[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
G09C 1/00
H04L 9/06

[12] 发明专利申请公开说明书

[21] 申请号 03800479.8

[43] 公开日 2004 年 8 月 4 日

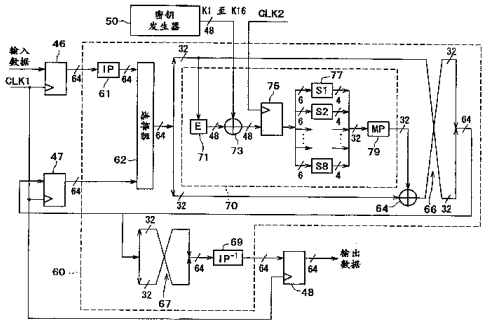
[11] 公开号 CN 1518733A

[22] 申请日 2003.4.18 [21] 申请号 03800479.8
[30] 优先权
[32] 2002. 4.19 [33] JP [31] 118508/2002
[86] 国际申请 PCT/JP2003/005011 2003.4.18
[87] 国际公布 WO2003/090187 日 2003.10.30
[85] 进入国家阶段日期 2003.12.19
[71] 申请人 索尼株式会社
地址 日本东京
[72] 发明人 松田宽美 细井隆史 田中理生 今孝安
[74] 专利代理机构 中国国际贸易促进委员会专利商标事务所
代理人 李德山
权利要求书 3 页 说明书 7 页 附图 5 页

[54] 发明名称 数据计算器件和加密器/解密器

[57] 摘要

本发明涉及数据计算器件和加密器/解密器，其中输入数据(纯文本数据或加密文本数据)被时钟 CLK1 闩锁，并且该数据在从选择器(62)输出之后，它的输出是初步反转的。选择器(62)的输出数据的最低位在与密钥数据 K1 异或并被时钟 CLK2 闩锁之后，被扩展反转。在闩锁之后的 48 位数据被 8 划分为 6 位，该数据被 4 位数据取代，合并，并被反转。在第二级和之后的算术运算中，被改组－合并电路(66)改组－合并的数据被时钟 CLK1 闩锁，并且从选择器(62)输出。在第 16 级算术运算之后，由改组电路(67)改组的数据被逆－反转。因而有可能实现一种加密/解密运算器件。



ISSN1008-4274

1. 一种计算器件，包括：

用于闩锁输入数据的第一闩锁部件；

用于计算所述第一闩锁部件的输出数据和从异步电路获得的数据的第一计算部件；

用于闩锁所述第一计算部件的输出数据的第二闩锁部件；以及

用于计算所述第二闩锁部件的输出数据的第二计算部件。

2. 一种计算器件，包括：

用于闩锁输入数据的第一闩锁部件；

用于计算从异步计算电路输入的异步数据和在所述第一闩锁部件中闩锁的输入数据的第一计算部件，其中，异步计算电路执行异步操作；

用于对在所述第一计算部件中计算并输出的数据执行同步的同步部件；以及

进一步计算在所述同步部件中同步的数据的第二计算部件。

3. 如权利要求2所述的计算器件，其中，所述第一闩锁部件的闩锁定时和所述同步部件的同步定时互不相同。

4. 如权利要求2所述的计算器件，进一步包括：

用于闩锁从所述第二计算部件输出的第二计算数据的第二闩锁部件；以及

用于选择在所述第二闩锁部件中闩锁的输入数据或由所述同步部件同步的数据的选择部件；

其中，所述第一计算部件对所述选择部件选择的数据以及从所述异步计算电路输入的异步数据执行预定的计算，所述选择数据即为在所述第一闩锁部件中闩锁的输入数据或由所述同步部件同步的数据。

5. 如权利要求2所述的计算器件，进一步包括：

选择信号产生部件，用于在预定定时使所述选择部件选择在所

述第二闩锁部件中闩锁的输入数据或由所述同步部件同步的数据;

其中，在所述第一闩锁部件中闩锁的输入数据在控制之下被所述第一和第二计算部件计算多次。

6. 一种加密器/解密器，包括:

根据输入的处理模式数据而对输入的密钥数据执行异步计算的异步计算处理部件;

根据从所述异步计算处理部件获得的计算密钥数据，对输入数据执行第一计算的第一计算部件;

对从所述第一计算部件输出的第一计算结果数据执行同步的同步部件;

对从所述同步部件输出的同步数据进一步执行第二计算的第二计算部件;

选择部件，用于选择将被处理的输入计算数据或从所述第二计算部件输出并输入到所述第一计算部件的第二计算结果数据; 以及

用于控制所述选择部件的选择定时的选择定时控制部件;

其中，在所述选择定时控制部件的控制下，根据输入的计算密钥数据，通过第一计算和第二计算对输入的计算数据进行多次处理。

7. 如权利要求 6 所述的加密器/解密器，其中，所述异步计算处理部件根据所述处理模式而从输入的密钥数据产生多个密钥数据。

8. 如权利要求 6 所述的加密器/解密器，进一步包括:

用于对输入计算数据的位进行换位的第一换位部件;

用于对从所述选择器件输出的选择数据的位进行换位的第二换位部件;

用于对从所述第二计算部件输出的第二计算结果数据的位进行换位的第三换位部件;

用于进一步对从所述第三换位部件获得的换位数据执行预定计算的第四计算部件; 以及

用于对从所述第四计算部件输出的第四计算结果数据的位进行换位的第四换位部件。

9. 如权利要求 6 所述的加密器/解密器，其中，所述选择部件的选择定时和所述同步部件的同步定时互不相同。

数据计算器件和加密器/解密器

技术领域

本发明涉及用于数据计算以对数据进行加密和/或解密的数据计算器件和数据加密器/解密器。

背景技术

图 5 所示器件被设计成符合 DES（数据加密标准）加密算法的加密器/解密器。

密钥数据（秘密密钥）和输入数据（纯文本数据或加密文本数据）每一个都由 64 位组成，并且根据时钟 CLK 而分别在闩锁电路 81 和 82 中闩锁。而且，表示加密或解密的模式信号根据时钟 CLK 在闩锁电路 83 中闩锁。

从闩锁电路 81 输出的密钥数据提供给密钥发生器 90，并且从密钥发生器 90 顺序地输出 16 级密钥数据 K1-K16，每一级密钥数据都由 48 位组成。

更具体地，从闩锁电路 81 输出的 64 位密钥数据在转换电路 91 中被转换为 56 位密钥数据，并且高 28 位数据和低 28 位数据在移位电路 93 和 94 中移 1 位或 2 位，接着合并在一起形成 56 位密钥数据，此 56 位密钥数据在转换电路 95 中被转换为 48 位密钥数据，由此产生第一级密钥数据。

随后，执行相似的移位和转换，从而产生 16 级密钥数据并接着输入到选择器 99 中。随后，选择器 99 由从闩锁电路 83 输出的模式信号控制，并且，根据时钟脉冲 CLK 而顺序输出 16 级密钥数据 K1-K16，每一级密钥数据都包括 48 位。

闩锁电路 82 的输出数据（纯文本数据或加密文本数据）提供给计算器 100，在此执行以下计算。

首先，从闩锁电路 82 输出的 64 位数据在初始换位电路 101 中逐位换位，并且，在此初始换位之后获得的全部 64 位数据中的低 32 位与密钥数据 K1 一起在第一级转换电路 102 中计算，并且进一步地，在用函数元件 F 进行转换之后从转换电路 102 输出的 32 位数据与在初始换位之后获得的全部 64 位数据中的高 32 位一起在 XOR（异或）电路 103 中计算。

接着，从 XOR 电路 103 输出的 32 位数据与密钥数据 K2 一起在第二级转换电路 104 中计算，并且，在用函数元件 F 进行转换之后从转换电路 104 输出的 32 位数据与在初始换位之后获得的全部 64 位数据中的低 32 位一起在 XOR 电路 105 中计算。

随后，与以上相似地，高 32 位和低 32 位互相替换，在执行第三和后续级中的计算之后，输入到第 16 级转换电路 107 中的 32 位数据和从第 16 级 XOR 电路 108 输出的 32 位数据相互合并，并且在此合并之后获得的 64 位数据在反向换位电路 109 中逐位换位。

在此反向换位之后的 64 位数据根据时钟 CLK 在闩锁电路 84 中闩锁，接着，从闩锁电路 84 输出加密或解密的数据。

然而，在上述加密/解密计算器件中，密钥发生器 90 是不包括任何闩锁电路（取样电路）的异步电路，其中，16 级密钥数据每次从输入的密钥数据产生，并且只由选择器 99 选择，从而在转变点附近，在从密钥发生器 90 输出的密钥数据 K1-K16 上叠加许多噪声（信号线电势中的变化），从而，增加计算器 100 中的功率消耗。

发明内容

考虑到这些问题，本发明的目的在于实现一种适于显著减少功率消耗的改良计算器件。

本发明的计算器件包括用于闩锁输入数据的第一闩锁部件；用于计算从异步计算电路输入的异步数据和在第一闩锁部件中闩锁的输入数据的第一计算部件，其中，异步计算电路执行异步操作；用于对从第一计算部件输出的计算数据同步化的同步部件；以及进一步计算

从同步部件获得的同步数据的第二计算部件。在以上结构的计算器件中，可显著减少功率消耗，并且其电路规模也可以减小。

附图说明

图 1 为示出加密/解密计算器件的框图，该器件作为代表本发明计算器件的实施例；

图 2 为示出图 1 加密/解密计算器件中主要部件的框图；

图 3 为用于解释在图 1 加密/解密计算器件中执行的操作的视图；

图 4 为示出作为本发明数据接收器实施例的数据记录/再现装置的框图；以及

图 5 为示出常规加密/解密计算器件的框图。

具体实施方式

[计算器件的实施例：图 1-3]

图 1 和 2 示出代表本发明计算器件的实施例，该器件构造成加密/解密计算器件，其中，图 2 示出图 1 所示计算器 60 内的转换电路 70 的细节。

在此实施例的加密/解密计算器件中采用的加密算法符合 DES 加密算法。

密钥数据（秘密密钥）和输入数据（纯文本数据或加密文本数据）每一个都包括 64 位，并根据时钟 CLK1 而分别闩锁在闩锁电路 41 和 46 中。

而且，在闩锁电路 42 中根据时钟 CLK1 闩锁表示加密或解密的模式信号。进而，时钟 CLK1 由 16 级计数器 44 从起始信号时间点开始计数。

从闩锁电路 41 输出的密钥数据、从闩锁电路 42 输出的模式信号以及计数器 44 的输出信号提供给密钥发生器 50，并且，从密钥发生器 50 顺序地输出每个都由 48 位组成的 16 级密钥数据 K1-K16。

更具体地，从闩锁电路 41 输出的 64 位密钥数据在转换电路 51 中被转换为 56 位密钥数据，并且，56 位密钥数据根据闩锁电路 42 的输出信号而在移位寄存器 53 中顺序地移位，每次移一位或两位，由此获得每个都包括 56 位的 16 级密钥数据。

进一步地，16 级 56 位密钥数据在转换电路 55 中都被转换为 48 位密钥数据，并且在选择器 57 中，根据计数器 44 的输出信号，在时钟 CLK1 的每个脉冲上顺序地选择 16 级 48 位密钥数据，从而，在时钟 CLK1 的每个脉冲上顺序地获得前述密钥数据 K1-K16。

因而，在密钥发生器 50 中，仅仅执行从输入的密钥数据每次生成 16 级密钥数据并由选择器 57 选择数据的操作，其中，从密钥发生器 50 输出的密钥数据 K1-K16 为以下情形：在转变点附近在数据上叠加许多噪声（信号线电势中的变化）。

闩锁电路 46 的输出数据（纯文本数据或加密文本数据）提供给计算器 60。此计算器 60 形成为：16 级计算由图 4 所示计算器 100 中的单级计算电路循环重复。

也就是说，首先，从闩锁电路 46 输出的 64 位数据在初始换位电路 61 中逐位换位，并且在初始换位之后的 64 位数据在计数器 44 的控制之下从选择器 62 输出。接着，全部 64 位数据中的低 32 位与密钥数据 K1 一起在转换电路 70 中计算，在这，所述数据使用函数元件 F 进行转换。

更具体地，在转换电路 70 中，如图 2 所示，低 32 位数据在扩展换位电路 71 中逐位换位，并且多次选择相同的位，从而，以上数据转换为 48 位数据，随后，因此获得的 48 位数据和 48 位密钥数据 K1 一起在 XOR 电路 73 中计算。

进一步地，从 XOR 电路 73 输出的 48 位数据根据与前述时钟 CLK1 相位不同的时钟 CLK2，在闩锁电路 75 中闩锁。

根据与时钟 CLK1 相位不同的时钟 CLK2 而执行闩锁 XOR 电路 73 输出数据的操作的理由是：密钥发生器 50 的输出密钥数据 K1-K16 与扩展换位电路 71 的输出数据从如图 3 所示的时钟 CLK1 的转

变点（前沿）延迟，XOR 电路 73 的输出数据也被延迟，从而，在根据时钟 CLK1 而闩锁 XOR 电路 73 的输出数据的情况下，闩锁数据是那些提前一个时钟脉冲的数据。更具体地，例如，时钟 CLK2 在相位上设置得与时钟 CLK1 相反。

由于 XOR 电路 73 的输出数据因此在闩锁电路 75 中闩锁，因此吸收密钥发生器 50 的输出密钥数据 K1-K16 中的前述噪声，从而，闩锁电路 75 的输出信号的电势只在时钟 CLK2 的转变点上变化，因此显著减少在闩锁电路 75 之后的电路中的功率消耗。

从闩锁电路 75 输出的 48 位数据分为 8 个数据，每个数据包括 6 位，并且每个 6 位数据根据检查表 77 而置换为 4 位数据。

进而，在此置换之后的 8 个 4 位数据合并在一起形成 32 位数据，所述 32 位数据接着在换位电路 79 中逐位换位。

在第一级计算过程中，上述处理完全在转换电路 70 中执行。随后，从换位电路 79 输出的 32 位数据与在初始换位之后从选择器 62 输出的全部 64 位数据中的高 32 位数据在 XOR 电路 64 中计算，作为第一级计算。

因而完成第一级中的计算。随后，输入到扩展换位电路 71 中的 32 位数据与从 XOR 电路 64 输出的 32 位数据合并在一起，以后述方式形成 64 位数据，其中，高 32 位和低 32 位在置换/合并电路 66 中相互置换，并且，在此合并之后获得的 64 位数据根据时钟 CLK1 而在闩锁电路 47 中闩锁。

在第二级和后续级的每一级执行的计算中，闩锁电路 47 输出的 64 位数据从选择器 62 输出，以取代从初始换位电路 61 输出的数据，并且向转换电路 70 中的 XOR 电路 73 输入密钥数据 K2 或随后的密钥数据，以取代密钥数据 K1，而且，执行与第一级计算相同的计算。

在完成第 16 级中的计算之后，不再需要在置换/合并电路 66 中置换高 32 位和低 32 位，从而，在电路 66 中置换和合并之后获得的 64 位数据提供给置换电路 67，在这，高 32 位和低 32 位相互转换，

接着，所述数据在反向换位电路 69 中逐位换位。

在此反向换位之后的 64 位数据根据时钟 CLK1 在闩锁电路 48 中闩锁，接着，从闩锁电路 48 输出加密或解密的数据。

如上所述，在此实施例的加密/解密计算器件中，功率消耗明显减少。而且，由于计算器 60 构造得使 16 级的计算通过单级计算电路的循环重复而执行，因此，计算装置中的门的数量可减少，最终减小电路规模。

上述实施例代表符合 DES 加密算法的典型情形。然而，不一定只需要符合 DES 加密算法，通过改变输入数据（纯文本数据或加密文本数据）和密钥数据的位长，或增加计算的级数，而进行一些修改。

[数据接收器的实施例：图 4]

图 4 示出包括记录/再现装置的数据接收系统，所述系统作为本发明数据接收器的实施例，该接收器配置有本发明的加密/解密计算器件。

在此实例的数据接收系统中，在诸如 PC 的终端单元 10 中，通过从记录介质 1 获取或使用因特网从传送系统 2 下载而接收用秘密密钥加密的编码数据。

因此接收的加密数据从终端单元 10 发送给连接到终端单元 10 中 USB（通用串行总线）端口的记录/再现装置 20。

记录/再现装置 20 在记录介质 5 上记录数据并且从该介质再现数据。装置 20 配置有加密器/解密器 30。

加密器/解密器 30 包括由前述图 1 和 2 所示加密/解密计算器件组成的加密/解密处理器 40，而且还包括：具有总线 32 的 CPU 31，其中，总线 32 连接到写有程序和所需固定数据的 ROM 33，用于传送将由 CPU 31 执行的命令而且对数据进行加密和解密；用作 CPU 31 工作区的 RAM 34；用于从和/或向终端单元 10 传送命令并从终端单元 10 获得数据的 USB 36；用于向记录/再现装置的 DSP（数字信

号处理器）26 输出数据的接口 37；以及，用于从和/或向记录/再现装置的 CPU 21 传送命令的接口 39。

加密器/解密器 30 形成在单芯片 LSI（大规模集成）电路中。

在记录/再现装置中，具有连接到 CPU 21 的总线 22 的 ROM 23、RAM 24 以及前述 DSP 26，其中，在 ROM 23 中写有将由 CPU 31 执行的程序以及所需要的固定数据，RAM 24 用作 CPU 21 的工作区。并进一步地，记录/再现处理器 27 和输出处理器 28 连接到 DSP 26。

在加密器/解密器 30 中，用秘密密钥加密并通过 USB 接口 36 从终端单元 10 输入的编码数据在加密/解密处理器 40 中如上所述地进行解密，并且，作为解密纯文本数据的编码数据通过接口 37 发送给 DSP 26，在 DSP 26 中进行处理之后，数据通过记录/再现处理器 27 记录到记录介质 5 上，或者在由输出处理器 28 转换为模拟信号之后传送到输出端 29。

记录介质 5 可以是任何一种光盘、硬盘、软盘、磁带、存储卡和半导体存储器。

本发明不仅可应用于此种记录/再现装置，而且可应用于没有记录功能而只能接收、解密和再现加密数据的装置。

工业应用性

如上所述，根据本发明，有可能实现一种显著减少功率消耗的改良计算器件。

图1

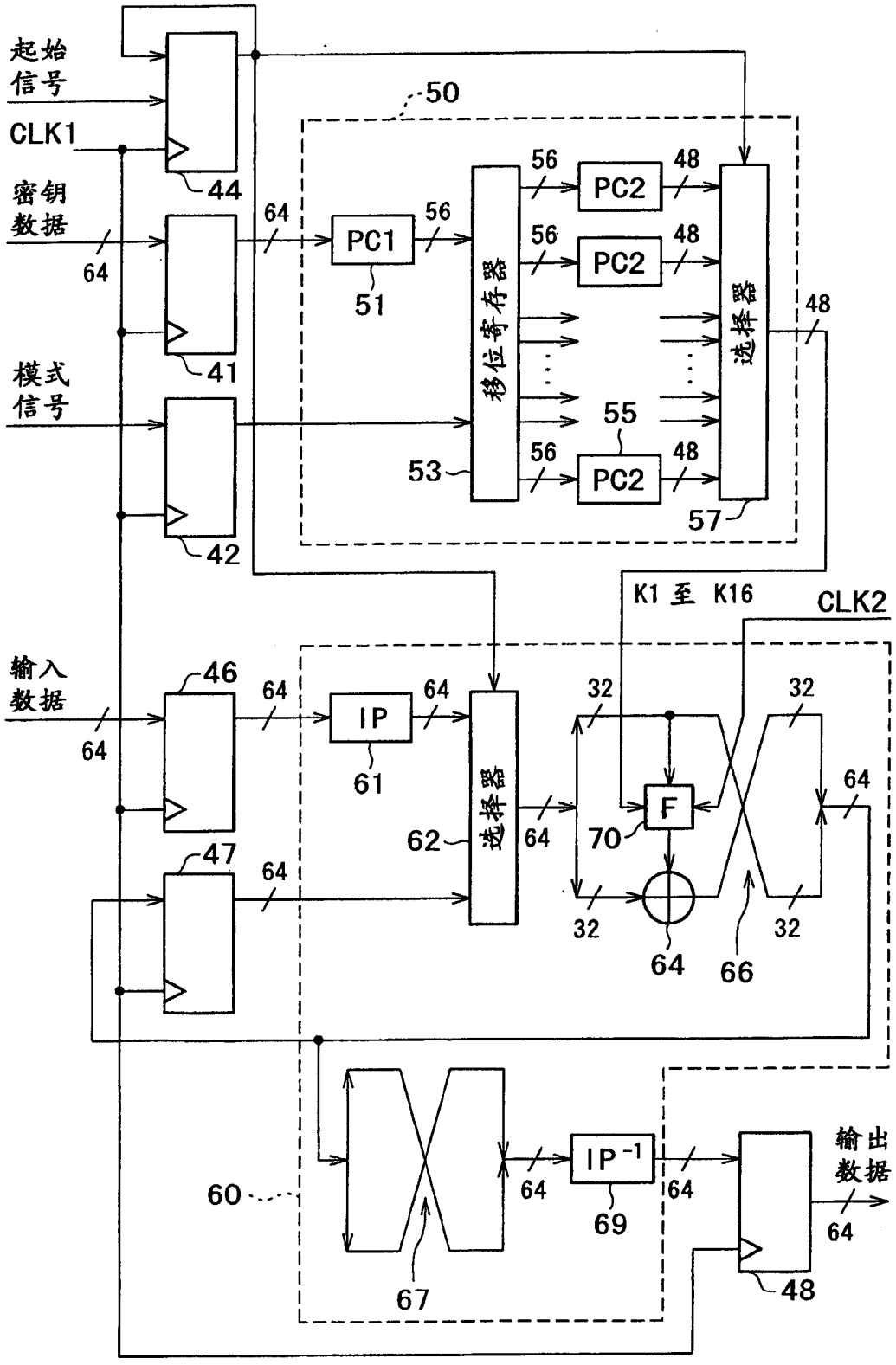

起始信号
CLK1
密钥数据
64
模式信号
输入数据
64
44
41
42
46
47
50
64
PC1
56
51
移位寄存器
53
56
PC2
48
55
选择器
57
48
K1 至 K16
CLK2
64
IP
61
64
选择器
62
64
32
32
F
70
64
32
32
64
66
64
IP -1
69
64
60
67
输出数据
64
48

图 2

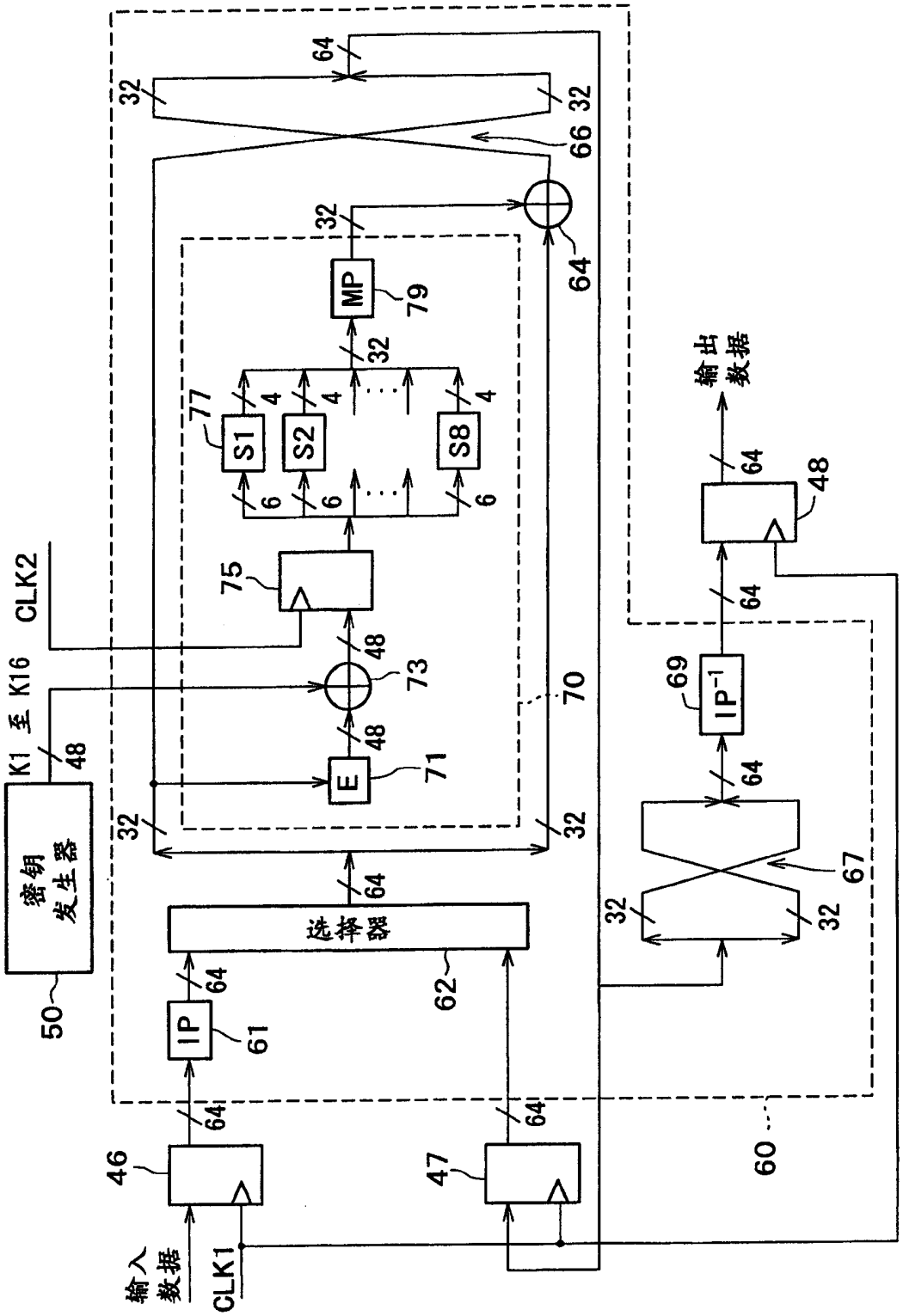

输入数据
CLK1
46
47
64
IP
61
50
密钥发生器
K1 至 K16
48
CLK2
选择器
62
32
66
E
71
73
75
S1
S2
S8
77
4
6
MP
79
70
60
IP-1
69
67
48
输出数据

图 3

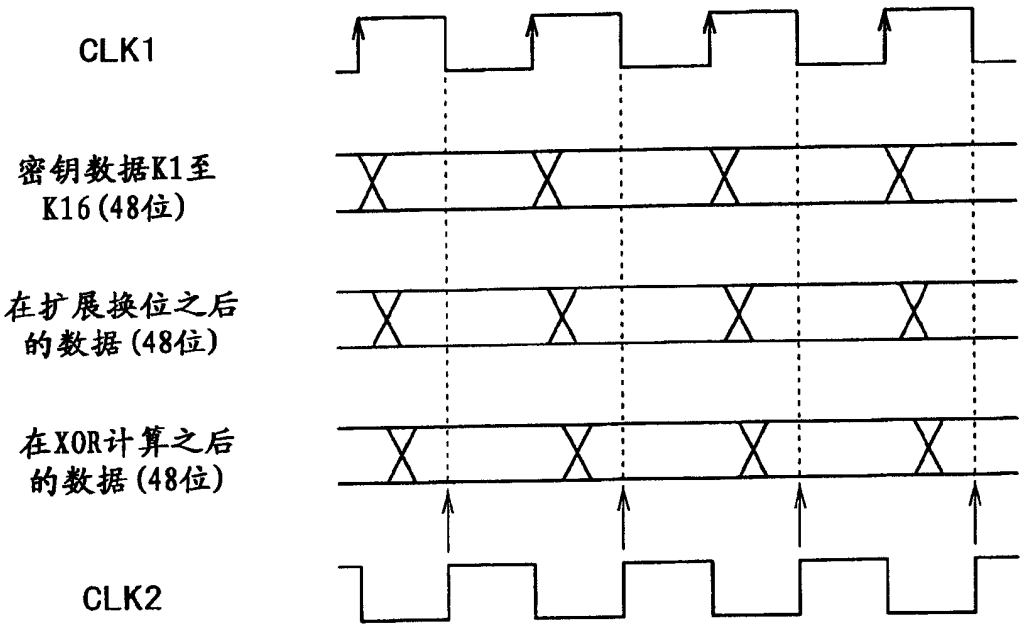


图4

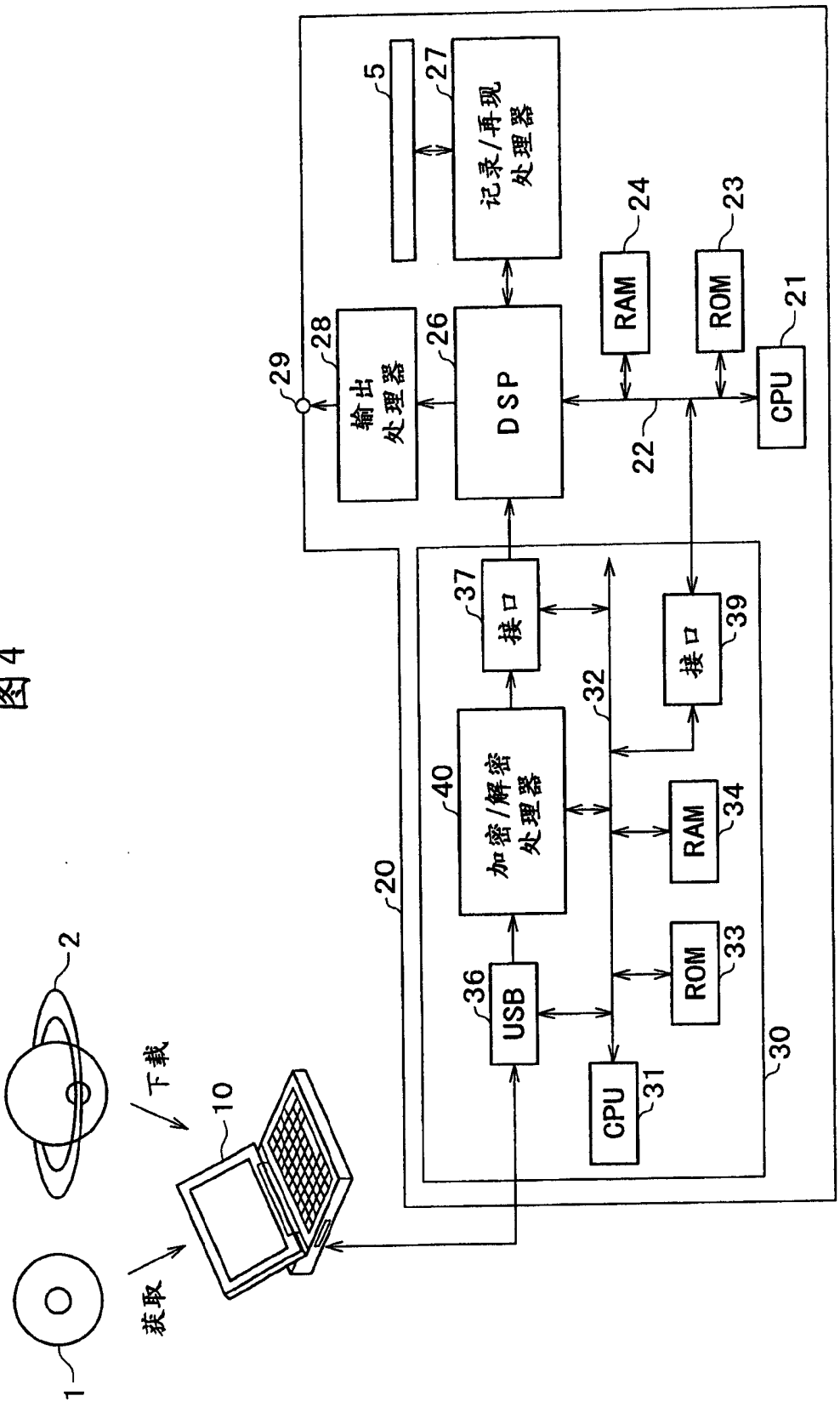
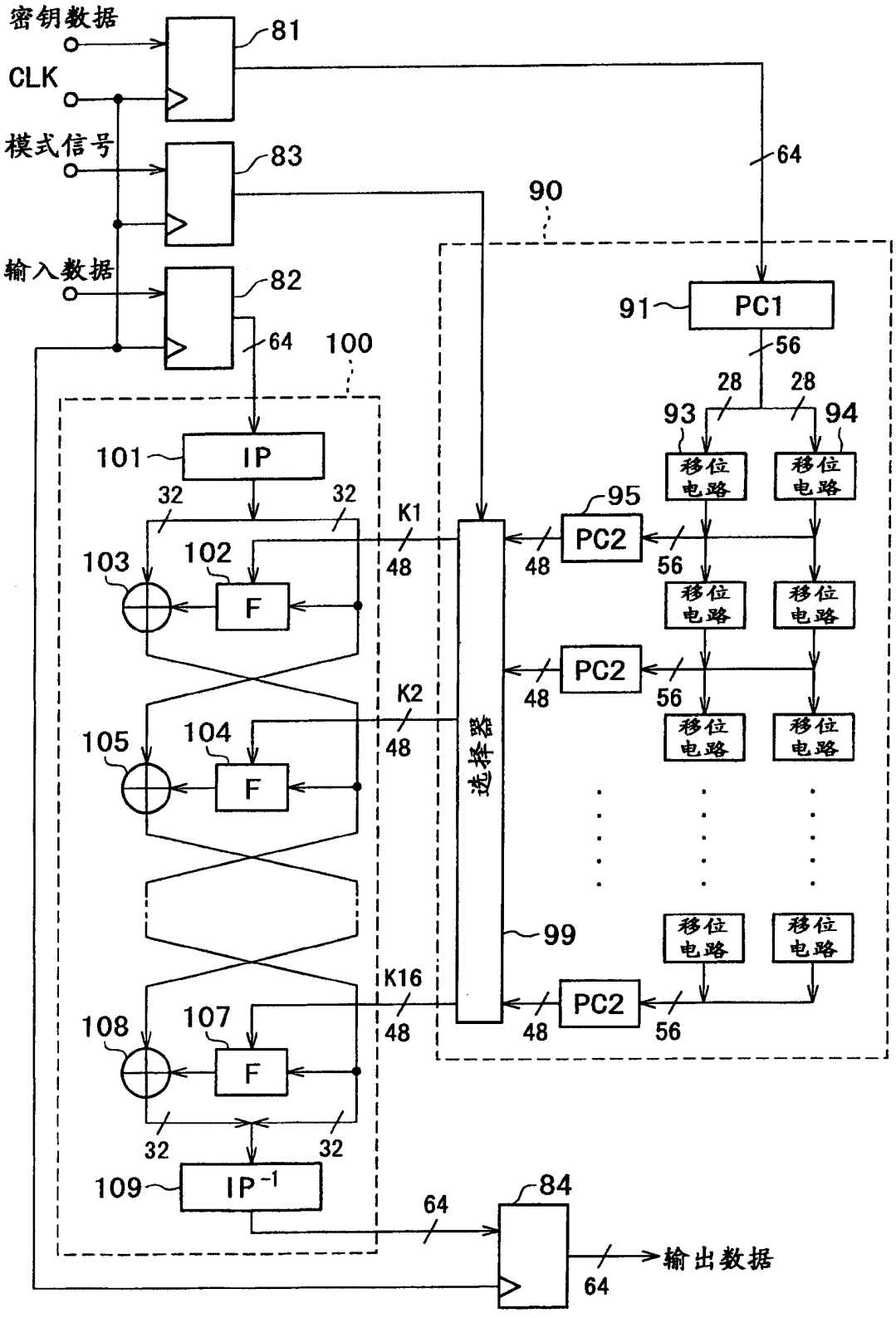

1
获取
2
下载
10
20
30
5
27
记录/再现
处理器
24
RAM
23
ROM
21
CPU
29
28
输出
处理器
26
DSP
22
37
接口
39
接口
32
40
加密/解密
处理器
34
RAM
36
USB
33
ROM
31
CPU

图5


密钥数据
CLK
模式信号
输入数据
81
83
82
64
90
91
PC1
56
28
28
93
94
移位电路
100
101
IP
32
32
K1
48
95
PC2
48
56
103
102
F
K2
105
104
99
选择器
K16
108
107
32
32
109
IP-1
84
64
输出数据
64