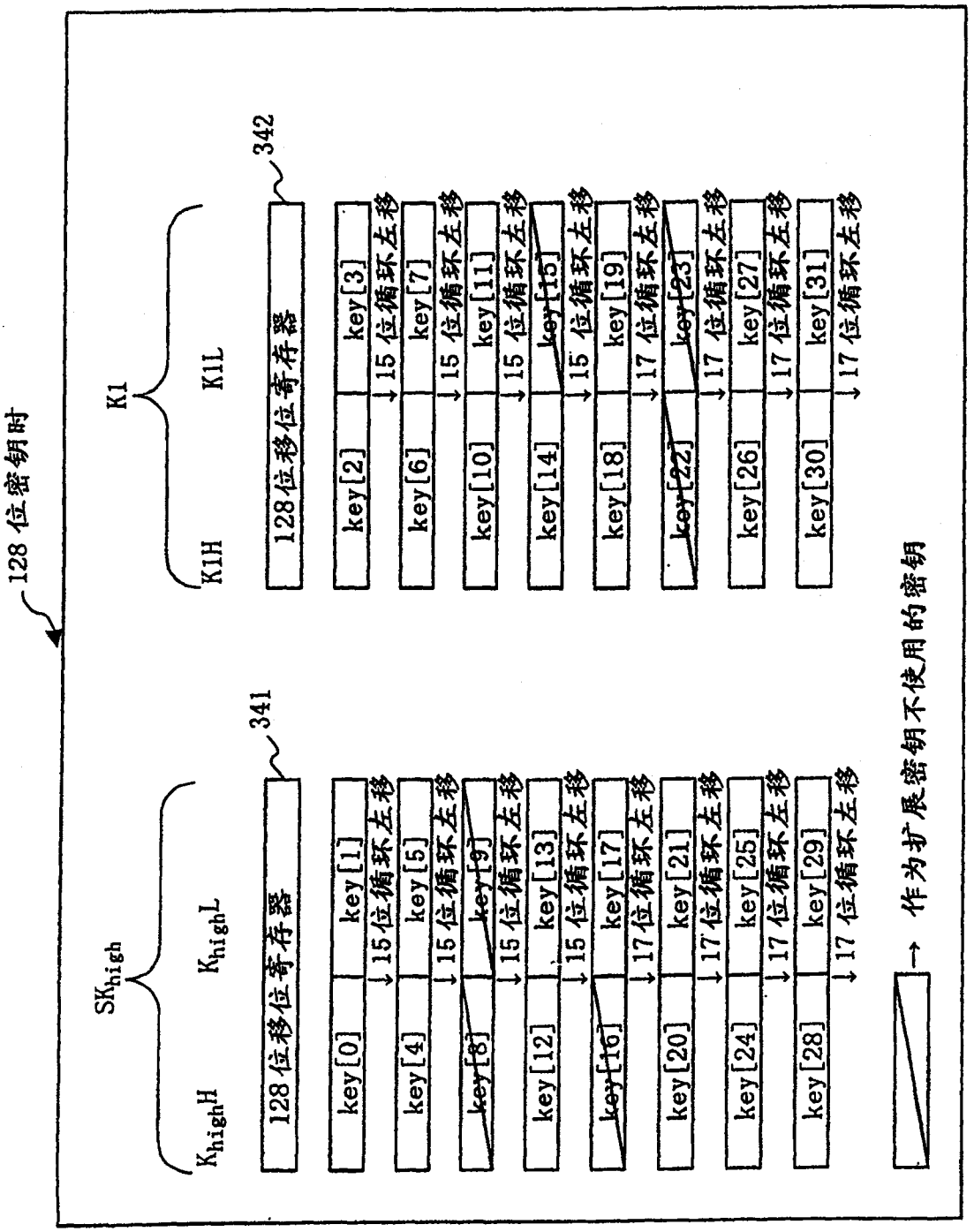

128 位密钥时
SK_{high}
$K_{high}H$
$K_{high}L$
341
128 位移位寄存器
key[0]
key[1]
15 位循环左移
key[4]
key[5]
15 位循环左移
key[8]
key[9]
15 位循环左移
key[12]
key[13]
15 位循环左移
key[16]
key[17]
17 位循环左移
key[20]
key[21]
17 位循环左移
key[24]
key[25]
17 位循环左移
key[28]
key[29]
17 位循环左移
作为扩展密钥不使用的密钥
K1
K1H
K1L
342
128 位移位寄存器
key[2]
key[3]
15 位循环左移
key[6]
key[7]
15 位循环左移
key[10]
key[11]
15 位循环左移
key[14]
key[15]
15 位循环左移
key[18]
key[19]
17 位循环左移
key[22]
key[23]
17 位循环左移
key[26]
key[27]
17 位循环左移
key[30]
key[31]
17 位循环左移

图 20

输入的	kw1	key[0]	key[1]
第1段	k1	key[2]	
第2段	k2	key[3]	
第3段	k3	key[4]	
第4段	k4	key[5]	
第5段	k5	key[6]	
第6段	k6	key[7]	
FL, FL^{-1}	k11 , k12	key[10]	key[11]
第7段	k7	key[12]	
第8段	k8	key[13]	
第9段	k9	key[14]	
第10段	k10	key[17]	
第11段	k11	key[18]	
第12段	k12	key[19]	
FL, FL^{-1}	k13 , k14	key[20]	key[21]
第13段	k13	key[24]	
第14段	k14	key[25]	
第15段	k15	key[26]	
第16段	k16	key[27]	
第17段	k17	key[28]	
第18段	k18	key[29]	
输出的	kw2	key[30]	key[31]

图 21

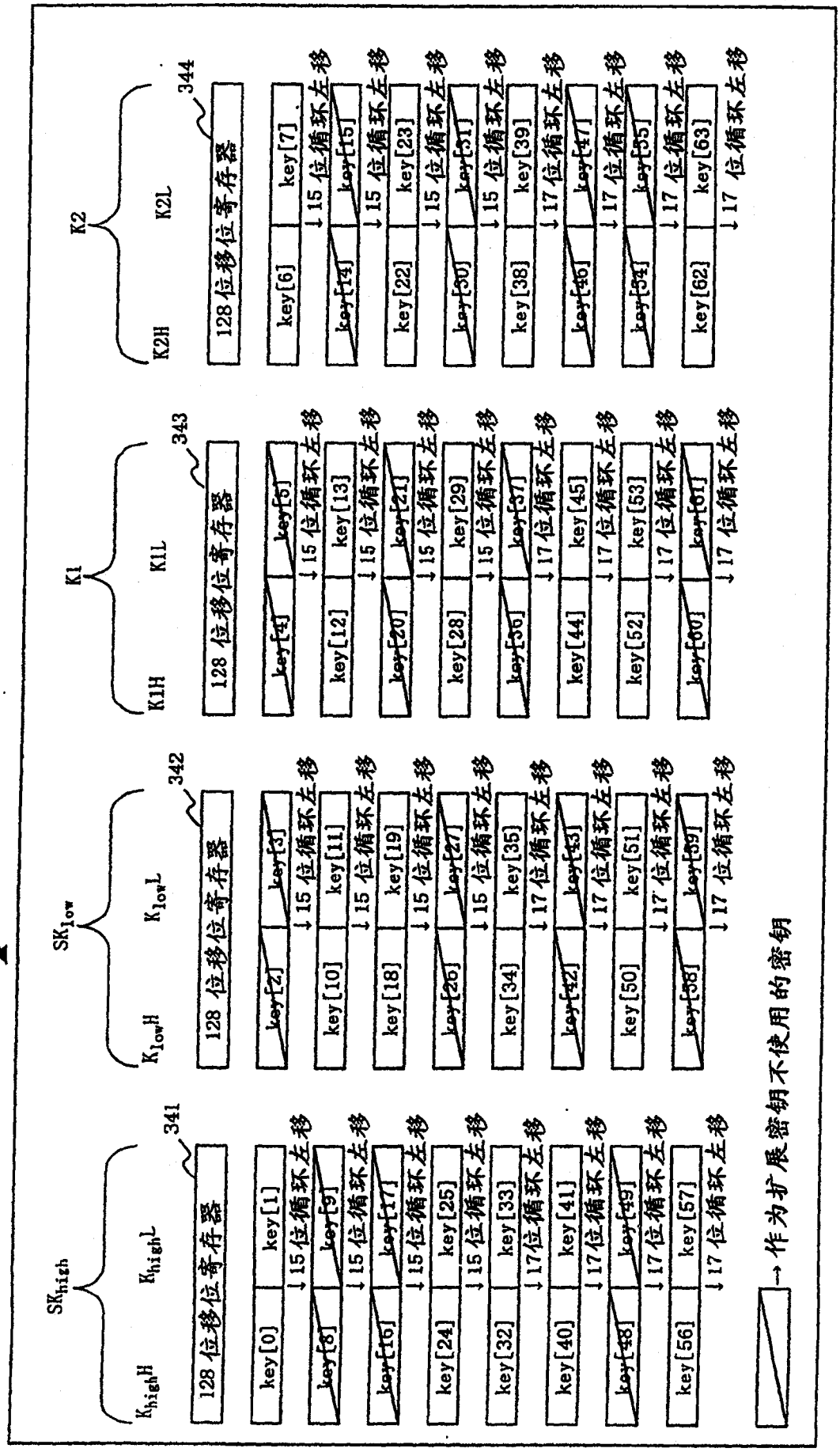

192位或256位密钥时
SK_high
K_high^H
K_high^L
341
128 位移位寄存器
SK_low
K_low^H
K_low^L
342
128 位移位寄存器
K1
K1H
K1L
343
128 位移位寄存器
K2
K2H
K2L
344
128 位移位寄存器
key[0]
key[1]
key[2]
key[3]
key[4]
key[5]
key[6]
key[7]
key[8]
key[9]
key[10]
key[11]
key[12]
key[13]
key[14]
key[15]
key[16]
key[17]
key[18]
key[19]
key[20]
key[21]
key[22]
key[23]
key[24]
key[25]
key[26]
key[27]
key[28]
key[29]
key[30]
key[31]
key[32]
key[33]
key[34]
key[35]
key[36]
key[37]
key[38]
key[39]
key[40]
key[41]
key[42]
key[43]
key[44]
key[45]
key[46]
key[47]
key[48]
key[49]
key[50]
key[51]
key[52]
key[53]
key[54]
key[55]
key[56]
key[57]
key[58]
key[59]
key[60]
key[61]
key[62]
key[63]
↓15 位循环左移
↓17 位循环左移
→作为扩展密钥不使用的密钥

图 22

输入的	kw1	key[0]	key[1]
第1段	k1	key[6]	
第2段	k2	key[7]	
第3段	k3	key[10]	
第4段	k4	key[11]	
第5段	k5	key[12]	
第6段	k6	key[13]	
FL, FL^{-1}	k11 , k12	key[18]	key[19]
第7段	k7	key[22]	
第8段	k8	key[23]	
第9段	k9	key[24]	
第10段	k10	key[25]	
第11段	k11	key[28]	
第12段	k12	key[29]	
FL, FL^{-1}	k13 , k14	key[32]	key[33]
第13段	k13	key[34]	
第14段	k14	key[35]	
第15段	k15	key[38]	
第16段	k16	key[39]	
第17段	k17	key[40]	
第18段	k18	key[41]	
FL, FL^{-1}	k15 , k16	key[44]	key[45]
第19段	k19	key[50]	
第20段	k20	key[51]	
第21段	k21	key[52]	
第22段	k22	key[53]	
第23段	k23	key[56]	
第24段	k24	key[57]	
输出的	kw2	key[62]	key[63]

图 23

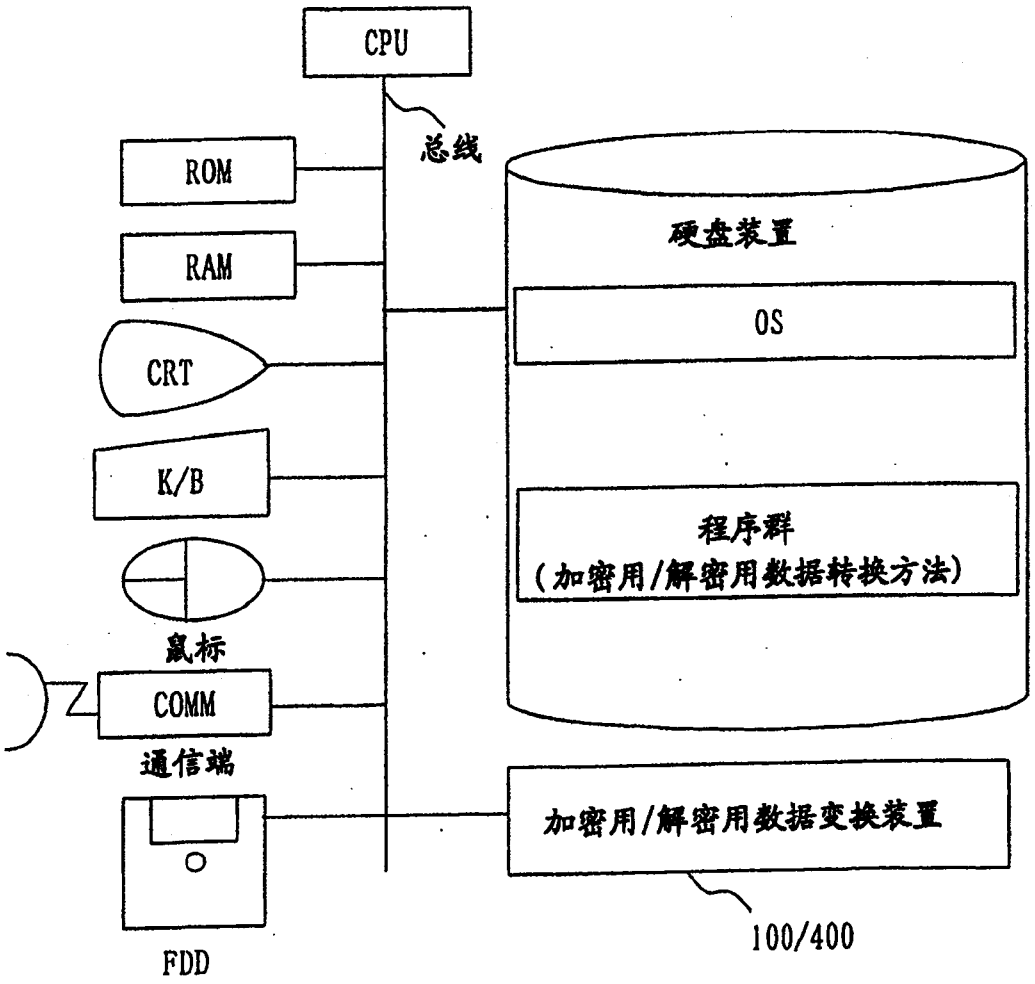

CPU
总线
ROM
RAM
CRT
K/B
鼠标
COMM
通信端
FDD
硬盘装置
OS
程序群
(加密用/解密用数据转换方法)
加密用/解密用数据变换装置
100/400

图 24

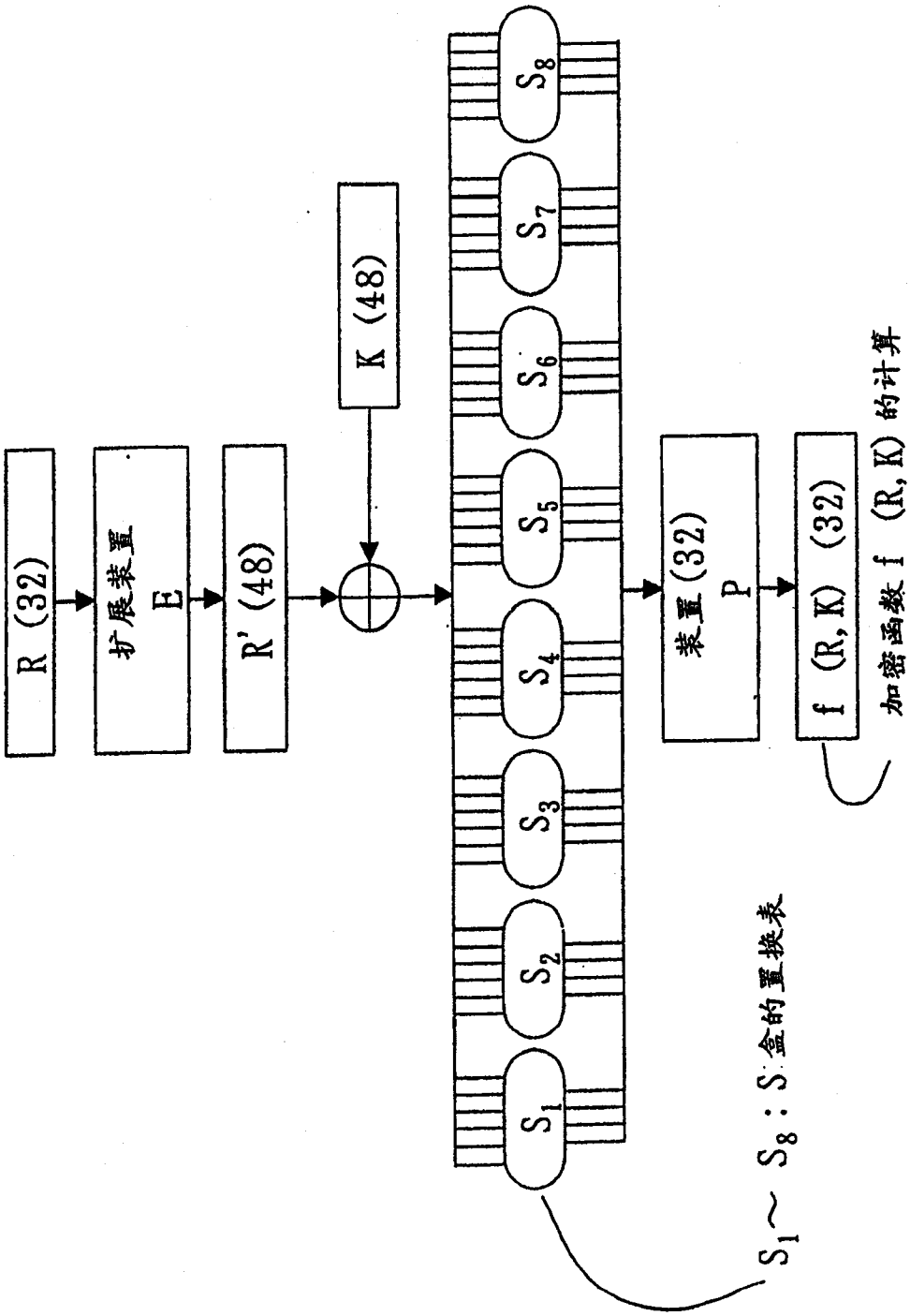

R (32)
扩展装置
E
R' (48)
K (48)
S1
S2
S3
S4
S5
S6
S7
S8
装置 (32)
P
f (R, K) (32)
加密函数 f (R, K) 的计算
S1～S8：S盒的置换表

图 25

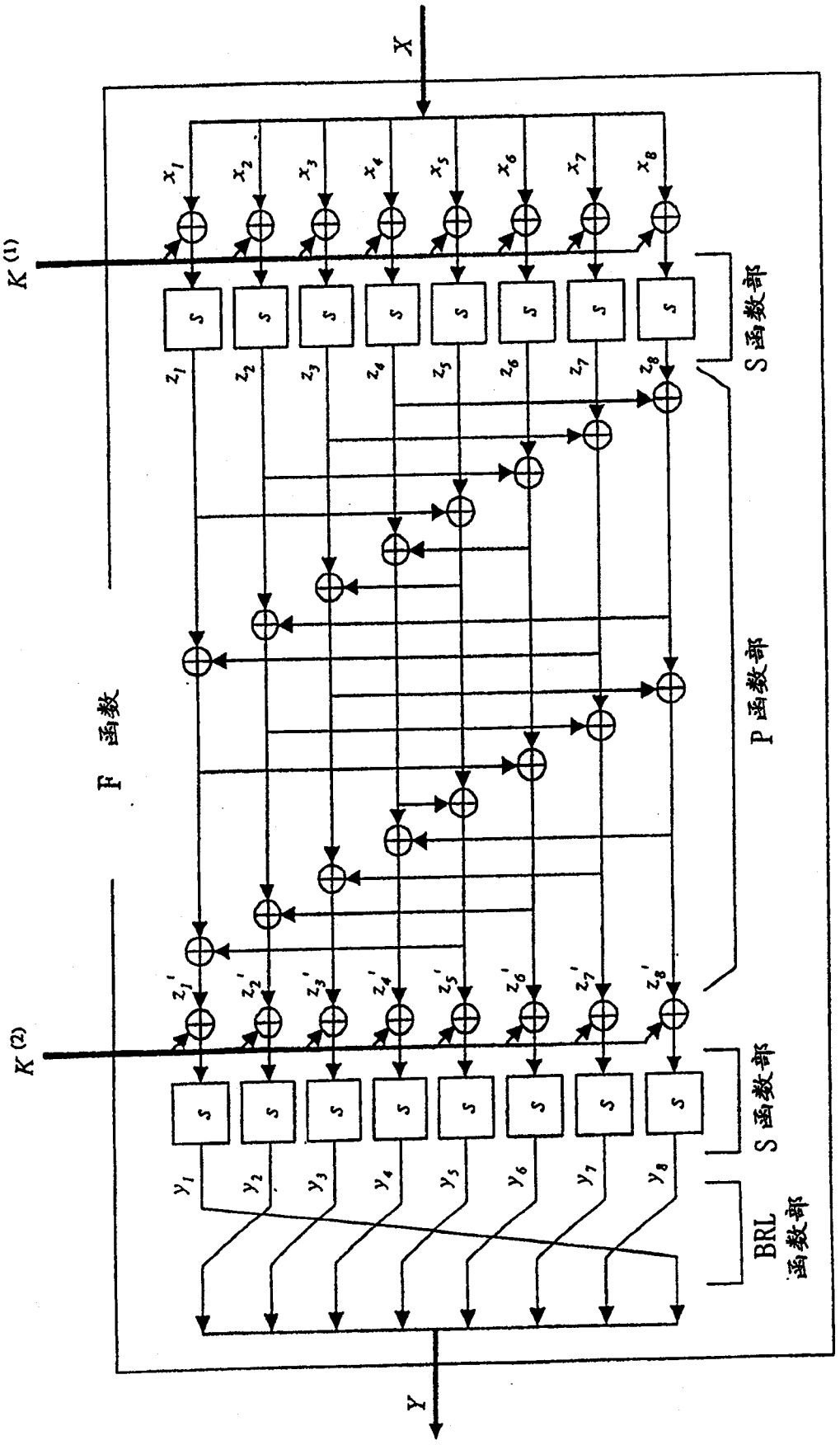


图 26

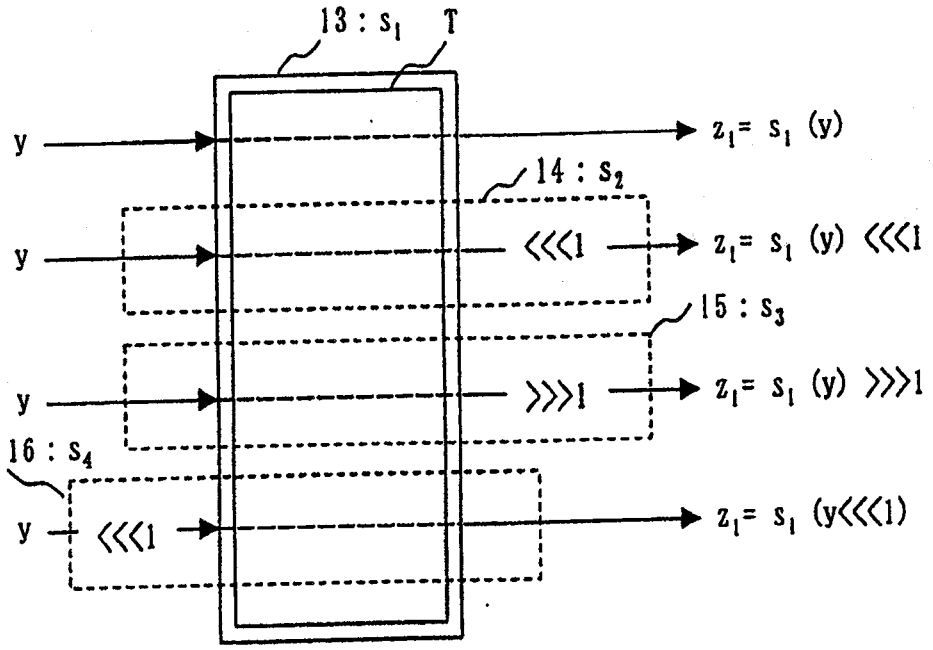


图 27

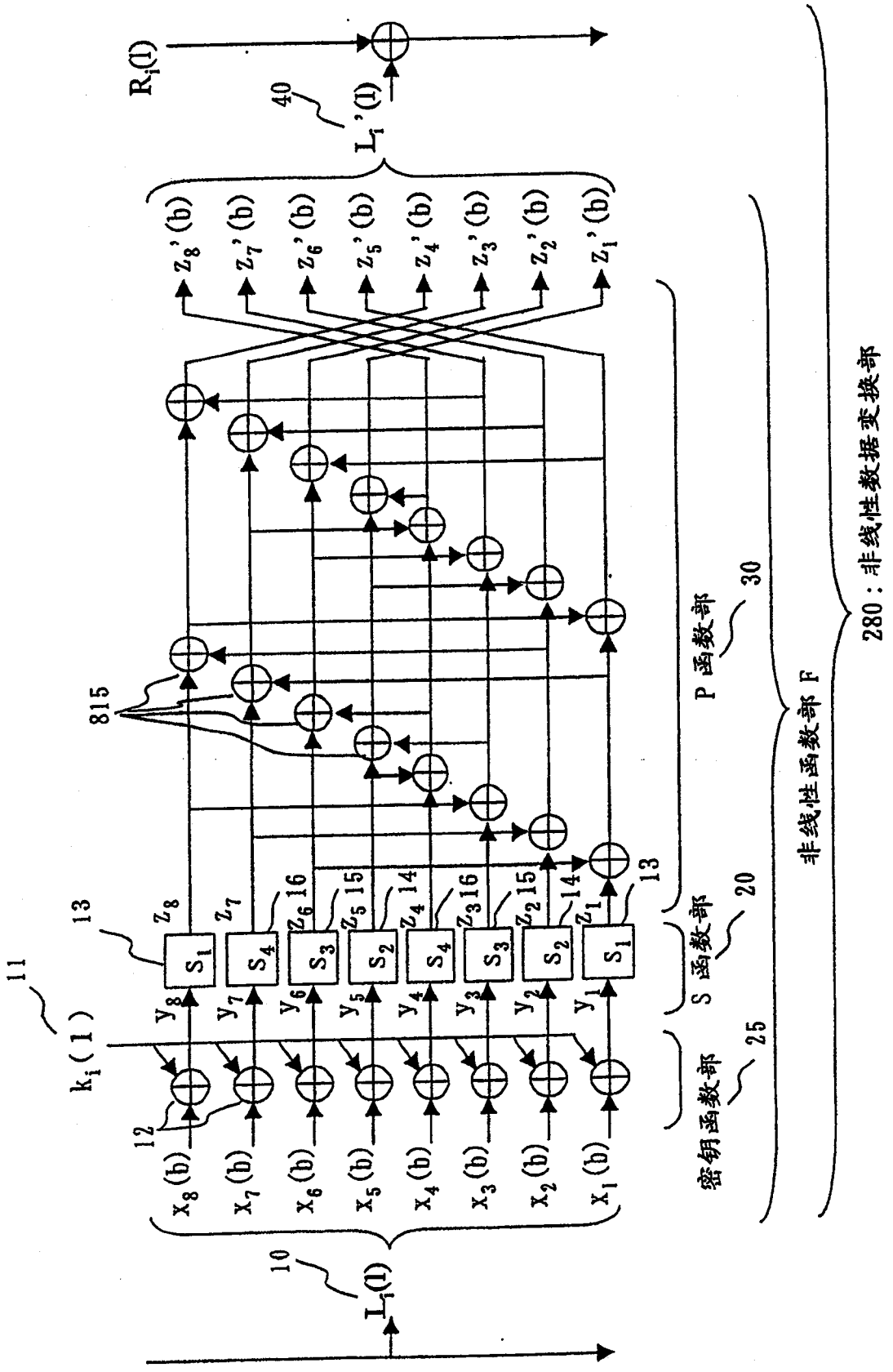

$R_i(l)$
40
$L_i'(l)$
$z_8'(b)$ $z_7'(b)$ $z_6'(b)$ $z_5'(b)$ $z_4'(b)$ $z_3'(b)$ $z_2'(b)$ $z_1'(b)$
815
13
z_8 z_7 z_6 16 z_5 15 z_4 14 z_3 16 z_2 15 14 z_1
S_1 S_4 S_3 S_2 S_4 S_3 S_2 S_1
y_8 y_7 y_6 y_5 y_4 y_3 y_2 y_1
11
$k_i(l)$
12
$x_8(b)$ $x_7(b)$ $x_6(b)$ $x_5(b)$ $x_4(b)$ $x_3(b)$ $x_2(b)$ $x_1(b)$
10
$L_i(l)$
密钥函数部 25
S 函数部 20
P 函数部 30
非线性函数部 F
280：非线性数据变换部

图 28

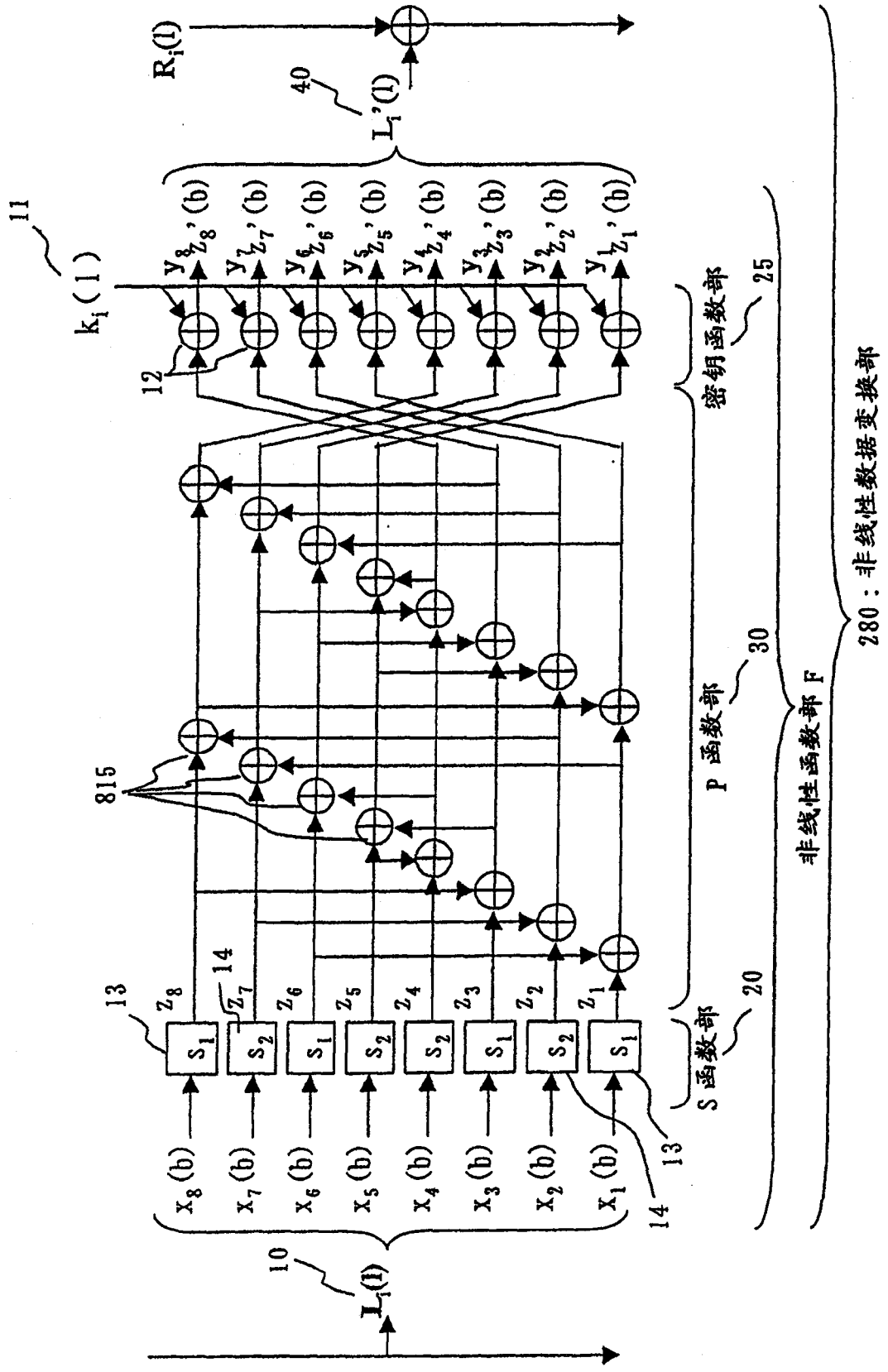

$R_i(l)$
40
$L_i'(l)$
11
$k_i(1)$
12
815
13
14
10
$L_i(l)$
密钥函数部 25
P 函数部 30
S 函数部 20
非线性函数部 F
280：非线性数据变换部

图 29

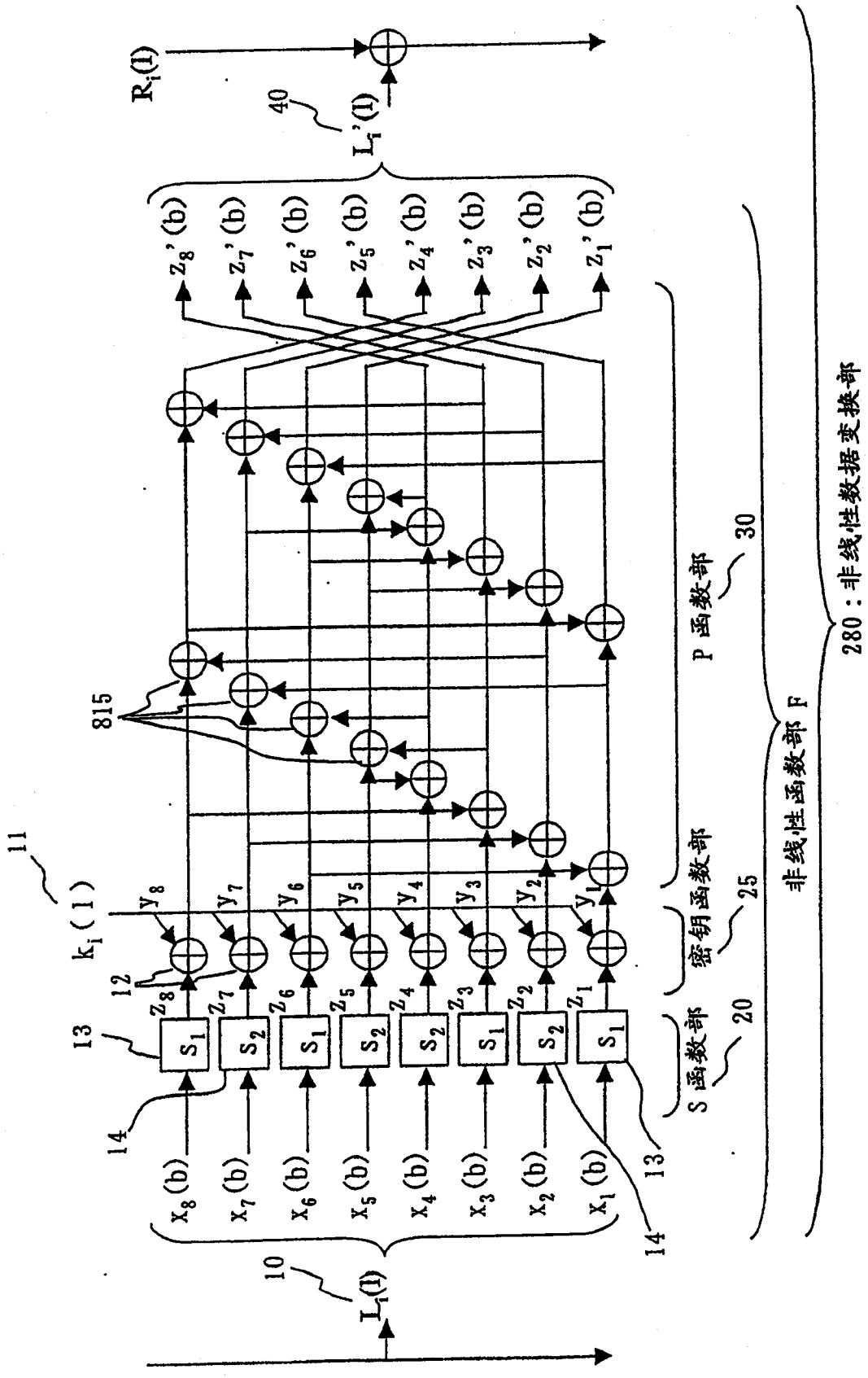

$R_i(l)$
40
$L_i'(l)$
$z_8'(b)$ $z_7'(b)$ $z_6'(b)$ $z_5'(b)$ $z_4'(b)$ $z_3'(b)$ $z_2'(b)$ $z_1'(b)$
815
11
$k_i(l)$
y_8 y_7 y_6 y_5 y_4 y_3 y_2 y_1
12
z_8 z_7 z_6 z_5 z_4 z_3 z_2 z_1
13
S_1 S_2 S_1 S_2 S_2 S_1 S_2 S_1
14
$x_8(b)$ $x_7(b)$ $x_6(b)$ $x_5(b)$ $x_4(b)$ $x_3(b)$ $x_2(b)$ $x_1(b)$
10
$L_i(l)$
S 函数部
20
密钥函数部
25
P 函数部
30
非线性函数部 F
280：非线性数据变换部

图 30

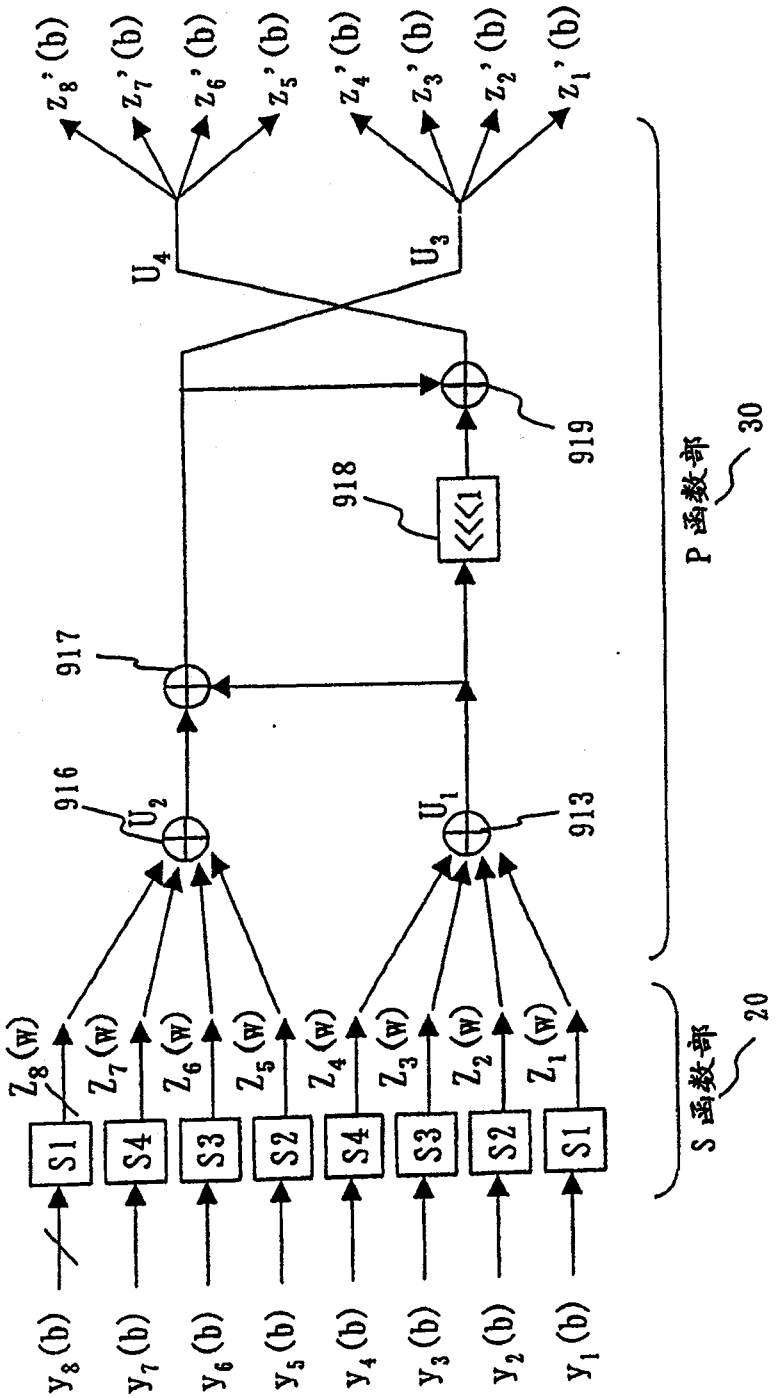

y8(b)
y7(b)
y6(b)
y5(b)
y4(b)
y3(b)
y2(b)
y1(b)
S1
S4
S3
S2
S4
S3
S2
S1
Z8(w)
Z7(w)
Z6(w)
Z5(w)
Z4(w)
Z3(w)
Z2(w)
Z1(w)
S 函数部
20
P 函数部
30
916
U2
917
U1
913
918
<<<1
919
U4
U3
z8'(b)
z7'(b)
z6'(b)
z5'(b)
z4'(b)
z3'(b)
z2'(b)
z1'(b)

图 31

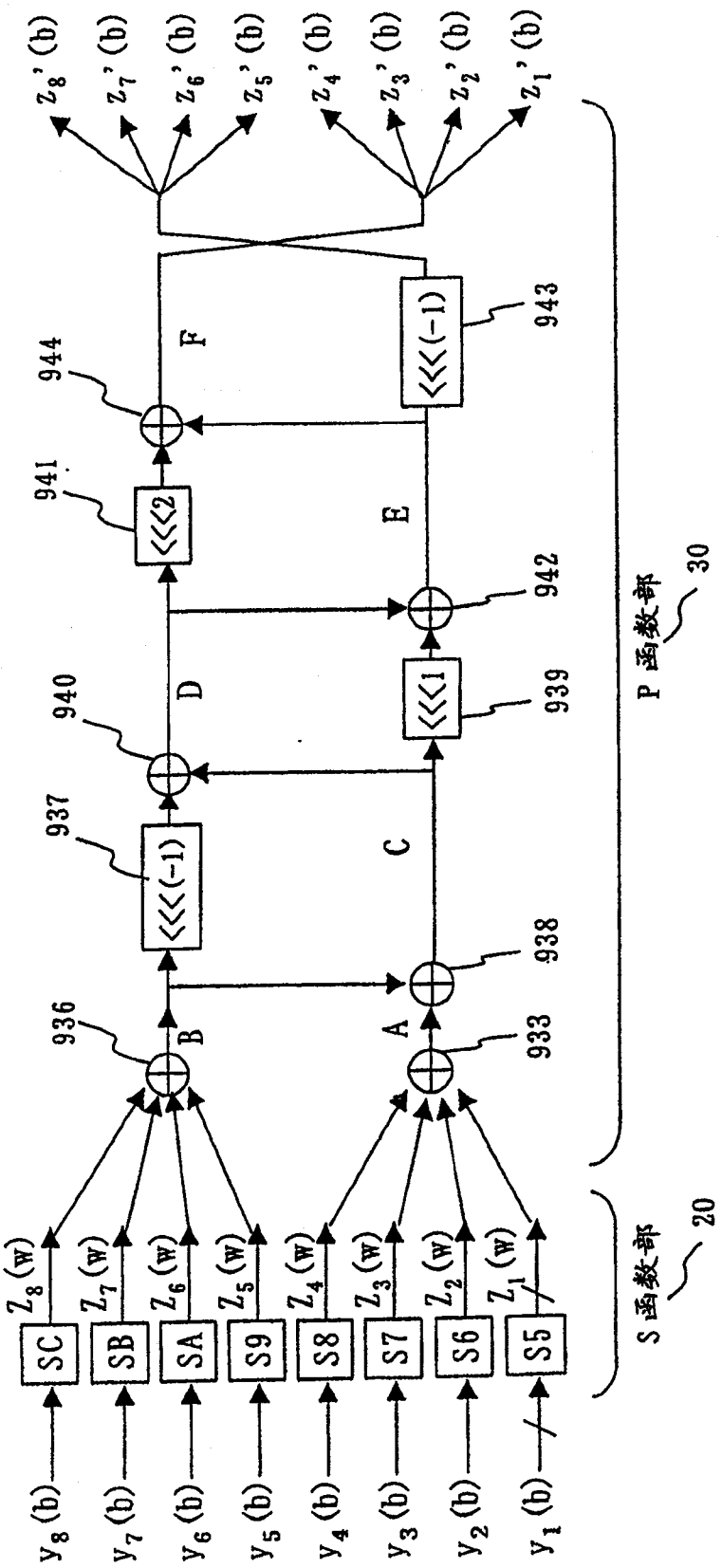

y_8 (b)
y_7 (b)
y_6 (b)
y_5 (b)
y_4 (b)
y_3 (b)
y_2 (b)
y_1 (b)
SC
SB
SA
S9
S8
S7
S6
S5
Z_8 (w)
Z_7 (w)
Z_6 (w)
Z_5 (w)
Z_4 (w)
Z_3 (w)
Z_2 (w)
Z_1 (w)
S 函数部
20
P 函数部
30
936
937
940
941
944
933
938
939
942
943
A
B
C
D
E
F
<<<(-1)
<<<2
<<<1
<<<(-1)
z_8' (b)
z_7' (b)
z_6' (b)
z_5' (b)
z_4' (b)
z_3' (b)
z_2' (b)
z_1' (b)

图 32

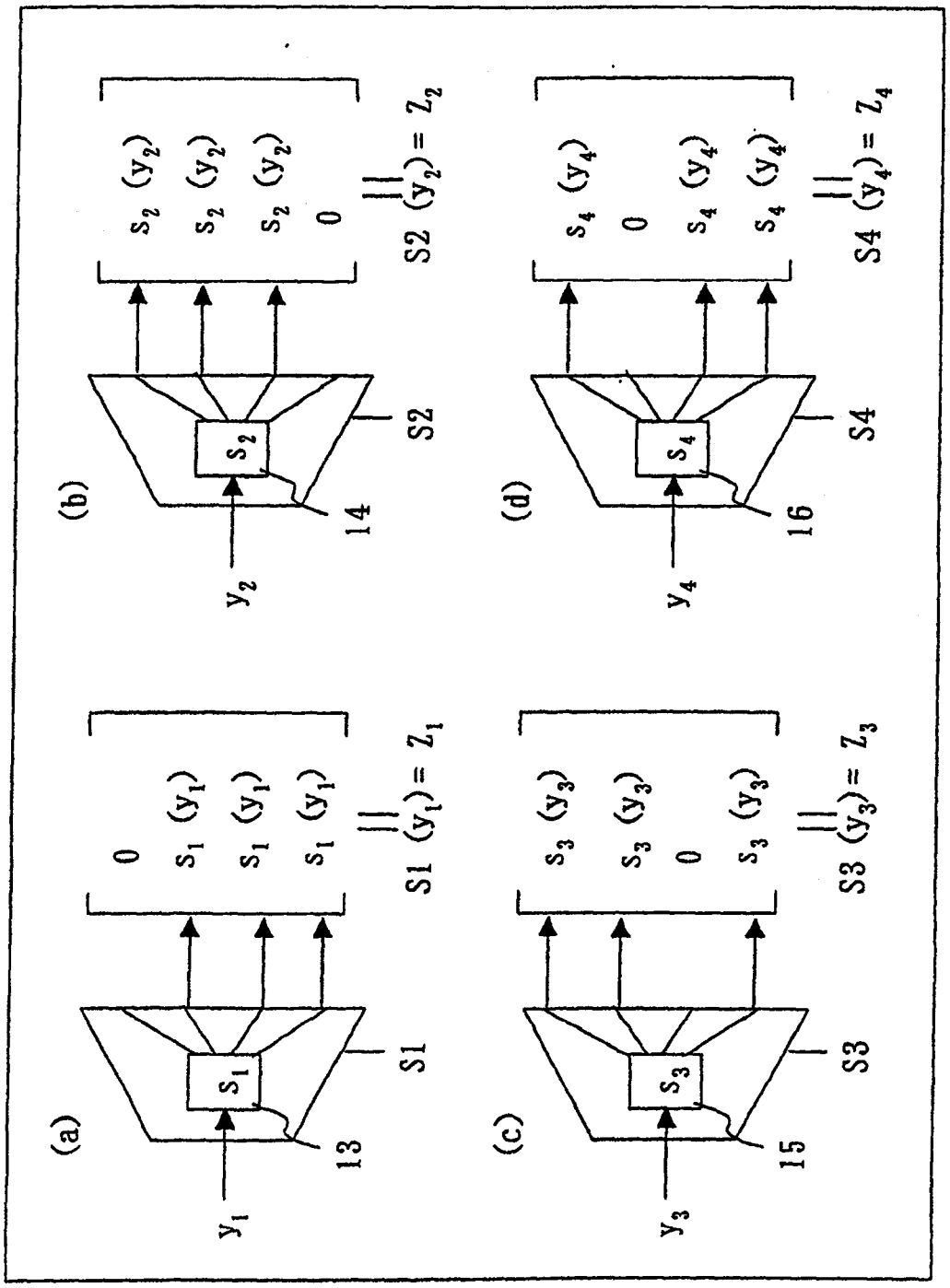

(a)
(b)
(c)
(d)
S1
S2
S3
S4
13
14
15
16
y_1
y_2
y_3
y_4
s_1
s_2
s_3
s_4
0
$s_1(y_1)$
$s_2(y_2)$
$s_3(y_3)$
$s_4(y_4)$
S1 (y_1)= Z_1
S2 (y_2)= Z_2
S3 (y_3)= Z_3
S4 (y_4)= Z_4

图 33

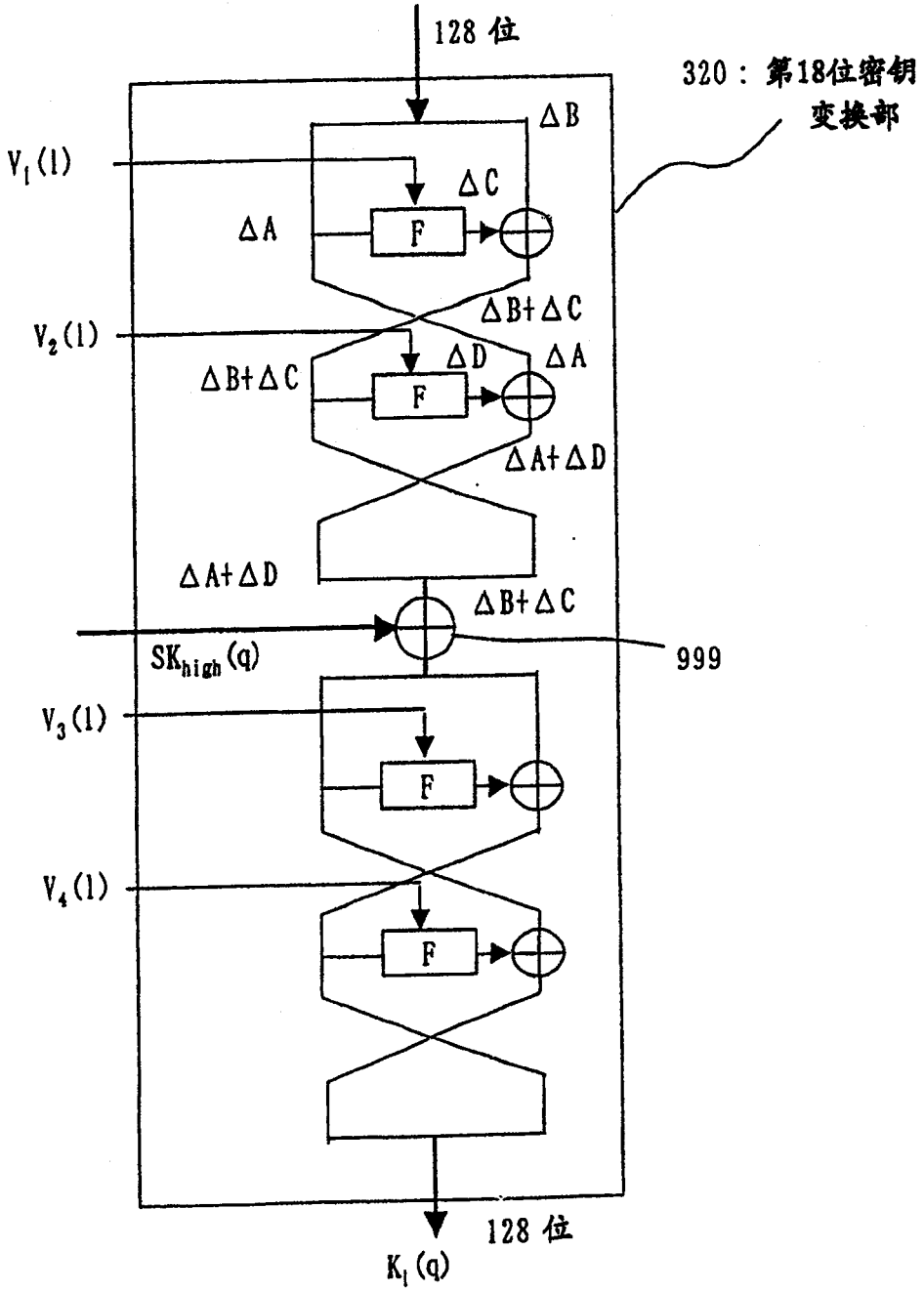

128 位
320：第18位密钥
变换部
ΔB
V1(1)
ΔC
ΔA
F
ΔB+ΔC
V2(1)
ΔD
ΔA
ΔB+ΔC
F
ΔA+ΔD
ΔA+ΔD
ΔB+ΔC
SKhigh(q)
999
V3(1)
F
V4(1)
F
128 位
K1(q)

图 34

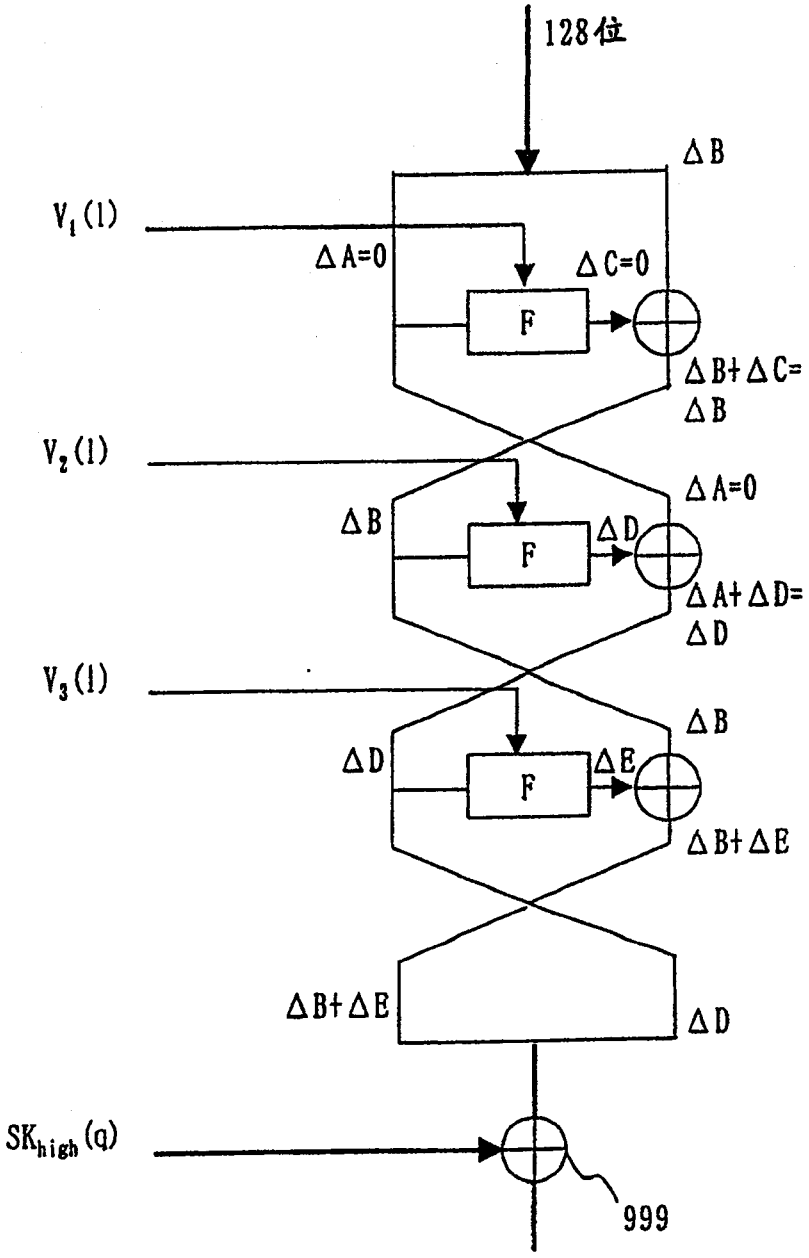

128位
ΔB
V1(1)
ΔA=0
ΔC=0
F
ΔB+ΔC=
ΔB
V2(1)
ΔA=0
ΔB
F
ΔD
ΔA+ΔD=
ΔD
V3(1)
ΔB
ΔD
F
ΔE
ΔB+ΔE
ΔB+ΔE
ΔD
SKhigh(q)
999

图 35

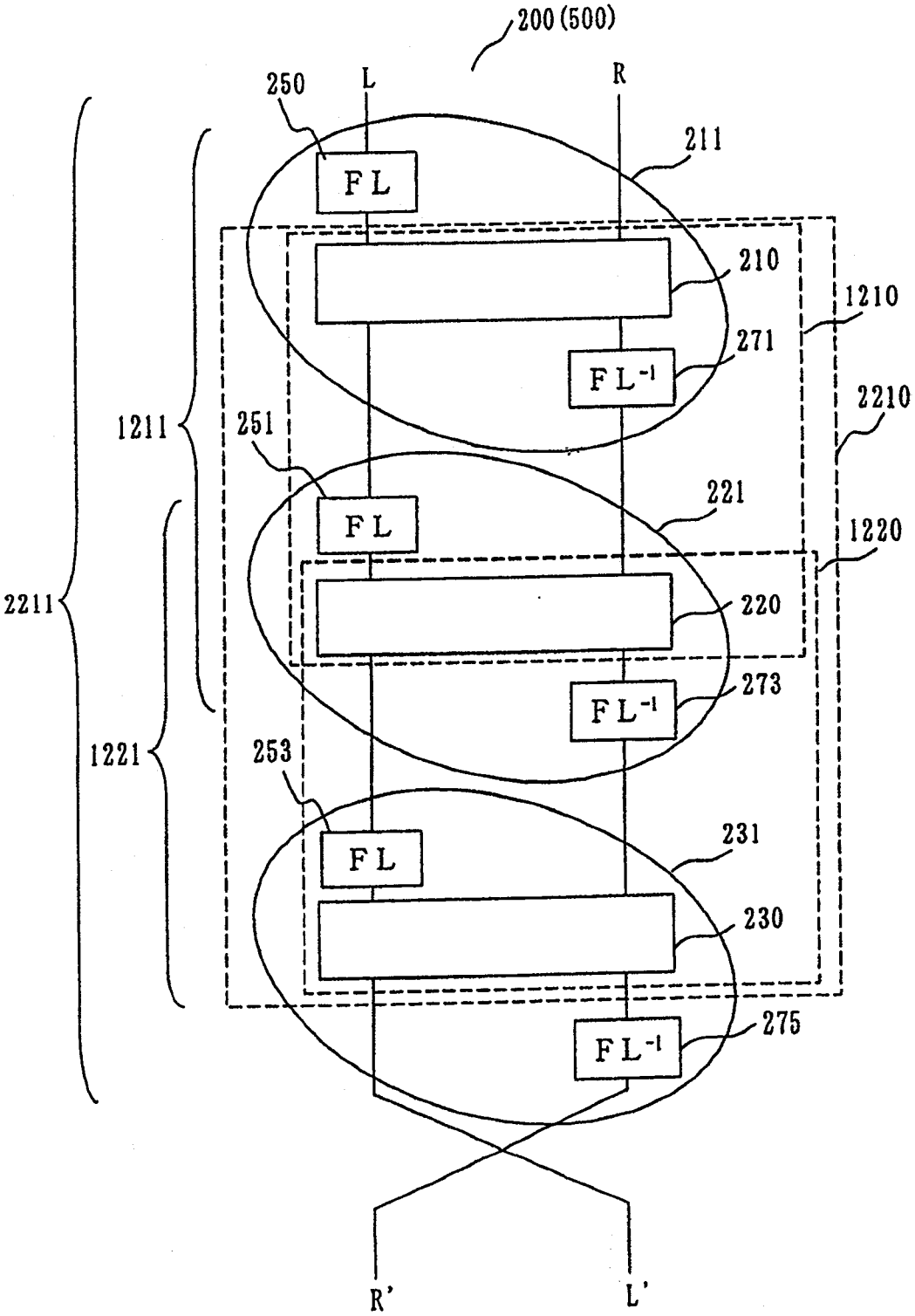

200(500)
250
L
R
211
FL
210
1210
271
FL-1
2210
1211
251
221
FL
1220
220
2211
273
FL-1
1221
253
231
FL
230
275
FL-1
R'
L'

图 36

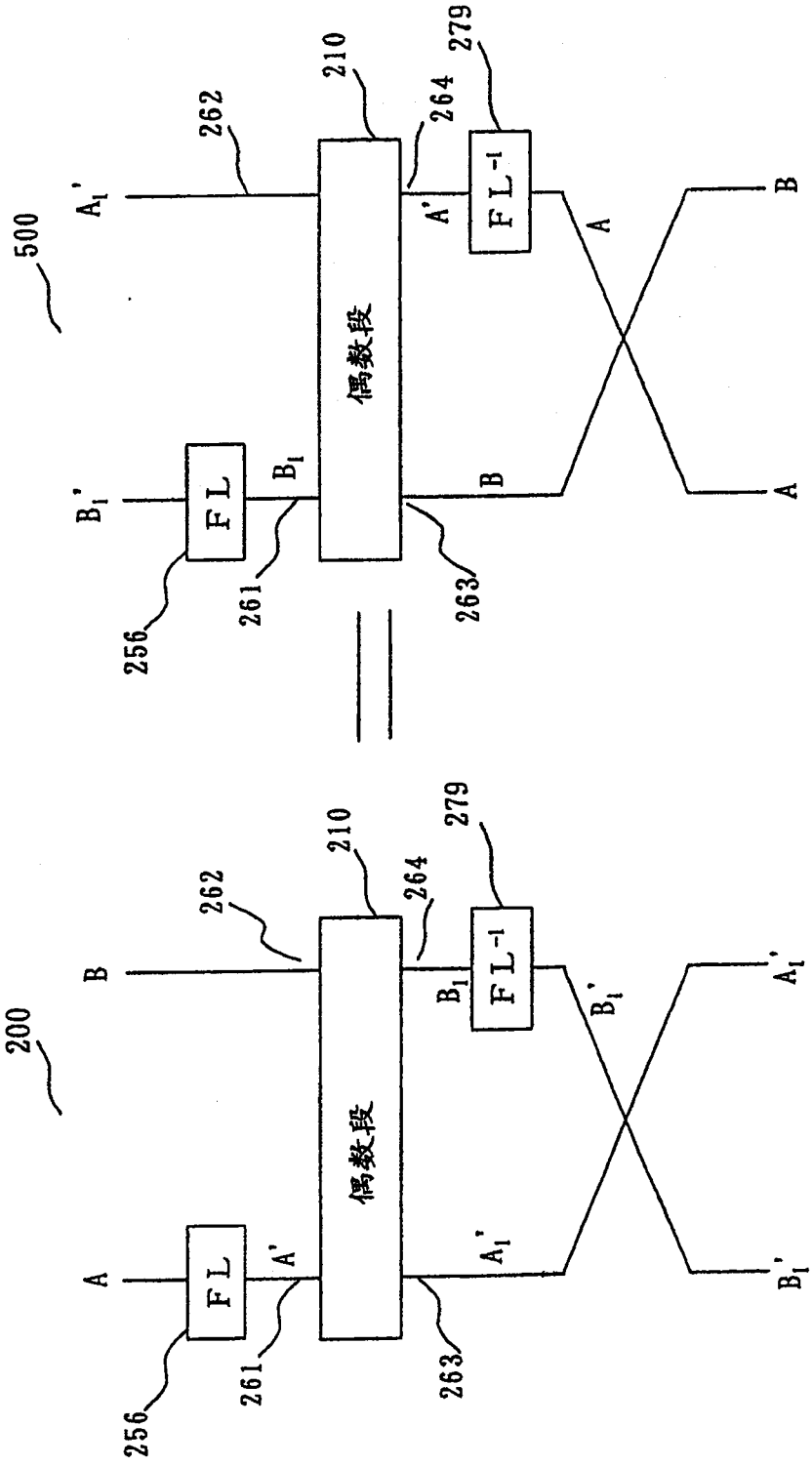

500
200
偶数段
偶数段
FL
FL
FL-1
FL-1
256
261
263
264
279
262
210
A
A'
B
B'
A1'
B1'
B1

图 37

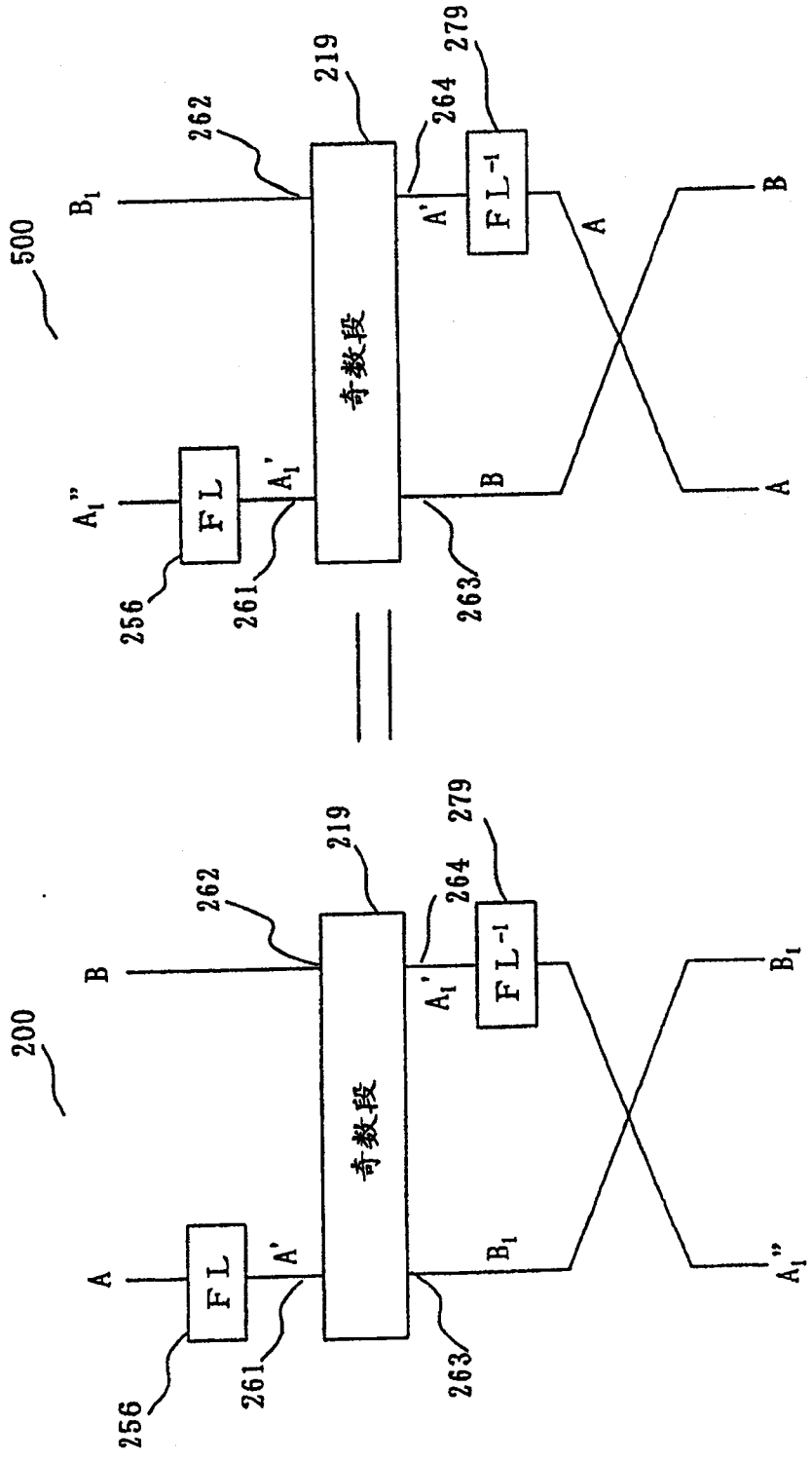

500
200
奇数段
奇数段
FL
FL
FL-1
FL-1
A
B
B1
A1"
A'
A1'
219
256
261
262
263
264
279

图 38

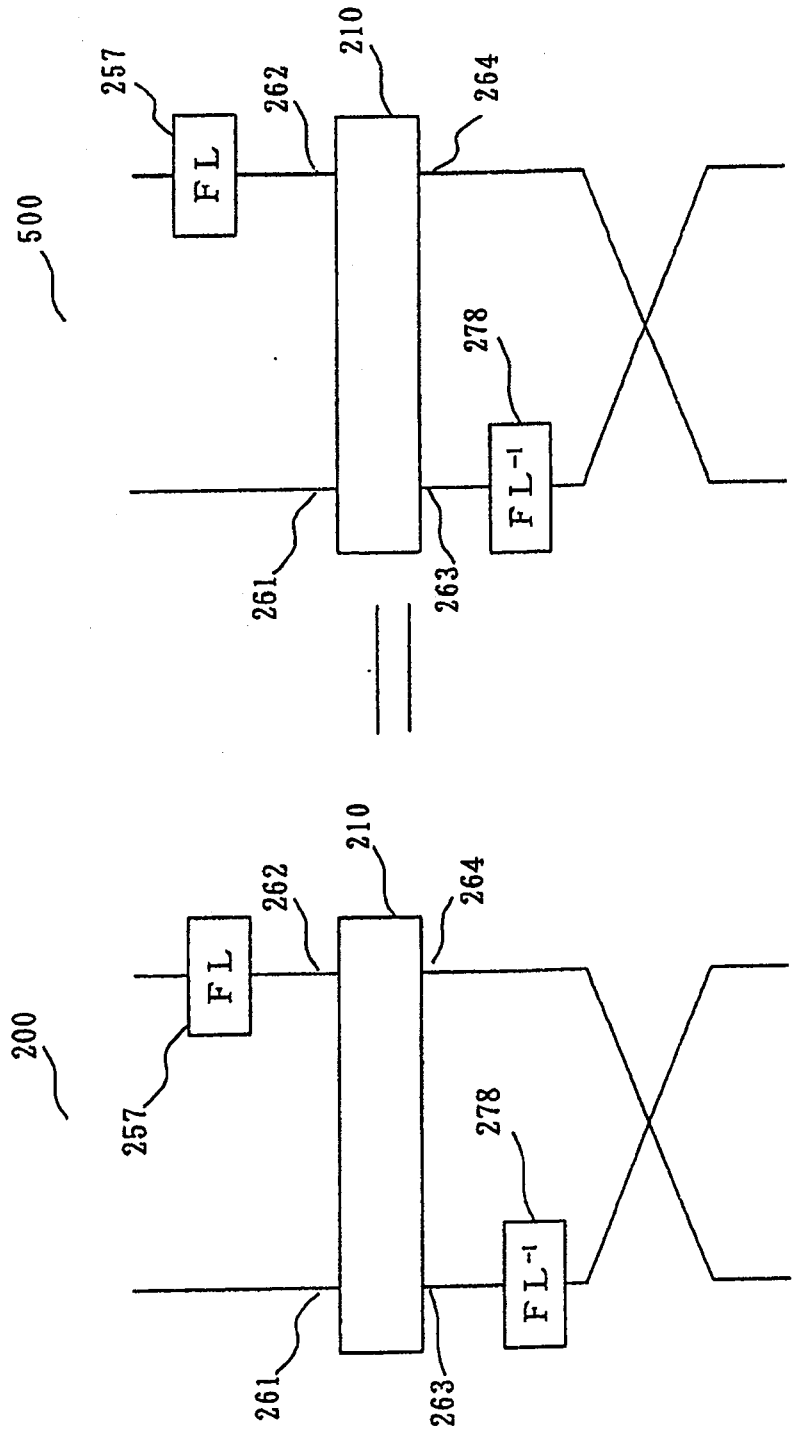

500
257
FL
262
210
264
278
FL⁻¹
261
263
200
257
FL
262
210
264
278
FL⁻¹
261
263

图 39

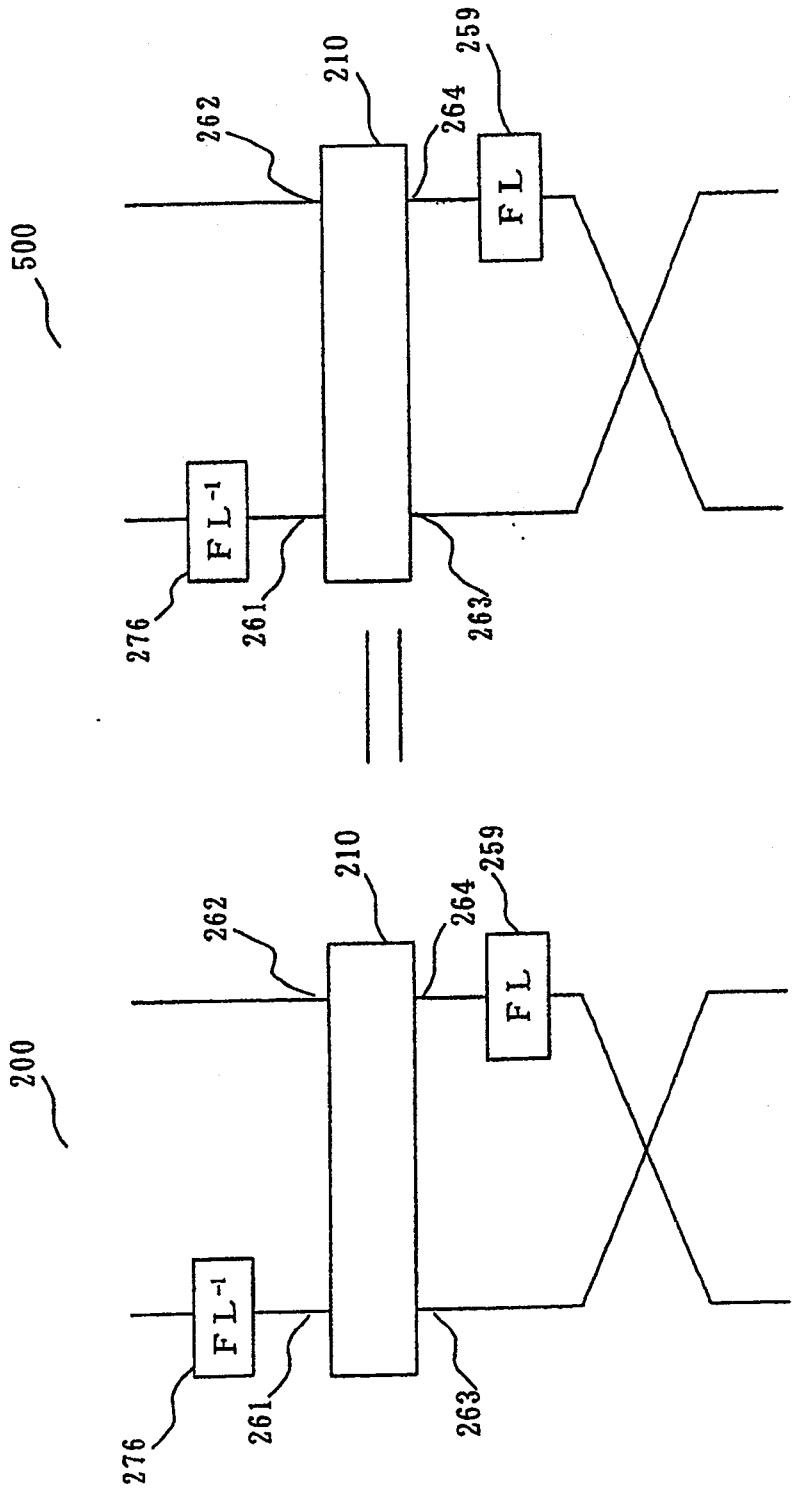

500
262
210
264
259
FL
FL-1
276
261
263
200
262
210
264
259
FL
FL-1
276
261
263

图 40

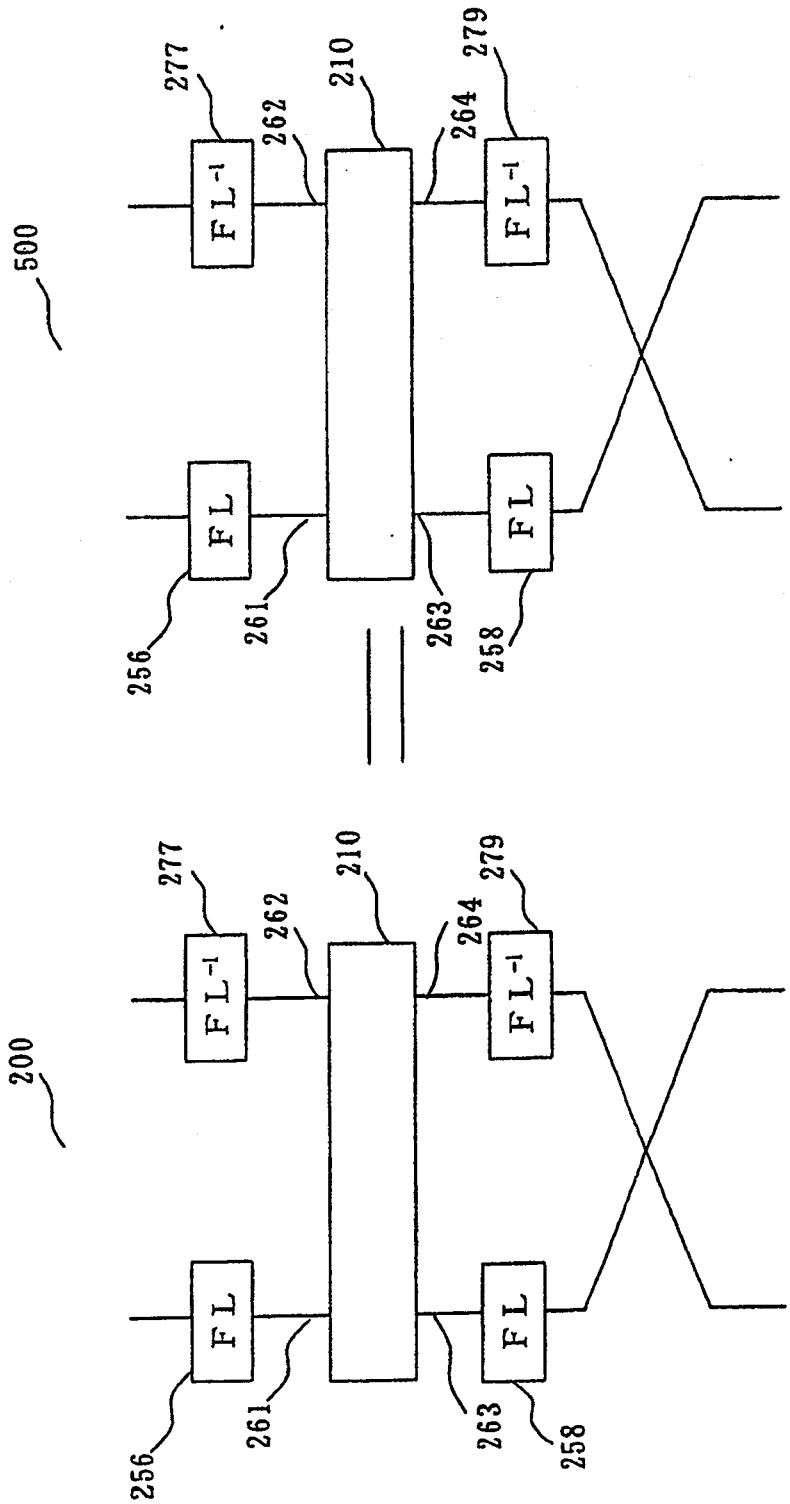

500
277
262
210
264
279
FL-1
FL
256
261
263
258
200
277
262
210
264
279
FL-1
FL
256
261
263
258

图 41

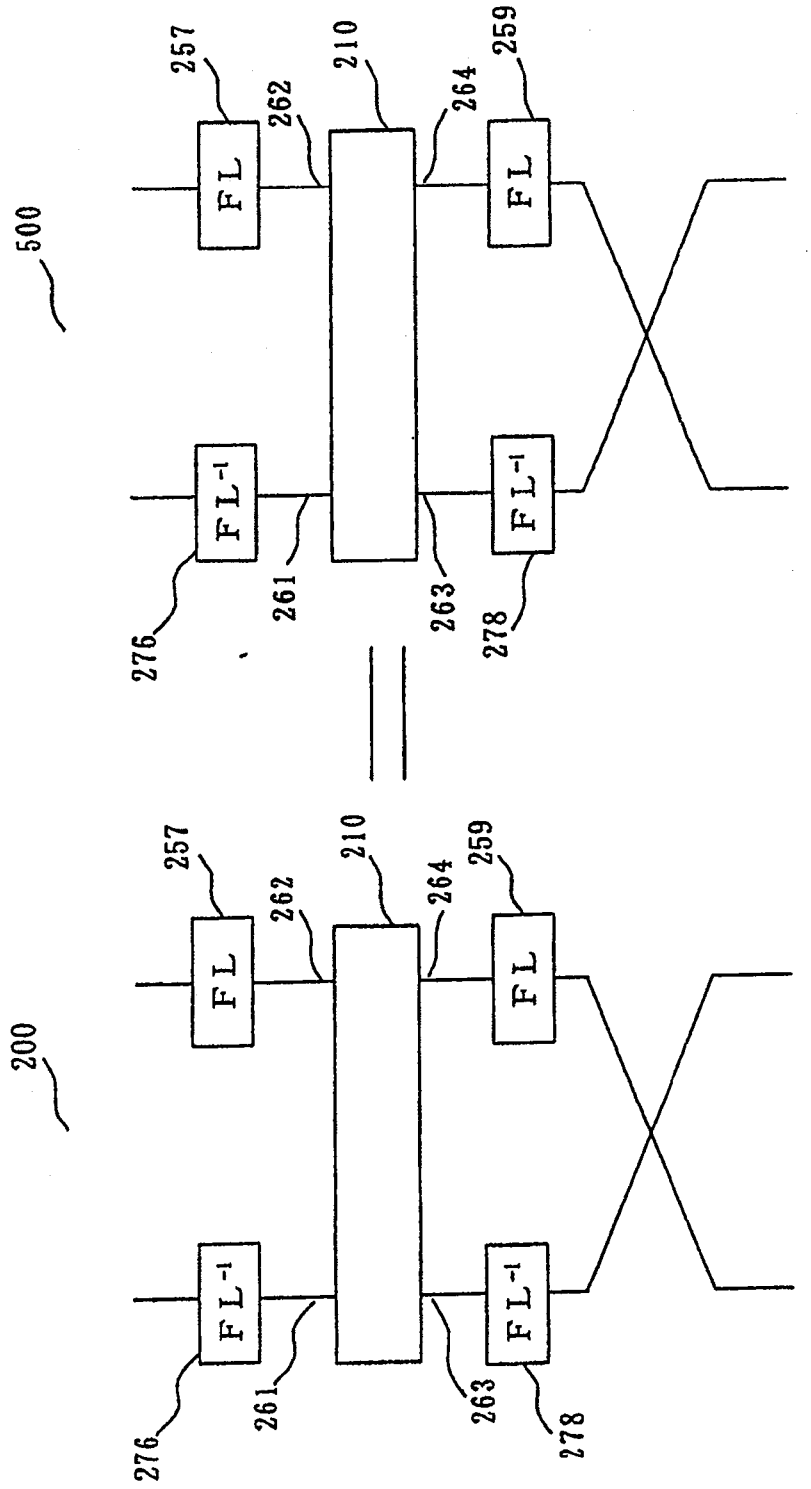

500
257
262
210
264
259
FL
FL
FL-1
FL-1
276
261
263
278
200
257
262
210
264
259
FL
FL
FL-1
FL-1
276
261
263
278

图 42

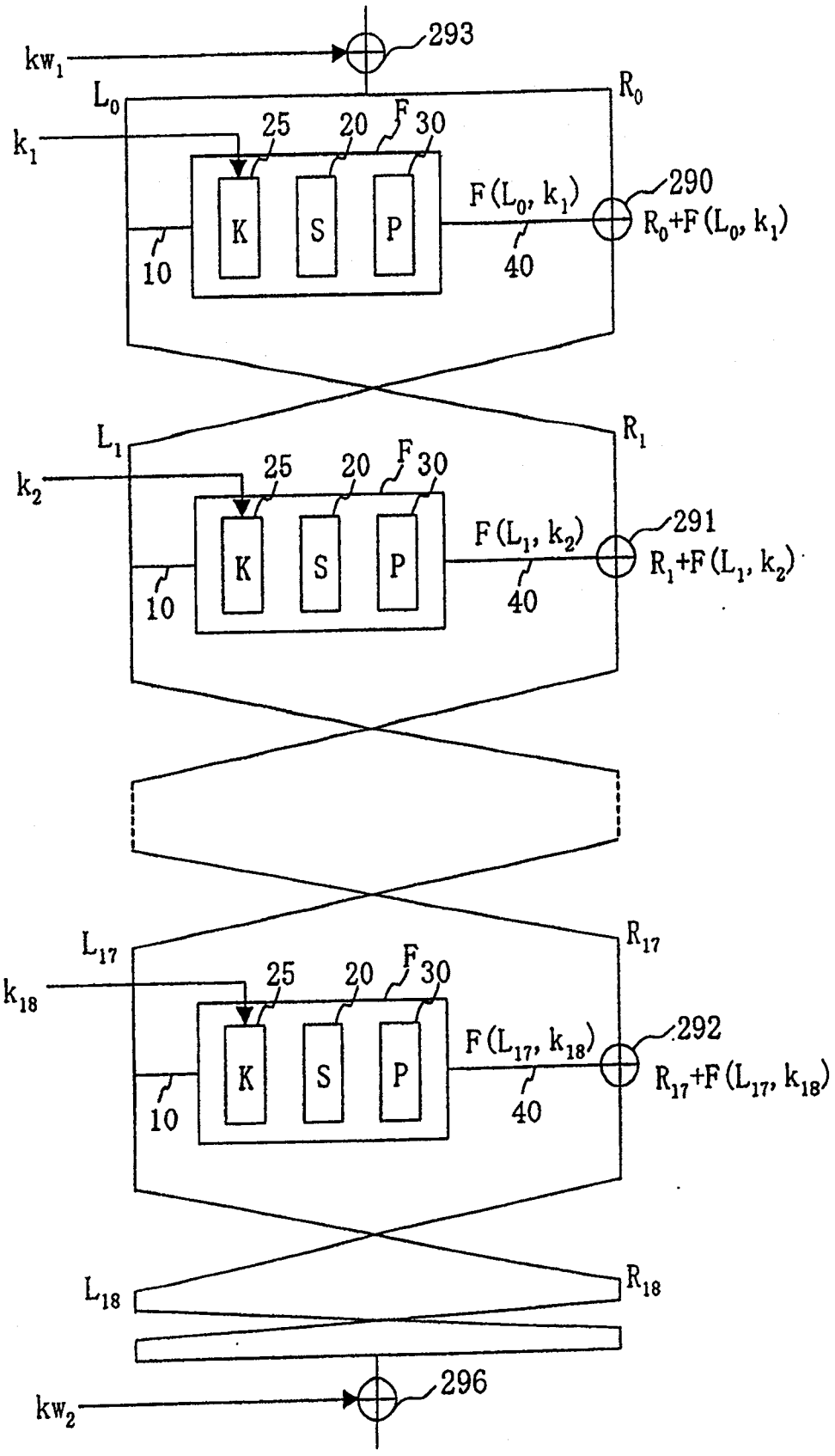

kw1
293
L0
R0
k1
25
20
F
30
K
S
P
F(L0, k1)
290
R0+F(L0, k1)
10
40
L1
R1
k2
F(L1, k2)
291
R1+F(L1, k2)
L17
R17
k18
F(L17, k18)
292
R17+F(L17, k18)
L18
R18
kw2
296

图 43

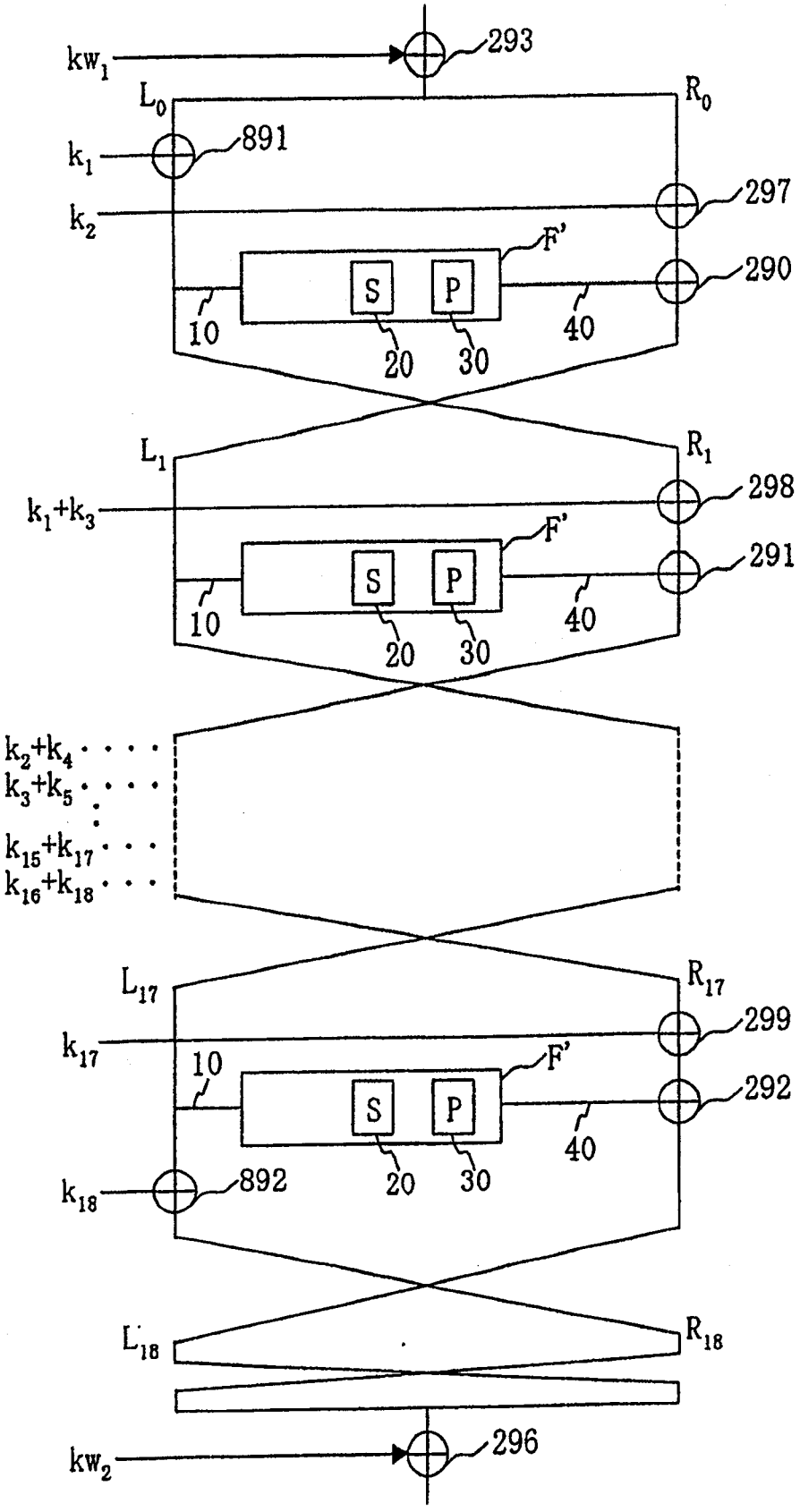

kw1
293
L0
R0
k1
891
297
k2
F'
290
S
P
10
20
30
40
L1
R1
298
k1+k3
F'
291
k2+k4
k3+k5
k15+k17
k16+k18
L17
R17
299
k17
F'
292
k18
892
L18
R18
kw2
296

图 44

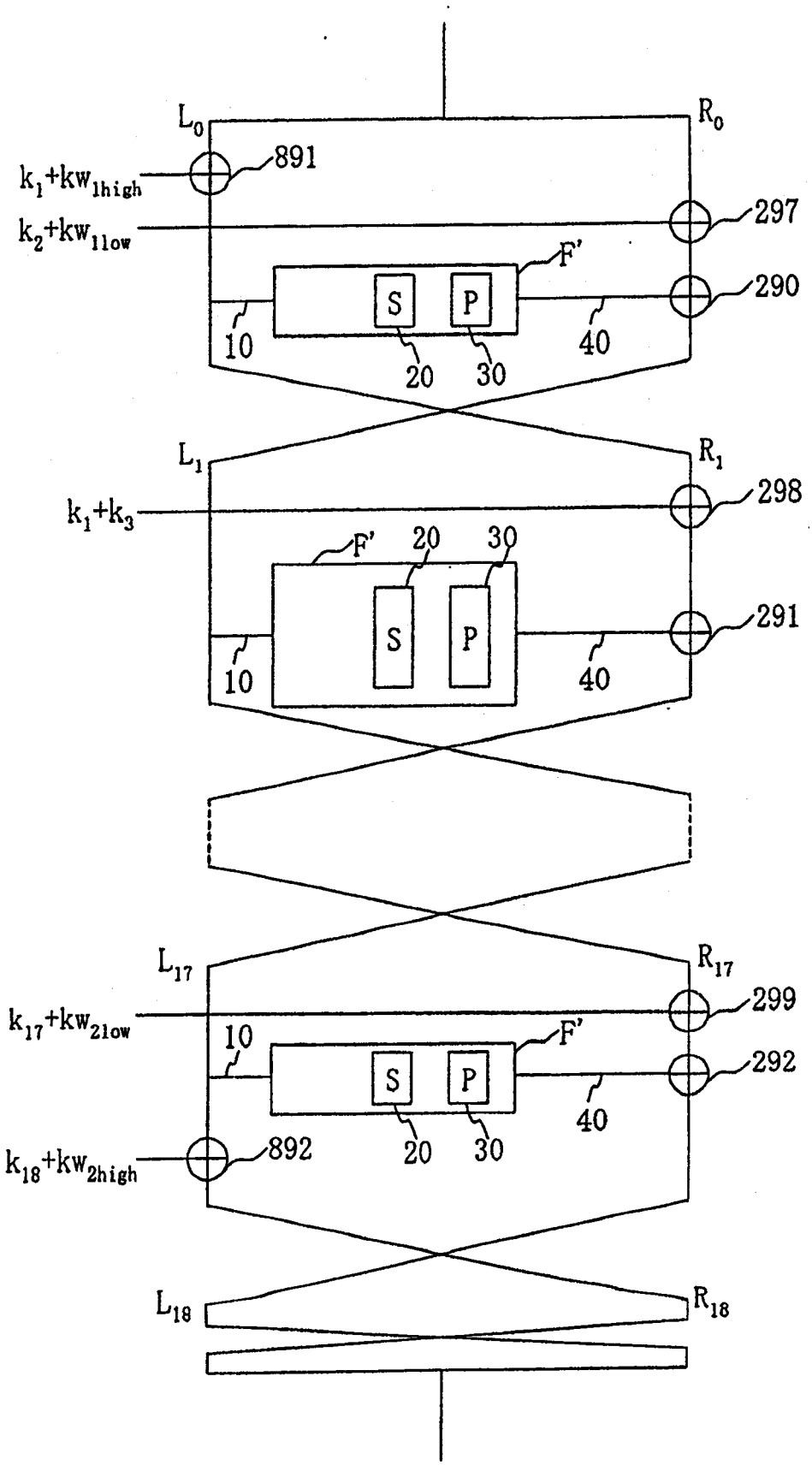

L_0
R_0
891
k_1+kw_{1high}
k_2+kw_{1low}
297
F'
S
P
290
10
20
30
40
L_1
R_1
k_1+k_3
298
F'
20
30
S
P
291
10
40
L_{17}
R_{17}
299
$k_{17}+kw_{2low}$
10
F'
S
P
292
40
$k_{18}+kw_{2high}$
892
20
30
L_{18}
R_{18}

图 45

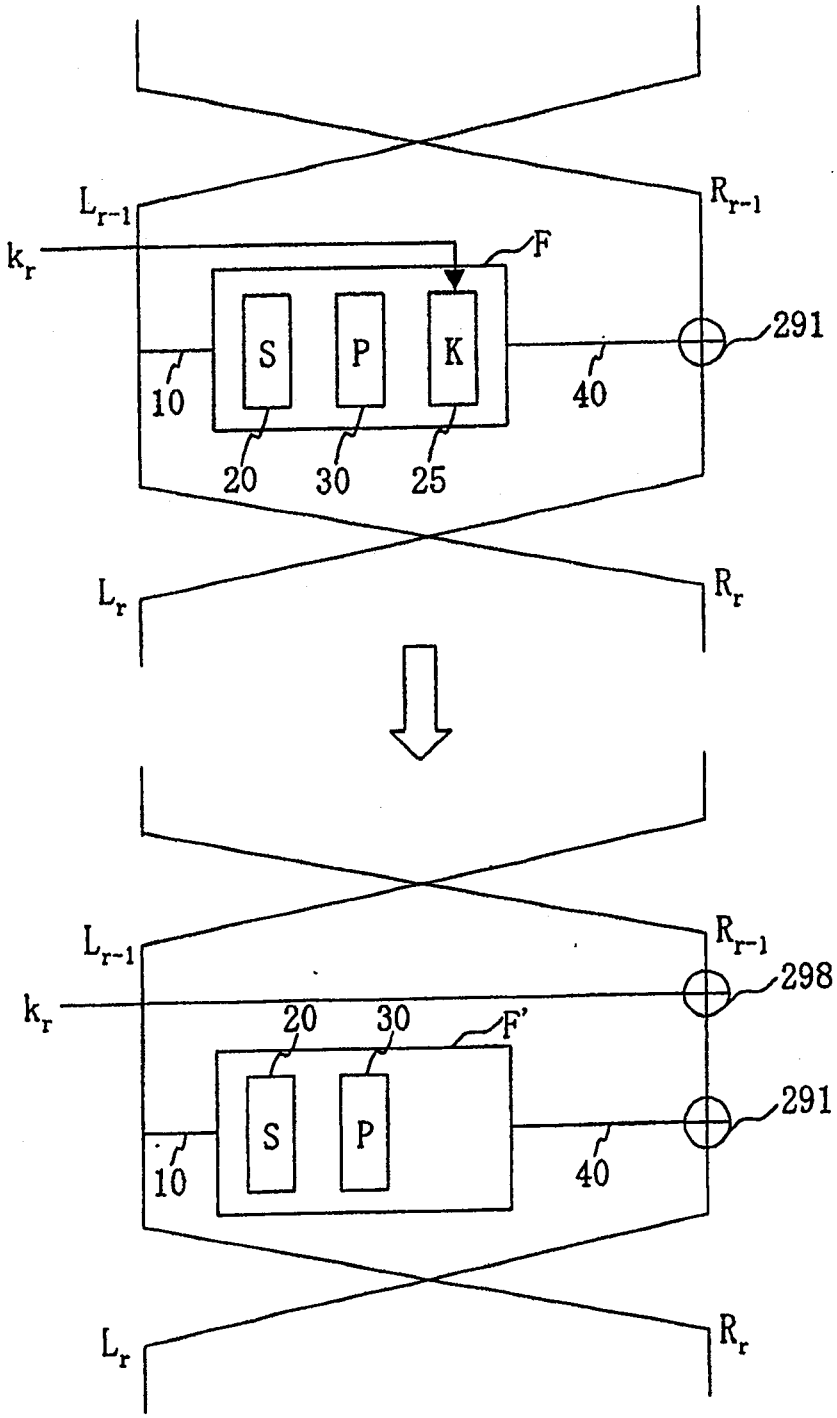

L_{r-1}
R_{r-1}
k_r
F
S
P
K
291
10
40
20
30
25
L_r
R_r
L_{r-1}
R_{r-1}
298
k_r
20
30
F'
S
P
291
10
40
L_r
R_r

图 46

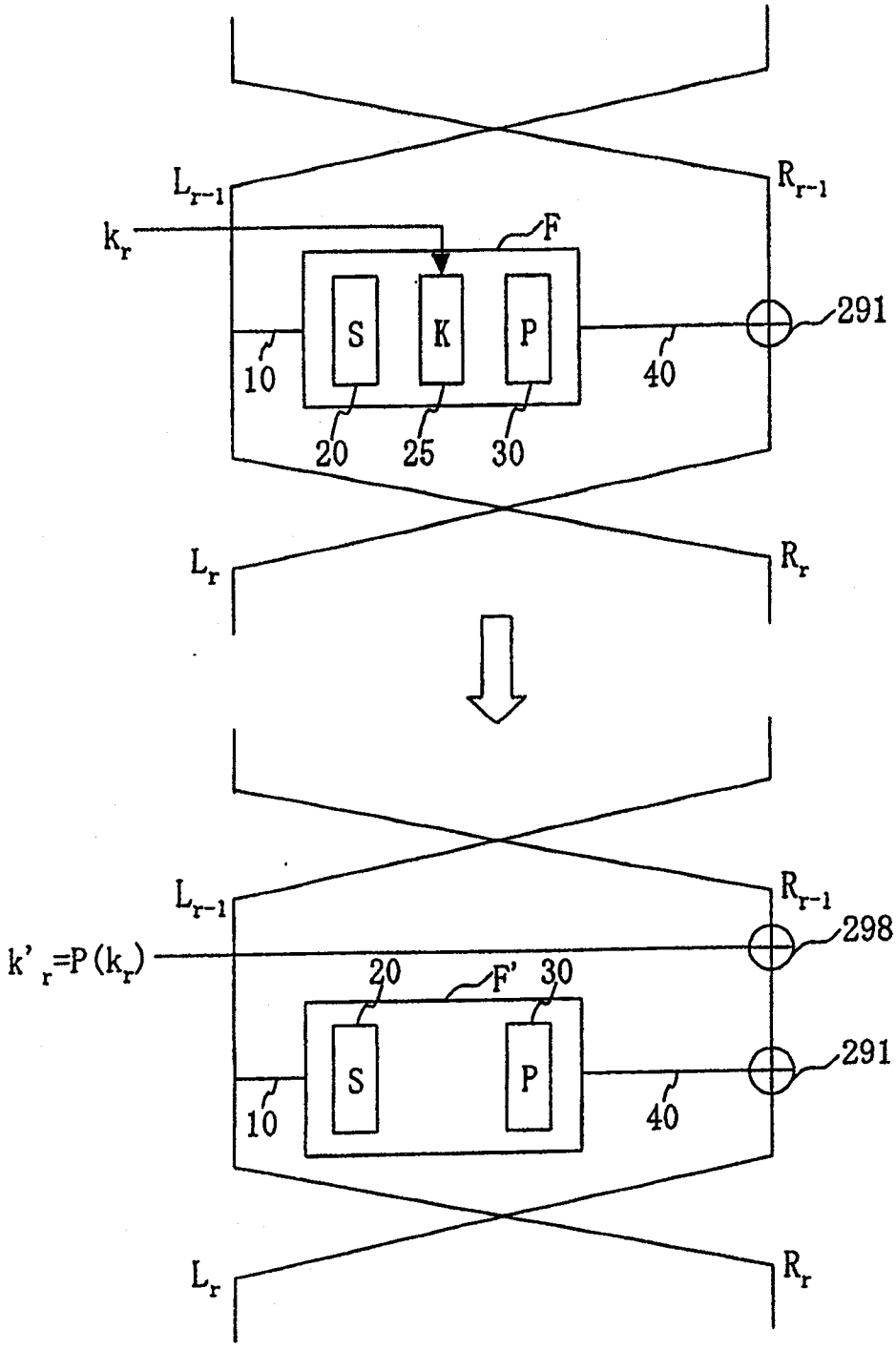

L_{r-1}
R_{r-1}
k_r
F
S
K
P
291
10
40
20
25
30
L_r
R_r
L_{r-1}
R_{r-1}
298
$k'_r=P(k_r)$
20
F'
30
S
P
291
10
40
L_r
R_r

图 47