



[12] 发明专利申请公开说明书

[21] 申请号 02816541.1

[43] 公开日 2004年11月17日

[11] 公开号 CN 1547824A

[22] 申请日 2002.8.22 [21] 申请号 02816541.1

[30] 优先权

[32] 2001.8.24 [33] US [31] 60/314,926

[32] 2002.6.6 [33] US [31] 10/164,070

[86] 国际申请 PCT/US2002/026617 2002.8.22

[87] 国际公布 WO2003/019459 英 2003.3.6

[85] 进入国家阶段日期 2004.2.23

[71] 申请人 ZIH 公司

地址 百慕大群岛汉密尔顿

[72] 发明人 克莱夫·P·霍博格

博里斯·Y·茨尔莱恩

[74] 专利代理机构 中原信达知识产权代理有限责
任公司

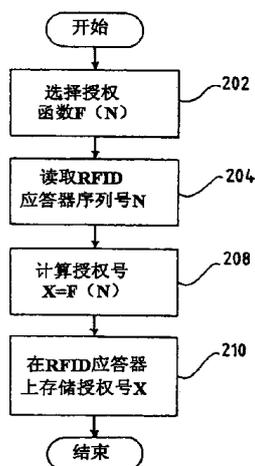
代理人 林潮 顾红霞

权利要求书 12 页 说明书 22 页 附图 13 页

[54] 发明名称 用于用品鉴别的方法和装置

[57] 摘要

一种鉴别方法，用于鉴别设备中的耗材，其包括以下步骤：a) 读取存储在该耗材中的标识号，b) 读取存储在耗材上的授权号，c) 至少部分地基于标识号，确定输入号，d) 对输入号应用授权函数，计算输出号，e) 只有在授权号与输出号相一致时才判定该耗材为正品，以及 f) 如果该耗材为正品则允许在设备中使用该耗材，如果该耗材不是正品则禁止使用该耗材。



1. 一种用于鉴别设备中用品的鉴别方法，该方法包括以下步骤：
读取存储在该用品中的标识号；
5 读取存储在用品上的授权号；
至少部分地基于标识号，确定输入号；
对输入号应用授权函数，计算输出号；
只有在授权号与输出号相一致时才判定该用品为正品；以及
如果该用品为正品则允许在设备中使用该用品，如果该用品不是
10 正品则禁止使用该用品。

2. 根据权利要求 1 的鉴别方法，其特征在于，授权函数为输入号的一种加密变换。

15 3. 根据权利要求 1 的鉴别方法，其特征在于，还包括读取存储在该用品商的媒质类型号的步骤。

4. 根据权利要求 3 的鉴别方法，其特征在于，还包括至少部分地基于媒质类型号来确定输入号的步骤。

20 5. 根据权利要求 2 的鉴别方法，其特征在于，实施加密变换的步骤还包括以下步骤：

提供第一素数 Q ；

提供第二素数 M ；

25 第二素数为第一素数的素数伽罗瓦域的素元；以及
根据以下公式计算输出号：

输出号 = $M^N \text{ MOD } Q$ ，其中 N 为输入号。

6. 根据权利要求 5 的鉴别方法，其特征在于，选择第二素数，使得第二素数大于 0、第二素数不等于 1、且第二素数不等于第一素数减 1 的差的一半。

5 7. 根据权利要求 5 的鉴别方法，其特征在于，确定输出值的步骤还包括以下步骤：

a) 通过以下步骤对部分积进行初始化：

将系数赋值为第二素数；

如果输入号的最低有效位等于 0，则将部分积赋值为 1；

10 如果预设号的最低有效位等于 1，则将部分积赋值为系数对第一素数取模；

b) 通过以下步骤从输入号的最低有效位到输入号的最高有效位迭代地估算部分积：

将系数乘以二；

15 如果输入号的下一个未估值位等于 0，则将部分积重新赋值为原部分积对第一素数取模；

如果所述预设号的下一个未估值位等于 1，则将部分积重新赋值为(a) 原部分积乘以系数对第二素数取模的结果而得到的积(b) 再对第二素数取模；以及

20 c) 在对输入号的最高有效位进行了部分积估值之后终止对部分积进行迭代估值。

8. 根据权利要求 1 的鉴别方法，其特征在于，还包括以下步骤：

在用品上提供计数器，计数器用于被设备所读取；

25 当使用该用品时，在计数器中周期性地更新用品的使用值，从而反映该用品的使用程度或耗用程度；

由设备读取该用品的耗用值；

只有在该耗用值大于预设值时才判定该用品为正品；以及

30 在该用品为正品时，允许在设备中使用该用品，并且在该用品不是正品时，在设备中禁用该用品。

9. 根据权利要求 8 的鉴别方法, 其特征在于, 还包括以下步骤:
提供可由该设备存取的数据表, 该数据表包括与在设备中使用的
多个用品相对应的识别号;

5 每个识别号都在数据表中有相关的数据项, 对应于之前读取的在
设备中曾使用的每个用品的用品耗用值;

 只有在其用品耗用值小于数据表中相应识别号的之前读取的用品
耗用值时, 才将安装在设备中的用品判定为正品; 以及

10 如果用品为正品, 则允许在设备中使用该用品, 且如果该用品不
是正品, 则禁止在该设备中使用该用品。

10. 根据权利要求 1 的鉴别方法, 其特征在于, 还包括将 RFID
应答器安装到用品上的步骤, 其中识别号和授权号都存储在 RFID 应
答器中。

15

11. 根据权利要求 1 的鉴别方法, 其特征在于, 还包括 将 RFID
收发器安装在设备上的步骤。

12. 一种设备, 用于鉴别可安装在该设备中的用品, 该设备包括:
20 读取器, 用于读取存储在该用品上的识别号, 该识别号对应于该
用品的身份;

 该读取器还适用于读取存储在用品中的授权号;

 存有计算机程序的该设备的存储器, 用于将识别号变换成输出
号, 并将输出号与授权号相比较; 以及

25 用品, 只有在输出号与授权号相等时, 该用品才得到验证, 如果
该用品为正品, 则允许在该设备中使用该用品, 如果该用品不是正品,
则不允许在该设备中使用该用品。

13. 根据权利要求 12 的设备, 其特征在于, 读取器为安装在设
30 备上的收发器。

14. 根据权利要求 12 的设备，其特征在于，将识别号变换为输出号的计算机程序包括：

设备的存储器中的准备程序，用于将识别号变换为中间号；

5 设备的存储器中的加密计算机程序，用于将中间号加密以提供输出号；以及

在其中，将输出号与授权号相比较，从而判断设备中的用品是否为正品。

10 15. 根据权利要求 14 的设备，其特征在于，预备计算机程序进行一对一的变换，从而使中间号等于识别号。

16. 根据权利要求 12 的设备，其特征在于，读取器用于读取存储在用品中的媒质类型号。

15

17. 根据权利要求 15 的设备，其特征在于，预备程序将媒质类型号用作输入来计算中间号。

18. 根据权利要求 14 的设备，其特征在于，加密计算机程序包含在计算机可读媒质中，该程序计算(a)第二素数的中间值次幂(b)对第一素数取模。

20

19. 根据权利要求 18 的设备，其特征在于，选择第二素数，使得第二素数大于 0、第二素数不等于 1、且第二素数不等于第一素数减 1 的差的一半。

25

20. 根据权利要求 18 的设备，其特征在于，包含在计算机可读媒质中的加密计算机程序还包括：

a) 进行以下工作的计算机程序初始化代码段

30 (i) 将系数赋值为第二素数；

(ii) 如果中间号的最低有效位等于 0，则将部分积赋值为 1；

(iii) 如果中间号的最低有效位等于 1，则将部分积赋值为系数对第一素数取模；

5 b) 计算机程序部分积估值代码段，其通过以下步骤从中间号的最低有效位到中间号的最高有效位迭代地估算部分积的值：

(i) 将系数乘以二；

(ii) 如果中间号的下一个未估值位等于 0，则将部分积重新赋值为原部分积对第一素数取模；

10 (iii) 如果所述中间号的下一个未估值位等于 1，则将部分积重新赋值为(a) 原部分积乘以系数对第二素数取模的结果而得到的积(b) 再对第二素数取模；

c) 在估算出与中间号的最高有效位相对应的部分积之后，终止对部分积进行迭代估值；以及

d) 将最终的部分积作为输出号输出。

15

21. 根据权利要求 20 的设备，其特征在于，还包括存储器，用于存储数据表，该数据表的每一项对应于中间号的每一位，该内容等于与该位相应的系数对第一素数取模。

20

22. 根据权利要求 12 的设备，其特征在于，该计算机程序包括用于产生多个输出号的代码，且只有在多个输出号中的一个与授权号相等时才对该用品授权。

25

23. 根据权利要求 12 的设备，其特征在于，还包括用品上的计数器，该计数器用于被设备读取，其中，读取器读取该计数器中的用品耗用值，用品耗用值反映了用品的使用或耗用程度。

30

24. 根据权利要求 12 的设备，其特征在于，该存储器还包括可由设备存取的数据表，该数据表包含对应于设备中曾使用的多个用品的识别号；以及

5 每个识别号在数据表中都具有相关的数据项，对应于之前读取的在设备中曾使用的每个用品的用品耗用值，且只有在其用品耗用值小于上次读取的数据表中相应识别号的用品耗用值时，该计算机程序判断安装在设备中的用品为正品，并且如果该用品为正品，则允许在设备中使用该用品，如果该用品不是正品，则在设备中禁用该用品。

25. 一种用于鉴别用品的主机，该主机包括：
用于读取存储在用品上的识别号的装置；
用于读取存储在用品上的授权号的装置；
10 用于至少部分地基于该识别号来确定输入号的装置；
用于对输入号应用授权函数以计算输出号的装置；
用于只有在授权号与输出号相一致的情况下才判定该用品为正品的装置；以及
用于在用品为正品时允许使用该用品并在用品不是正品时禁止使用该用品的装置。
15

26. 一种适于被主机鉴别的用品，该用品包括用于存储第一预设号和授权号的存储器系统，第一预设号对应于该用品的身份。

20 27. 根据权利要求 26 的用品，其特征在于，通过对第一预设号应用授权算法来计算授权号。

28. 根据权利要求 27 的用品，其特征在于，该预设号是唯一的、
25 厂家装载的序列号。

29. 根据权利要求 26 的用品，其特征在于，通过以下步骤计算授权号：

提供第一素数 Q；
提供第二素数 M；
30 第二素数为第一素数的素数伽罗瓦域的素元；以及

根据以下公式计算输出号：

输出号 = $M^N \text{ MOD } Q$ ，其中 N 为第一预设号。

5 30. 根据权利要求 29 的用品，其特征在于，选择第二素数，使得第二素数大于 0、第二素数不等于 1、且第二素数不等于第一素数减 1 的差的一半。

31. 根据权利要求 29 的用品，其特征在于，确定输出值的步骤还包括以下步骤：

10 a) 通过以下步骤对部分积进行初始化：

将系数赋值为第二素数；

如果第一预设号的最低有效位等于 0，则将部分积赋值为 1；

如果预设号的最低有效位等于 1，则将部分积赋值为系数对第一素数取模；

15 b) 通过以下步骤从第一预设号的最低有效位到第一预设号的最高有效位迭代地估算部分积：

将系数乘以二；

如果第一预设号的下一个未估值位等于 0，则将部分积重新赋值为原部分积对第一素数取模；

20 如果所述预设号的下一个未估值位等于 1，则将部分积重新赋值为(a) 原部分积乘以系数对第二素数取模的结果而得到的积(b) 再对第二素数取模；以及

c) 在对第一预设号的最高有效位进行了部分积估值之后终止对部分积进行迭代估值。

25

32. 一种计算机程序产品，包括：

含有计算机程序代码的计算机可读媒质，该计算机程序代码提供了第一素数、第二素数以及输入值，且第二素数是第一素数的素数伽罗瓦域的素元，该计算机程序代码具有：

30 a) 通过以下步骤对部分积进行初始化的计算机程序代码

- (i) 将系数赋值为第二素数；
- (ii) 如果输入号的最低有效位等于 0，则将部分积赋值为 1；
- (iii) 如果输入号的最低有效位等于 1，则将部分积赋值为系数对第一素数取模；
- 5 b) 通过以下步骤从输入号的最低有效位到输入号的最高有效位迭代地估算部分积：
- (i) 将系数乘以二；
- (ii) 如果输入号的下一个未估值位等于 0，则将部分积重新赋值为原部分积对第一素数取模；
- 10 (iii) 如果所述输入号的下一个未估值位等于 1，则将部分积重新赋值为(a) 原部分积乘以系数对第二素数取模的结果而得到的积(b) 再对第二素数取模；且其中
- c) 在对输入号的最高有效位进行了部分积估值之后终止对部分积进行迭代估值的计算机程序代码。
- 15
33. 用于确定整除余数的装置，该装置包括：
- 存储器；
- 存储器中的被除数存储位置；
- 存储器中的指数存储位置；
- 20 存储器中的减数存储位置；
- 存储器中的除数存储位置，存储在除数存储位置中的量等于二的存储在指数位置中的指数次幂减去存储在减数位置中的量；
- 存储在存储器中的累加算法，该累加算法将数列的各项累加，每项等于存储在被除数存储位置中的量除以存储在除数存储位置中的量得到的商，该算法在数列的第一个小于二分之一的项处停止；以及
- 25 存储在计算机存储器中的取模算法，该算法通过以下方法计算余数：存储在被除数存储位置中的量减去：存储在除数存储位置中的量乘以累加算法确定的量的整数部分所得的积。

34. 一种设计用于识别并禁用伪造媒质的媒质组件，用于热转印打印机、热打印机或其他打印机，或者用于摄影或 X 光相机或其他媒质处理系统，该媒质组件包括：具有数据存储器的防伪装置，存储器含有加密数据和与媒质组件唯一关联的参考数据；以及处理器，
5 用于存取加密数据和参考数据并在媒质不是伪造品的情况下允许使用该媒质。

35. 如权利要求 34 所述的装置，其特征在于，存储器也存储参考数据。
10

36. 如权利要求 34 所述的组件，其特征在于，所述加密数据指所述参考数据的安全变换函数。

37. 如权利要求 34 所述的组件，其特征在于，通过对参考数据实施加密算法而产生所述加密数据。
15

38. 如权利要求 34 所述的组件，其特征在于，通过实施单向函数产生所述加密数据。

39. 如权利要求 34 所述的组件，其特征在于，所述存储器还包括代表媒质的种类或型号的媒质类型数据。
20

40. 如权利要求 34 所述的组件，其特征在于，所述防伪装置包括 RFID 应答器。
25

41. 如权利要求 40 所述的组件，其特征在于，所述应答器包括构成所述数据存储器的存储器。

42. 如权利要求 41 所述的组件，其特征在于，所述防伪装置可响应于处于可见、红外或紫外光谱范围内的电磁信号。
30

43. 如权利要求 34 所述的装置，其特征在于，所述数据存储器为应答器存储器。

5 44. 如权利要求 34 所述的装置，其特征在于，所述防伪装置包括具有存储器 RFID 应答器，该存储器构成数据存储器。

45. 如权利要求 34 所述的装置，其特征在于，所述媒质处理系统为热转印打印机，且所述媒质为热转印色带。

10

46. 如权利要求 34 所述的装置，其特征在于，所述媒质处理系统为热转印打印机，且所述媒质为直接热记录媒质。

15

47. 一种轴形的媒质支撑件，用于热转印打印机、热打印机或其他打印机，或者用于摄影或 X 光相机或其他媒质处理器，其具有带有轴线和端部凸缘的轴杆，天线位于其上。

48. 如权利要求 47 所述的装置，其特征在于，所述天线包括至少一个与所述轴轴线同心的弧形导体。

20

49. 如权利要求 47 所述的装置，其特征在于，所述天线包括一系列成对的同心环形导体，它们由所述轴的所述端部凸缘支撑。

25

50. 如权利要求 49 所述的装置，其特征在于，所述导体包括集成电路。

51. 如权利要求 47 所述的装置，其特征在于，所述天线与数据存储器和数据存储器相连。

52. 如权利要求 51 所述的装置，其特征在于，所述数据存储单元含有加密数据。

53. 如权利要求 47 所述的装置，其特征在于，所述天线包括无线
5 应答器的一部分。

54. 如权利要求 53 所述的装置，其特征在于，所述应答器为 RFID
应答器。

10 55. 如权利要求 47 所述的系统，其特征在于，所述媒质处理器包括媒质耗用计数器，用于记录媒质的耗用情况并将耗用标志存储在媒质组件上。

15 56. 如权利要求 55 所述的系统，其特征在于，所述耗用标志用于拒绝这样的媒质组件：记录的耗用量大于等于预设的耗用值。

57. 如权利要求 55 所述的系统，其特征在于，所述媒质处理器为激光打印机。

20 58. 一种热转印打印机、热打印机或其他打印机，或者用于摄影或 X 光相机或其他媒质处理系统，用于识别伪造的媒质组件，所述系统包括用于执行加密算法的程序以便鉴别媒质组件。

25 59. 如权利要求 58 所述的系统，其特征在于，所述算法由安全微处理器执行。

60. 如权利要求 58 所述的系统，其特征在于，所述系统包括媒质处理器，且所述程序存放在所述处理器中。

61. 如权利要求 58 所述的系统，其特征在于，所述系统包括媒质处理器和远程处理站，且所述程序处于远程处理站中。

5 62. 如权利要求 58 所述的系统，其特征在于，所述加密算法对存储在媒质组件上的数据进行运算。

63. 如权利要求 62 所述的系统，其特征在于，所述数据包括参考数据和由参考数据产生出的加密数据。

10 64. 如权利要求 63 所述的系统，其特征在于，采用所述加密算法产生所述加密数据。

65. 如权利要求 58 所述的系统，其特征在于，所述加密算法包括单向函数。

15

66. 如权利要求 65 所述的系统，其特征在于，所述单向函数利用伽罗瓦域中的取模算法。

用于用品鉴别的方法和装置

5 技术领域

本发明总的涉及一种用在主机中的用品的鉴别技术。更具体地，本发明的一个具体的实施例涉及对热标记装置的墨盒或墨桶作出的一项改进，其中，能够对墨盒或墨带进行鉴别，确定其为合适的型号且来自于经授权的货源。

10

背景技术

曾经有其他的方法试图鉴别主机中的耗材，但事实证明它们都不能令人满意。特别是，以下讨论的现有方法都不能提供有效的防盗版手段。这些从前已知的方法无法提供足够的鉴别能力，且经常被复制、

15

电子欺骗或类似的技术所破解。

一种早期的鉴别耗材的技术依赖于耗材的键式外形。可以将这样的键式外形设计成只有有键式外形的耗材才能够配合进给定型号的主机中。例如，某种牌子的剃须刀可以设计为只接纳具有某种键形的刀片。再例如，喷墨打印机可以设计为只接纳具有某种键形的重灌墨盒。

20

使用这样的键式外形能够防止不同主机型号之间的耗材互换。但是，该方法总的来说对于防盗版是无效的，因为耗材的键式形状能够被轻易地观察到并被复制。

设计用于汽车安全系统的应答器中使用的“问答（challenge and response）”式鉴别算法，例如 Atmel TK556 等等，也是不能令人满意的。汽车安全系统设计用于“一锁多钥”应用，其中，将单一的密码编到每个钥匙和每个锁中。如果一个主机，例如打印机或照相机，是“锁”的话，那么这样的问答应答器就需要将所有的钥匙（媒质）

25

30

在如胶卷的耗材上和/或在如照相机的主机上提供编码作为识别用途并传递有关胶卷或相机的信息，这点已经是众所周知的。术语“编码”很宽泛地表明了实体媒质的特征，用于将一条或多条信息送给主机。5 “编码”包括文字数字的文本以及其他的标记、符号等等。可以采用各种手段来检测编码，包括光学、磁性、和/或打孔卡的读卡机，并且不止于此。

美国专利 No. 6,106,166 公开了一种具有应答器和收发器的装置。10 装在应答器中的电气的或电子的可编程读/写存储器与耗材整体相连。应答器能够接收第一 RF 频率电磁场并从其中得到能量和地址信息，之后生成第二 RF 频率电磁场作出应答。第二电磁场带有的特征是存储器中存储的数据。收发器位于主机内部，带有天线和支撑部件，用于轮流检测每个应答器。如控制逻辑处理器所指示的，收发器能够从15 应答器处读取制造信息并将用法和处理数据写入应答器以便存入存储器。

射频识别应答器可以呈各种形式。一种被称为“内置应答器”的形式是具有基本扁平形状 of 识别应答器。用于内置应答器的天线的形式是位于非导电支撑件上的导电路径。该天线可以呈扁平线圈等等的形状。还布置有天线的引线，且如果需要，在引线之间插入非导电层。20 存储器部件，RF 通讯，以及任何控制功能都由安装在支撑件上的芯片提供并通过引线以可工作方式连接到天线。内置应答器一直用作识别标签或标贴的叠层，以提供能够在一定距离之外得到的编码。在美国专利 No. 6,173,119 中公开了一种具有射频识别应答器的照相机，能够在一定距离之外访问该照相机以进行读写。25

另一种已知类型的应答器是射频识别（RFID）应答器。RFID 应答器通常可包括由制造者安装在非易失性存储器（non-volatile memory）中的独特的识别器。30

对于主机来说，提供带有应答器的耗材是众所周知的，例如墨盒。这样的主机，例如安装有墨盒的打印机，包括用于检测墨盒上媒质类型的收发机。在颁发给 Spurr 等人的美国专利 No. 6,099,178 中公开了这种总体类型的收发机和应答机。Spurr 的专利公开了一种打印机，用于检测装入媒质的类型，并包括射频收发器，用于发出第一电磁场并检测第二电磁场。但是，Spurr 没有描述或示意出用于鉴别承载应答器的媒质的装置。编码在 Spurr 专利的应答器中的信息可以被轻易地伪造，从而使得该系统在作为防盗版手段时变得无能为力。

10

国际公开号 WO 98/52762 公开了一种打印机，其使用一种 RFID 标签，用于识别装入喷墨打印机的纸张的类型。该方法提供了与附加到喷墨辊上的读/写存储器之间进行非接触式通讯的技术方案。然而，该发明并未记载或示意出与此发明相应的鉴别方法和装置。

15

因此，需要提供一种有效的采用应答器和收发器的防盗版手段来检测用于主机的耗材上的编码信息，例如用于打印机的媒质。

附图说明

应该相信，当与附图相结合时，从下面的说明中将能更好地理解本发明，在附图中：

图 1A 为根据一个实施例的装入主机中的耗材的顶视左视透视图。

图 1B 为根据一个实施例的装入主机中的耗材的顶视正视透视图。

图 2A 为程序流程图，示出制备可鉴别耗材的操作顺序的一个实施例。

图 2B 为程序流程图，示出制备可鉴别耗材的操作顺序的一个实施例。

图 3A 为根据一个实施例的要鉴别的耗材以及主机的顶视右视透视图。

图 3B 为根据一个实施例的用于鉴别的耗材以及用于对本发明进行鉴别的主机的顶视右视透视图。

5 图 4 为系统流程图，示出用于鉴别耗材的方法的一个实施例中的操作顺序以及数据流。

图 5 为装进主机中的耗材的部分顶视左视透视图，示出根据一个实施例的鉴别部件的位置。

10 图 6 为装进主机中的耗材的部分顶视右视透视图，示出根据一个实施例的鉴别部件的位置。

图 7A 为根据一个实施例的带有安装在一侧的鉴别器电路的耗材墨盒的透视图。

图 7B 为安装在耗材上的鉴别部件的放大图。

15 图 7C 为根据一个实施例的带有安装在一侧的鉴别器电路的耗材墨盒的侧视图。

图 7D 为根据一个实施例的带有安装在一侧的鉴别器电路的耗材墨盒的顶视图。

图 8 为根据一个实施例的耗材、主机、以及鉴别电路的框图。

20 图 9 为透视图，示出根据一个实施例的主机中用于鉴别耗材的电路板的位置。

图 10A 为用于安装在主机上以鉴别耗材的电路板的第一实施例的后视图。

图 10B 为用于安装在主机上以鉴别耗材的电路板的第一实施例的正视图。

25 图 11 为根据一个实施例的带有安装在凸缘上的鉴别器电路的耗材墨盒轴的透视图。

图 12A 为根据一个实施例的带有安装在凸缘上的鉴别器电路的耗材墨盒轴的侧视图。

30 图 12B 为根据一个实施例的带有安装在凸缘上的鉴别器电路的耗材墨盒轴的第一端视图。

图 12C 为根据一个实施例的带有安装在凸缘上的鉴别器电路的耗材墨盒轴的第二端视图。

图 12D 为根据一个实施例的带有安装在凸缘上的鉴别器电路的耗材墨盒轴的侧剖视图。

5 图 13 为根据采用网络连接的实施例的耗材、主机、以及鉴别电路的框图。

具体实施方式

10 本说明书特别用于说明形成根据本发明的装置的一部分的部件或与其更直接地配合的部件。应该理解，未具体示出或说明的部件可以呈本领域技术人员已知的各种形式。在此说明书中，术语“耗材”指设计用于在称为主机的设备中耗尽并更换的部件。耗材及其各自主机的例子包括：用在打印机中的喷墨墨盒，用在照相机中的胶片、用在打字机上的色带、和/或用在复印机中的色粉盒。

15

现在参考图 1A，主机 100 用于接纳耗材 120。此具体实施例中的主机 100 可以是用于在塑料卡片上采用热传递方法打印条形码的塑料卡打印机。此实施例的耗材 120 可以是含有色带 150 的色带盒，该色带 150 的例子如树脂基热转印色带或染料升华色带。塑料卡打印机主机 100 可包括其他的传统部件（未示出），例如打印头、磁编码台、电源开关、控制面板、进卡器、卡片输出斗、以及其他的部件。一个可打开的打印机盖 162 掩盖了色带盒耗材 120 的内部机构并有助于限制诸如尘土和异物的污物进入。在此实施例中，机盖释放按钮 160 在塑料卡打印机 100 的一侧示出。第二机盖释放按钮（未示出）可位于另一侧。此实施例中，左内壁 167L 和右内壁 167R 在塑料卡打印机主机 100 中形成直槽 165，用于接纳色带盒耗材 120。首先按下塑料卡打印机主机 100 的一侧的机盖释放按钮 160 打开打印机盖 162，之后将色带盒耗材 120 竖直插入直槽 165，并将色带盒耗材按下就位，通过上述步骤可将色带盒耗材 120 装入塑料卡打印机主机中。触觉或听觉的反馈能够指示出色带盒耗材 120 已经被正确安装。

20

25

30

还是参考图 1A 中示出的实施例，色带盒耗材 120 可包括供给轴 140 和拾取轴 145。使用色带盒耗材 120 之前，色带 150 围着供给轴 140 卷绕成一卷。当使用色带 150 且色带盒耗材 120 耗尽时，色带 150 卷绕在拾取轴 145 上。在图示的实施例中，由左支撑件 147L 和右支撑件 147R 将供给轴 140 和拾取轴 145 以相对固定的方式间隔开。供给轴 140、拾取轴 145、左支撑件 147L 以及右支撑件 147R 一起构成了四条边，形成色带 150 可穿过的矩形空间。在图 1A 示出的实施例中，射频识别（RFID）应答器 130 设置在色带盒 120 的左支撑件 147L 上。尽管在图示的实施例中，RFID 应答器 130 位于左支撑件 147L 上，但实际应用时也可将其设置在任何合适的位置，例如设置在右支撑件 147R 上。当然，如本领域内所公知的，无需将应答器限制为射频信号，且该应答器可利用任何形式的合适的电磁辐射，例如可见光、紫外线和红外线。

15

根据图 1A 示出的实施例，RFID 应答器 130 可包括独特的、工厂内编程的序列号 n 。这种能够买到的 RFID 应答器每个都包含了独特的 32 到 64 位的应答器序列识别号码 n ，用在“防冲突”协议中。该协议能够分开并单独识别同时出现在 RFID 读取器的场中的多个应答器，多个主机处于相对较近的范围时就可能导致这种情况。

20

使用由色带盒耗材 120 的制造商选择并保密的加密函数 F 计算授权号 x 。授权号永久储存在 RFID 应答器 130 中。打印机主机 100 在其工作期间能够得到加密函数 F 。例如，在图 8 示出的一个实施例中，可在制造过程中将保密的加密函数 F 事先编入打印机主机 100 中。在另一实施例中，打印机主机可在网络上得到保密的加密函数 F 。当色带盒耗材 120 装入打印机主机 100 时，打印机的内部 RFID 收发器（在图 1A 中未示出）从与色带盒耗材 120 相连或位于其上的 RFID 应答器 130 处读取序列号 n 以及授权号 x 的值。之后，它将判断授权号 x 在由保密的加密函数 F 变换之后，是否与序列号 n 相符。如果两个值

30

相符，则将色带盒耗材 120 视为可以在该打印机上使用的授权的媒质产品。

5 每个来自给定制造商的打印机 100 都可以在工厂中以相同的加密算法编码。当生产色带盒耗材 120 时，在打印机中提供相同的用于生成授权号的加密算法。一旦安装了色带盒耗材 120，就读取了应答器的独特序列号 n 。在优选实施例中，应答器的独特序列号 n 已经由制造商锁定在了 RFID 应答器 130 中。

10 色带盒耗材 120 的制造商还知道要制造的媒质的类型 y 。在另一实施例中，将 n 和 y 的值结合在一起以用在加密算法中来计算授权码 x 。之后，色带盒耗材 120 的制造商将 x 和 y 值编入并锁定在应答器 130 的存储器中。以此方法，能够生产出实际上无限数量的独特的媒质卷或卡盒，每个都包含着独特编码并锁定的序列号 n 的值、媒质类型号 y 的值、以及授权号 x 的值。

15 尽管序列号 n 、媒质类型号 y 、以及授权号 x 都是能够自由读取的，但优选地，保密的加密函数 F 从已知的没有明显反函数的函数类中选取。相应地，这样的函数是难以解码的，从而提供了安全的鉴别能力。为了制造出能在根据图 1 所示实施例的打印机 100 上工作的伪造的色带盒耗材 120，色带盒耗材 120 的伪造者将不得不重建能够用于打印机 100 的算法 F 。

25 如果算出 x 的值作为独特且无法复制的应答器序列号 n 的复杂函数，则 n 和 x 的值能够都存储在 RFID 应答器 130 中，在该处将两个号码编码加密并可由任何人读取。可选择地，如果将媒质类型号 y 也用在变换中，则也可将其存储在 RFID 应答器中。当色带盒耗材 120 安装在打印机 100 上时，打印机能够从应答器读取 x 和 n （以及可选地读取 y ），并验证读取的 x 值是否与读取的 n 值（以及可选地读取的 y 值）相符，从而验证是否是用于相应打印机 100 的色带盒耗材 120。

从已知的强加密算法中精心地选择一种算法用于 F，可使得破解该安全系统变得非常困难并且在实际操作上昂贵得使人望而却步。通过用一些函数将 n 加密，可采用加密法来计算授权码 x。伪造者能够得到的唯一信息就是给定色带的授权码 x 与给定的序列号 n 相符合。5 更具体地说，伪造者将不能够知道或研究出对于给定的 n 如何得到 x 的值。伪造者也无法随机地试验所有可能的 n 值，因为除非伪造者已经得到了同时具有那个 n 和相应的授权码 x 的正品媒质卷，否则就无法知道 x 的值。所以，伪造者只能拥有有限的 n、x 的样本用于测试。

10

对于用序列号 n 和媒质类型号 y 的函数来计算 x 的实施例来说也是同理。通过用一些函数对 n 和 y 进行加密，可采用加密法来计算授权码 x。同样的，伪造者能够得到的唯一信息就是给定色带的授权码 x 与给定的一对 n、x 相符。

15

为了进一步防止安全系统被破解，可将在测试值之间形成可接受关系的多个函数存储在主机中。之后，可将耗材用多个授权号编码，每个授权号都满足具体的授权函数关系。如果知道了任何具体的授权函数被破解，则可以采用一个其他的授权函数和授权值来验证媒质。20 可在主机中将被破解的授权函数关闭以防止授权给采用被破解的授权函数制造的盗版媒质。例如，根据在后续媒质中设定的标记或通过对主机软件或硬件进行升级，能够将被破解的授权函数关闭。

25

如本领域所公知的，主机或打印机 100 包括：合适的存储器，例如 RAM、ROM、EEPROM 等等、输入/输出设备、计算机或中央处理器、可选的磁盘存储以及相应的支持设备，所有这些部件均未示出。该计算机可以是，例如，具有例如 Pentium®或 Intel 系列微处理器的 IBM 兼容型计算机。可选择地，该计算机也可以是具有 Motorola 系列微处理器的 APPLE®兼容型计算机。但是，该计算机或中央处理器也可以是任何的计算机、处理器、中央处理器（CPU）、微处理器、RISC（精30

简指令集计算机)、大型计算机、工作站、单片机、分布式处理器、服务器、控制器、微控制器、离散逻辑设备、远程计算机、互联网计算机或网络计算机。与计算机相应的存储器和/或磁盘存储器设计用于存储程序指令，程序指令表示算法并执行在此描述的各个步骤。这样的程序指令可从磁盘存储器或从诸如 ROM、PROM、EPROM 等的非易失性存储器中“下载”，或者也可以通过网络或其他的通讯联接从远程数据源下载。

现在参考图 1B 所示的实施例，示出了塑料卡打印机主机 100 以及色带盒耗材 120。在图 1B 中示出，色带盒耗材 120 装入塑料卡打印机主机 100 中。在这个具体的实施例中，可将该色带盒耗材 120 插在左内壁 167L 和右内壁 167R 之间。图中示出 RFID 应答器安装在左支撑件 147L 上，但也可以安装在其他地方，例如安装在右支撑件 147R 上。装入色带盒耗材 120 之后，能够将机盖 162 盖上并操作塑料卡打印机主机 100。

为了简化说明，以下说明的本发明的实施情况将只采用序列号 n 和授权号 x 。但是，将媒质类型号 y 与序列号 n 一起使用以计算授权号 x ，这也在本发明的范围内。使用序列号 n 与使用媒质类型号 y 的不同之处可以在于，在制造 RFID 应答器时，序列号可永久地固定在其中，并且对于每个应答器都可以是独一无二的。另一方面，在工厂中可将媒质类型号 y 存储在 RFID 应答器中，且对于每种给定类型的媒质都是相同的。但是，此处说明的在鉴别或加密计算中对于序列号 n 的使用是与对于媒质类型号 y 的使用相同的。

图 2A 为程序流程图，示出用于准备一种用在主机中的可鉴别耗材的操作顺序的一个实施例。首先，制造商必须选择一个合适的授权函数，由选择授权函数 F 步骤 202 表示。优选地，如果只给出较少的几个 x 和 n 的值，函数 F 是非常难以识别的。在选择授权函数 F 的步骤 202 之后，下一步是读取 RFID 应答器的序列号 n 的步骤 204。可

鉴别式耗材的制造商必须从要安装到耗材上的 RFID 应答器中读取序列号 n 。序列号 n 在工厂中装载并且对于每个应答器都是独特的。下一步，制造商可执行计算授权号 $x = F(n)$ 的步骤 208。函数 F 的定义域不仅限于 n 的设定值，具体来说， F 可以是多变量函数，如以下将详细说
5 明。通过计算授权号 $x = F(n)$ 的步骤 208 计算出授权号 x 之后，接着通过将授权号 x 存储在 RFID 应答器中的步骤 210，将授权号 x 放在应答器的公共数据区。

在图 2B 中示出用于准备一种用在主机中的可鉴别耗材的操作顺序的另一个可选择的实施例。在此实施例中，制造商首先在选择授权函数 $F_{M,Q}$ 的步骤 202' 中选择授权函数。优选地，该可选实施例的选择授权函数 $F_{M,Q}$ 的步骤为在密码学中使用的经典的单向函数，其可以基于取模运算以及伽罗瓦域运算（Galois Field arithmetic）。伽罗瓦域运算，特别是配合单向函数 $[M^G \bmod Q]$ 时，在公钥密码学中广泛应用。
10 举一个例子来说，Diffie-Hellman 方法就采用了这种手段。对参数 M 和 Q 进行选择，独特地确定了函数 $F_{M,Q}(G) = M^G \bmod Q$ 。举例来说，如在本领域所公知的，在句子中可以按以下方式表达“取模”符号：

G 的函数值等于 M 的 G 次方的值对 Q 的值取模。

参数 M 和 Q 是两个素数值（prime values），它们之间的关系是， M 是 Q 阶素数伽罗瓦域（prime Galois Field） $GF(Q)$ 的素元（primitive element）。在选择授权函数 $F_{M,Q}$ 的步骤 202' 中设定好加密函数之后，下一步就是读取 RFID 应答器序列号 n 的步骤 204。图 2B 所示实施例的下一步是识别耗材类型 y 的步骤 206。数字 y 是由制造商选出零件号
20 码，用于指明媒质的具体类型，制造商将把该 RFID 应答器装配到该媒质上。

下一步是选择预备函数（preparatory function） $G(n, y)$ 的步骤 208。函数 $G(n, y)$ 的值域变为函数 $F_{M,Q}(G)$ 的定义域，从而使复合函数 $F \circ G$ 将
30 输入值 n, y 映射到授权号 x 。优选地，函数 $G(n, y)$ 是独特的（unique）

且对于可鉴别耗材的制造商是保密的。优选地，预备函数 $G(n,y)$ 可将每对 n 、 y 映射为唯一的结果，但这样的一对一映射并不是本发明所必须的。优选地，预备函数 $G(n,y)$ 应避免某些退化的 (degenerative)、病态的 (pathological) G 值。特别是，优选地该函数应该避免得到处于以下值域内的值：

$$G \leq 0,$$

$$G = 1,$$

$$G = \frac{Q-1}{2}, \text{ 和}$$

$$G = (Q-1).$$

如从伽罗瓦域数论中所知，产生这些值的函数 G 可能会破坏编码函数 $F_{M,Q}$ 的安全性。选择好合适的预备函数 $G(n,y)$ 之后，图 2B 所示实施例中示出的操作顺序中的下一步是计算授权号 $x = F_{M,Q}(G(n,y))$ 的步骤 208。计算完毕之后，在将授权号 x 存储到 RFID 应答器的步骤 210 中，将授权号 x 存储到一个实施例的 RFID 应答器的公共数据区。此外，在将耗材类型号 y 存储到 RFID 应答器的步骤 212 中，将代表媒质类型的数字 y 存储在应答器中，之后，即完成了图 2 的实施例中所示的操作顺序，使耗材媒质变得可以被鉴别。

图 3A 和 3B 示出将耗材 120A、120B 从主机 100 上卸下和安上的另一实施例，其中，耗材 120A、120B 为色带盒，且主机 100 为塑料卡打印机。为了在使用过耗材之后从塑料卡打印机主机 100 上卸下色带盒耗材 120A、120B，打开机盖 162，然后将主机 120B 中的色带盒耗材拉出 (310)，去掉色带盒耗材 120A。为了将色带盒耗材 120A 卸下，将其竖直地插入 (320) 并按压就位(120B)。

图 4 为系统流程图，总的示出该系统的运作流程以及数据流，用于一个具体的实施例，检测装入主机中的耗材是否为正品。当耗材媒质装在打印机主机上时，主机首先在检测耗材的步骤 410 中检测到新装入耗材。可以通过机械传感器、识别邻近的 RFID 应答器、或者其他任何合适的用于此类检测的传感装置来检测该耗材。在检测到新耗

材之后，打印机的内部 RFID 收发器从安装在媒质上的应答器处读取序列号 n 、授权号 x 、以及耗材类型 y 的值。

5 这在图 4 所示的实施例中以三个连续的步骤示出：读取序列号 n 的步骤 415、读取耗材类型号 y 的步骤 420、以及读取授权号 x 的步骤 425。这些操作的顺序并不重要，并且在其他的实施例中，在不背离本发明的范围的前提下，可以按照不同的顺序来执行这些操作。读取耗材类型号 y 之后，在图 4 所示的实施例中，在检查耗材类型有效性的步骤 430 中对耗材对于该具体主机的有效性进行检查。在此实施例中，对于具体主机的有效媒质类型 y 是已知的。如果耗材属于对于该主机无效的类型，则主机将采用报告状态步骤 480 来报告不兼容色带盒的状态并终止工作。如果媒质类型与该主机不兼容，则不必检查该媒质是否为正品。

15 还是参考图 4 的实施例，授权函数数据 490 可以用于检查耗材媒质是否为正品。可在出售前在主机中编入相同的授权函数，随后利用该函数制造用于该主机的耗材。可将确定该授权函数的步骤顺序作为授权函数数据 490 存储在主机中。如果耗材属于对于该主机有效的类型 y ，则在检查授权号的步骤 440 中使用授权函数 490 检查授权号 x 。检查授权号的步骤 440 将 n 和 y 作为输入执行形成授权关系的算法，并将其内部计算的 $x = F_{M,Q}(G(n,y))$ 的值与从应答器读取到的 x 值进行比较。如果它们相同，则这是一个类型为 y 的经过授权的媒质产品，可以在该打印机上使用。如果检测出一卷媒质带有不正确的授权码 x ，则由重置标志步骤 475 将所有的有效性标志和剩余媒质计数器重置为零并锁定。打印机不仅检测出了这个伪造的媒质，而且一旦检测出其状态设定为“完全耗尽”，就使其在将来不能用于任何应用。

30 在此实施例中，主机可以得到曾用耗材列表数据 470，从而确保从前用尽的色带盒不被插入。在该耗材通过验证之后，在使用耗材的步骤 460 中将其在主机中使用，例如使用色带盒来打印产品。在一个

实施例中，当判断出耗材已被使用耗材的步骤 460 完全耗尽时，将耗材的一个标识（如唯一的序列号 n）存储在用尽耗材列表数据 470 中，表示该耗材已经用尽。在另一实施例中，曾用耗材列表数据 470 可以包括装入主机中的所有耗材的标识以及在每个耗材中剩余使用寿命的百分比。曾用耗材列表数据 470 能够廉价地存储关于大量从前用过的耗材的信息，例如，在塑料卡打印机中用过的前 512 个墨盒的列表。如果一个色带盒或色带卷再次出现，并且带有比存储在塑料卡打印机的存储器中更高的剩余计数量，则该塑料卡打印机将重复装入的色带盒或色带卷视为具有无效的授权，并且不仅能够拒绝使用该媒质，而且还能将其应答器锁定为“完全耗尽”的状态。

接着参考图 5 和 6 的实施例，在图 5 中示出包含可鉴别耗材的主机的一个实施例的顶视左视部分透视图。图 6 示出包含可鉴别耗材的主机的一个实施例的顶视右视部分透视图。图中示出耗材 120 装载在主机 100 中、示出射频识别（“RFID”）应答器 130 装载在耗材 120 上。主机 100 中的天线 510 使其能够读取耗材 100 上 RFID 应答器 130 中存储的信息。

接着参考图 7A-7D，有若干示出耗材的视图。色带盒在图 7A 的透视图示出。色带盒耗材 700 在一端具有供给轴 710，在另一端具有拾取轴 720，通过左支撑件 730L 和右支撑件 730R，供给轴 710 和拾取轴 720 彼此相连。图中示出通讯部件 740，其可以是射频识别（RFID）应答器。在两个支撑件 730L、730R 之间，色带 750 从一个轴 710 穿到另一轴 720。

图 7B 为一个实施例中的通讯部件 740 的 RFID 应答器标签及其装配。应答器可以位于左支撑件 730L 或右支撑件 730R 的内侧或外侧。标签也可以位于支撑件上以说明 RFID 应答器。

图 7C 为根据一个具体实施例的耗材 700 的侧视图。色带盒耗材 700 在一端具有供给轴 710，在另一端具有拾取轴 720。供给轴 710 和拾取轴 720 通过支撑件 730 相连。在支撑件 730 上安装有通讯部件 740，其可以是一个 RFID 应答器。

5

图 7D 为根据本发明的一个具体实施例的耗材 700 的顶视图。色带盒耗材 700 在一端具有供给轴 710，在另一端具有拾取轴 720。通过左支撑件 730L 和右支撑件 730R，供给轴 710 和拾取轴 720 彼此相连。通讯部件 740 安装在左支撑件 730L 或右支撑件 730R 上，该通讯部件 740 可以是 RFID 应答器。

10

现在参考图 8，图中示出用于在主机中鉴别耗材的耗材鉴别系统的示意图。耗材 800 可包括，例如，具有供给轴 805、拾取轴 810 以及支撑件 815 的色带盒。耗材 800 可包括通讯部件 820、835，用于将信息发送到主机 850。在一个实施例中，通讯部件 820、835 可以是低成本 RFID 应答器，其具有两种特性。首先，优选地，该低成本类型的 RFID 应答器可包括厂家编入的唯一序列号 n (830)，用户无法将其改变，也无法通过将公共数据区 825 复制到其他类似型号的应答器中而将其复制。因此，每个应答器都是唯一编码的，这正是大多数类型的具有“防冲突”协议的 RFID 应答器的一个要求，能够区分所有的处于 RFID 读取器的天线场中的多个应答器。

15

20

第二，优选地，低成本 RFID 应答器具有这样的能力，能够将数据值 x 和 y 一次性地写入（或写入并锁定）到应答器的公共数据区 825 中。在此具体实施例中，值 y 为媒质类型信息，因为不是所有的媒质类型都能够所有型号的打印机上工作。非零数据值 x 将是 y 与该应答器的唯一标识号 n 的复杂函数。在这个示出的例子中，值 x 将由厂家在制造媒质时编入应答器，或者至少是在其离开制造商的库房前编入应答器。

25

飞利浦 (Philips) I*Code 及其等同物以及任何符合 ISO (国际标
准组织) 15693 号标准的 13.56 MHz RFID 应答器都具有厂家编程的、
不可复制的 48 位序列号, 能够在芯片中永久地存储相应的 (从序列
号产生出的) 授权码。ISO 15693 的第 4.1 部分说明了每个符合标准的
5 应答器都应由 64 位的唯一标识 (UID) 所表示, 该唯一标识应由 IC
制造商永久地设定, 并按如下形式构成:

MSB

LSB

64	57	56	49	48
				1
十六进制'E0'		IC 制造商码		IC 制造商序列号

10 最重要的字节是十六进制'E0', 后面跟着 8 位的 IC 制造商码,
该码由 ISO 7816-6/AM1 分配。48 位的序列号应由上述的 IC 制造商分
配。可以预计, 各个制造商将生产符合 ISO 15693 标准的应答器, 并
在工厂内向其中编入序列号以及在 ISO 7816 下注册的唯一的制造商
ID。可以将制造商的唯一的 8 位 ID 或者合格制造商的 ID 列表作为鉴
15 别过程的一部分包括在其中。

还是参考图 8 的具体实施例, 主机 850 包括通讯部件 855、860,
用于读取存储在耗材上的 n 、 x 、和 y 的值。处理器 865 能够接收存储在
耗材上的信息并能够采用处理器能得到的授权函数 (870)
20 $F(M, Q, x, y)$ 来确定授权码 x 和序列号 n 以及媒质类型码 y 之间存在着
授权关系。优选地, 处理器 865 是安全微处理器。打印机的媒质鉴别
程序存储在安全微处理器中, 因此对于潜在的盗版行为是隐藏的。鉴
别程序无法从打印机中读出, 也不能在其运行的过程中观察到该程
序。这有助于防止潜在的盗版者判断或重建出用于从 n 和 y 计算出 x
25 的授权算法。

优选地, 耗材包括标志 827, 以便指出媒质部件的数目, 例如用
在耗材上的色带板。每个色带卷芯或色带盒只能使用一次。应答器中

的其他存储元件记录媒质的使用情况，并保留媒质计数。在用完媒质的每个单位部分（通常为 10-15%）时，应答器存储器中的标志被重置并锁定。由于最多只有 15%的额外媒质能够重装到色带芯或色带盒上，所以这使得重复利用部分用过的色带芯或盒变得在经济上不具有吸引力。当然，该标志也可以用于指示任何程度的使用情况。

参考图 8 中示出的实施例，处理器 865 可以得到曾用耗材的列表 880。“曾用盒”列表保存在每个打印机中。之前的 512 个色带盒的序列号 n 以及它们的剩余条数计数存储在每个打印机中。如果一个色带盒再次出现且具有高于存储在打印机存储器中的剩余条数计数，则打印机能够将该重装的色带盒或色带卷视为具有无效的授权，并且不仅拒绝使用该媒质，还能够将其应答器锁定到“完全耗尽”的状态，从而防止用过的媒质被再次填充。

接着参考图 9，示出了安装在主机上的通讯部件的具体实施例，用于读取耗材上通讯部件。图中示出了主机框架 910。此处示出的具体的主机框架 910 为塑料卡打印机框架，去掉了外部塑料外壳。电路板 920 安装在该主机框架 910 上。电路板 920 包括天线 930，用于读取射频识别应答器（未示出）。电路板 920 上的天线 930 为收发器，用于读取要装到主机框架 910 中的耗材中的应答器（未示出）。此收发器只是读取存储在耗材中信息的一种形式的通讯部件的一个实施例。通讯部件的其他例子包括：电气触点，用于连通电路、红外或其他光传感器，以便与 LED 等元件通讯；机械开关，由例如机电装置或任何合适的装置设定，用于传递这样的信号。

在图 10A 和图 10B 中示出了适于实施本发明的一种形式的电路板。图 10A 是电路板的正视图而图 10B 是电路板的后视图。在此具体实施例中，插口 1015 设置在电路板上，用于接纳微处理器。如图 8 所示，通过存储在安全微处理器中，优选地，打印机的媒质鉴别程序对于潜在的盗版行为是隐藏的。

接着参考图 11，示出了用于安装在耗材上的通讯部件的一个可选实施例。提供用在耗材中的轴 1310。在一个实施例中，耗材可以是，例如，用在主机中的色带盒。在另一实施例中，耗材可以是，例如，用在照相机中的一卷胶卷。色带或媒质卷绕在轴 1310 上。凸缘 1320 可位于轴 1310 的一端，或位于与轴 1310 相连的任何传统位置。在图示的实施例中，位于凸缘上的同心圆形的导电带 1330 起到通讯部件的作用，从而将存储在耗材上的信息传递给主机。

接着参考图 12A-12D，示出了用在耗材中的一个零件的多个视图。图 12A 为卷绕轴 1405 的侧视图。提供卷绕鼓(winding drum) 1410，媒质可卷绕在该卷绕鼓上，例如用在打印机中的色带盒中的色带，或者用在照相机中的胶卷中的胶片。凸缘 1415 与卷绕鼓相连，并且能够，例如，连接到卷绕鼓的一端。也可以有其他的构造，并且将这些构造都视为等同物。通讯部件可以安装在凸缘上，用于与诸如打印机或照相机的主机进行通讯。

图 12B 为从与卷绕鼓 1410 上的凸缘 1415 相对的一端观察的端视图。在所示的该具体实施例中，卷绕鼓 1410 是空心的，具有形成空腔的内表面 1420。图 12C 为从安装有凸缘 1415 的一端观察的端视图。也能看出此具体实施例所具有的形成空心圆柱腔的内表面 1420。

现在参考图 12D，示出沿图 12A 中的线 A-A 截开的剖视图。心轴 1405 具有带有外表面 1425 的卷绕鼓 1410，诸如用于打印机的色带或用于相机的胶片能够缠绕在其上。此实施例中的内表面 1420 在空心的内部形成空腔。可利用一端上的凸缘 1415 以安装通讯部件，例如 RFID 应答器。在另一实施例中，第一通讯部件 1430，例如 RFID 应答器，可以安装在内表面 1420 上，其通过在轴的内壁形成的空腔内轴向放置的第二通讯部件（未示出）与主机通讯。

30

现在参考图 13，公开了一示意图，示出用于鉴别主机中耗材的
耗材鉴别系统。耗材 1500 可包括：例如，具有供给轴 1505、拾取轴
1510 以及支撑件 1515 的色带盒。耗材 1500 可包括通讯部件 1520、
5 1535，用于将信息传送给主机 1550。在一个实施例中，通讯部件 1520、
1535 可以是低成本的 RFID 应答器，其具有两种特性。首先，优选地，
该低成本的 RFID 应答器可包括厂家编入的唯一序列号 n (1530)，
用户无法将其改变，也无法通过将公共数据区 1525 复制到其他类似
型号的应答器中而将其复制。因此，每个应答器都是唯一编码的，这
正是大多数类型的具有“防冲突”协议的 RFID 应答器的一个要求，
10 能够区分所有的处于 RFID 读取器的天线场中的多个应答器。

第二，优选地，低成本 RFID 应答器具有这样的能力，能够将数
据值 x 和 y 一次性地写入(或写入并锁定)到应答器的公共数据区 1525
中。在此具体实施例中，值 y 为媒质类型信息，因为不是所有的媒质
15 类型都能够所有型号的打印机上工作。对于图示的情况来说，非零
数据值 x 将是 y 与该应答器的唯一标识号 n 的复杂函数。在这个示出
的例子中，值 x 将由厂家在制造媒质时编入应答器，或者至少是在其
离开制造商的库房前编入应答器。

20 在图中还示出了主机 1550，其包括通讯部件 1555、1560，用于
读取存储在耗材上的 n 、 x 、以及 y 的值。在步骤 1565 中能够受到存
储在耗材上的信息并能够用处理器能得到的授权函数 (1570)
 $F(M, Q, x, y)$ 来确定授权码 x 与序列号 n 以及媒质类型码 y 之间存在授
权关系。处理器 1565 可以远离主机且可以通过通讯信道 1590 与主机
25 通讯，例如通过网络或远程通讯联接。

优选地，耗材包括标志 1527，以便指出媒质部件的数目，例如
用在耗材上的色带板。每个色带卷芯或色带盒只能使用一次。应答器
中的其他存储元件记录媒质的使用情况，并保留媒质计数。在用完媒
30 质的每个单位部分(通常为 10-15%)时，应答器存储器中的标志被重

置并锁定。由于最多只有 15%的额外媒质能够重装到色带芯或色带盒上，所以这使得重复利用部分用过的色带芯或盒变得在经济上不具有吸引力。

5 仍然参考图 13，处理器 1565 可以得到曾用耗材的列表 1580。“曾用盒”列表保存在每个打印机中。之前的 512 个色带盒的序列号 n 以及它们的剩余条数计数存储在每个打印机中。如果一个色带盒再次出现且具有高于存储在打印机存储器中的剩余条数计数，则打印机能够
10 将该重装的色带盒或色带卷视为具有无效的授权，并且不仅拒绝使用该媒质，还能够将其应答器锁定到“完全耗尽”的状态，从而防止用过的媒质被再次填充。

实施上述方法和装置的过程包括 M^N 形式的重复运算，其中 M 和 N 都是大素数。当 M 和 N 都是大素数时，则 M^N 在理论上可以是几百
15 位数。为了更好地实施上述的授权算法，已经产生了一种方法，能够在小型微处理器中迅速估算出 M^N 并将位数限制为 Q 的长度的两倍。

举例来说，假设 $M \ll Q$ 且 Q 为 64 位数，因此所需要的只是进行
20 64 位乘 64 位的乘法。这个例子只是出于说明的目的，也可以有其他的实施例。

将 N 定义为 64 位的二进制数，它是 n 和 y 的某个函数：

$$N(n, y) = c_0 2^0 + c_1 2^1 + \dots + c_{63} 2^{63} = \sum_{i=0}^{63} c_i 2^i \quad \text{等式 1}$$

在此等式中，每个 c_i 都代表连续的二进制数位。将上式代入 M^N ，
25 得到：

$$M^N = M^{c_0 2^0 + c_1 2^1 + \dots + c_{63} 2^{63}} = M^{\sum_{i=0}^{63} c_i 2^i} \quad \text{等式 2}$$

$$M^N = \prod_{i=0}^{63} M^{c_i 2^i}$$

利用 M^N 的这种变形，可以采用以下定理估算等式 $M^N \bmod Q$ 的值：

$$(a \times b) \bmod c = [(a \bmod c) \times (b \bmod c)] \bmod c \quad \text{等式 3}$$

应用此定理，得到：

$$M^N \bmod Q = \left(\prod_{i=0}^{63} (M^{c_i 2^i}) \bmod Q \right) \bmod Q \quad \text{等式 4}$$

令

$$T_i = (M^{c_i 2^i}) \bmod Q \quad \text{等式 5}$$

5 则

$$M^N \bmod Q = \left(\prod_{i=0}^{63} T_i \right) \bmod Q \quad \text{等式 6}$$

现在利用每个 c_i 都等于 0 或 1 这一事实，可对每一项 T_i 进行估算。

$$\text{如果 } c_i = 0 \text{ 则 } T_i = M^{c_i 2^i} \bmod Q = M^0 \bmod Q = 1 \quad \text{等式 7}$$

$$\text{如果 } c_i = 1 \text{ 则 } T_i = M^{c_i 2^i} \bmod Q = M^{2^i} \bmod Q$$

10 $c_i = 1$ 时， T_i 的值最大不超过 64，可以将这些值预先算出并存储在数据表中，或者也可以继而进行估算。对 T_i 采用该数据表或这些计算出的值，则可以将 $M^N \bmod Q$ 的值逐步算出。令 P_i 为每一阶段的部分乘积， i 从 1 到 63。以递归的逐对方式进行计算：

$$\begin{aligned} P_1 &= (T_0 \times T_1) \bmod Q \\ P_2 &= (P_1 \times T_2) \bmod Q \\ &\vdots \\ P_i &= (P_{i-1} \times T_i) \bmod Q \end{aligned} \quad \text{等式 8}$$

15 直到

$$M^N \bmod Q = P_{63} = (P_{62} \times T_{63}) \bmod Q \quad \text{等式 9}$$

利用当 $c_i = 0$ 时则 $T_i = 1$ 这样一个事实，将 64x64 位乘法运算的数量平均减少了 50%。但是，为了实施此处所述的安全系统，还需要快速进行 64 位数对 Q 取模的 128 位运算。

20

对于以上的每一步，当 $c_i = 1$ 时，必须进行形如 $(W \bmod Q)$ 的简化。通常，这由整数长除运算来完成，从而得到整数余数。在此处的例子中，除数 Q 为 64 位数，而被除数 W 为 128 位数，必须进行大量的移位和减法运算。

25

为了更好地实施此处所述的安全系统，已经开发出了一种比长除快大约 20 倍的方法。设将 Q 选择为

$$Q = 2^n - k, \text{ 其中 } k \ll 2^n \quad \text{等式 10}$$

这包括了呈 $2^n - 1$ 形式的莫尚 (Mersenne) 素数。但是，如果能够准确地估计 $(W \text{ div } Q)$ 的值 (即，该除法运算的整数商)，则可容易地通过下式找到余数：

$$W \bmod Q = W - Q \times (W \text{ div } Q) \quad \text{等式 11}$$

可以用下式估计该除法运算的整数商。首先，写出等价的形式

$$W \text{ div } Q = \text{int} \left(\frac{W}{2^n - k} \right) \quad \text{等式 12}$$

将右侧的分子和分母都乘以 2^{-n} ，得到

$$W \text{ div } Q = \text{int} \frac{2^{-n} W}{1 - 2^{-n} k} \quad \text{等式 13}$$

因为 Q 通常较大 (此处为 $n \sim 63$ 位数)，所以 $(2^{-n} k) \ll 1$ 并且可用无穷级数将等式 13 中的分母展开

$$\frac{1}{1-u} = \sum_{i=0}^{\infty} u^i \quad \text{等式 14}$$

将等式 14 代入等式 13，得到：

$$W \text{ div } Q = \text{int} \left(2^{-n} W \sum_{i=0}^{\infty} (2^{-n} k)^i \right) \quad \text{等式 15}$$

估算等式 15 的前几项，发现

$$W \text{ div } Q \approx \text{int} (2^{-n} W + 2^{-2n} k W + 2^{-3n} k^2 W + \dots) \quad \text{等式 16}$$

已知 n 、 k 、以及 W 的最大值，则能够估算等式 16 的各项，直到得到足够小 (例如小于 $\frac{1}{2}$) 的第一项，使得后面各项不会影响整数部分，因为所有的后项都更小。此时，可将这些不影响整数部分值的各项在等式 16 的估算中安全地省略。

实际上，可以选择 W 、 Q 和 k ，使得等式 16 在仅仅几项之后就收敛。在实际操作中已经证明，这种计算 $W \bmod Q$ 的方法比直接通过长除求值要快很多倍。

作为可选实施例的一个例子，耗材和主机可通过光耦合进行通讯。其他的例子包括电触点以及磁读写头。此说明书中所列举的耗材

与主机之间的通讯的任何具体的示例形式对本发明都不构成限制，并且，所附的权利要求意在含盖任何合适的通讯方式。

5 尽管本发明在说明时是按照实施为热转印打印机形式的媒质处理系统的优选方案说明的，但本发明对于下列主机都具有相同的可实施性：如美国专利 5,266,968 和 5,455,617 中所述的热打印机（thermal printer）、如美国专利 6,106,166,所述的图像处理装置、如美国专利 6,173,119 所述的照相机、如美国专利 5,428,659,所述的 X 光相机、以及喷墨打印机、激光打印机等等。尽管本发明以实施为媒质处理系统
10 的形式进行说明，且其中媒质组件与媒质处理系统之间进行无线通讯，但本发明也可以容易地用在媒质组件与媒质处理系统通过有线连接通讯的系统中，如美国专利 5,266,968 和 5,455,617 所示。

15 出于对本发明的制造和使用方式进行说明的目的，在以上已经说明了本方法和装置的具体实施例。应该理解，本发明的其他变化和修改的实施方案以及本发明的各个方面对于本领域的技术人员来说是清楚的，且本发明并不局限于所述的具体实施例。因此，本发明意图含盖任何的和所有的处于在此公开并要求保护的基本原则的要旨和范围
20 之内的修改、变化或等价方案。

20

图1A

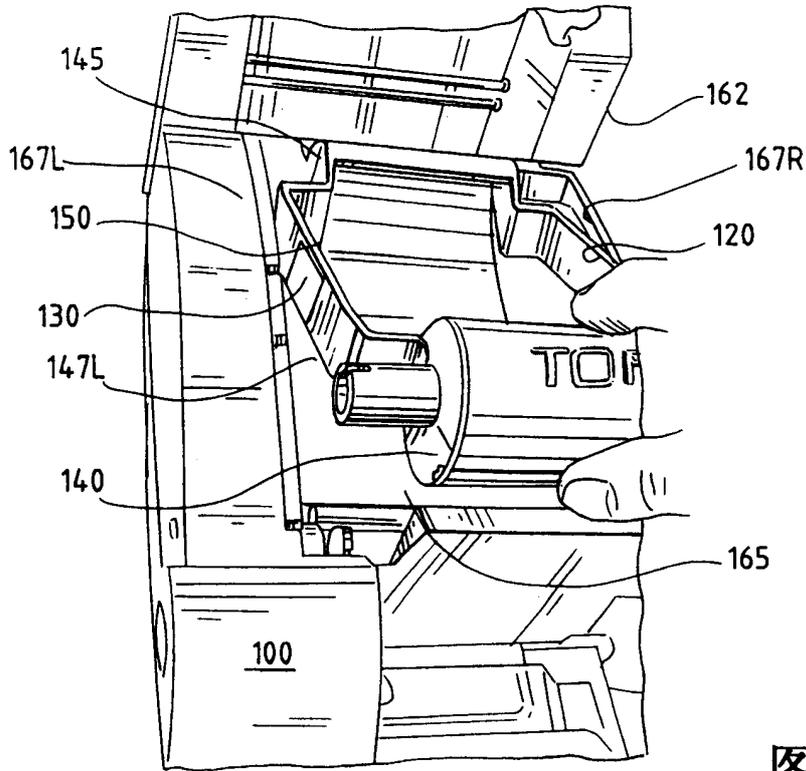


图1B

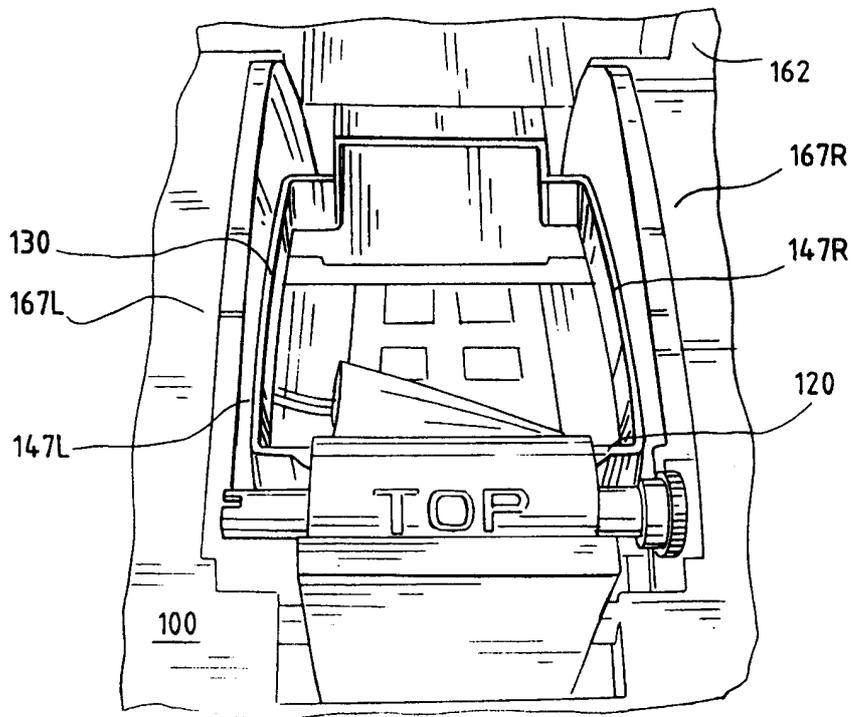


图2A

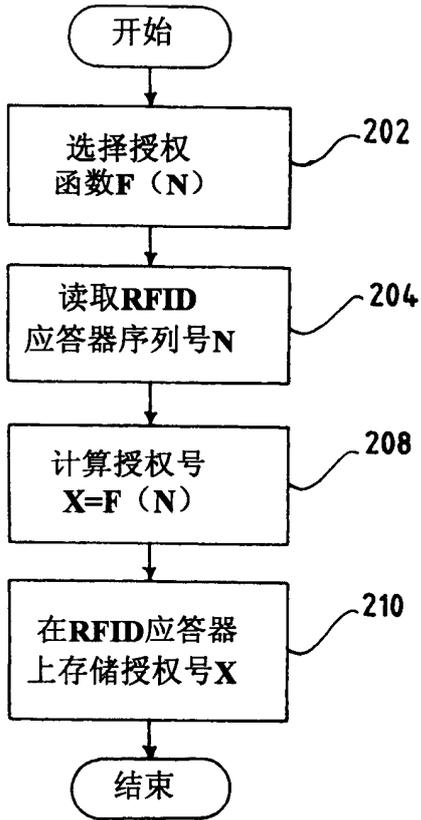


图2B

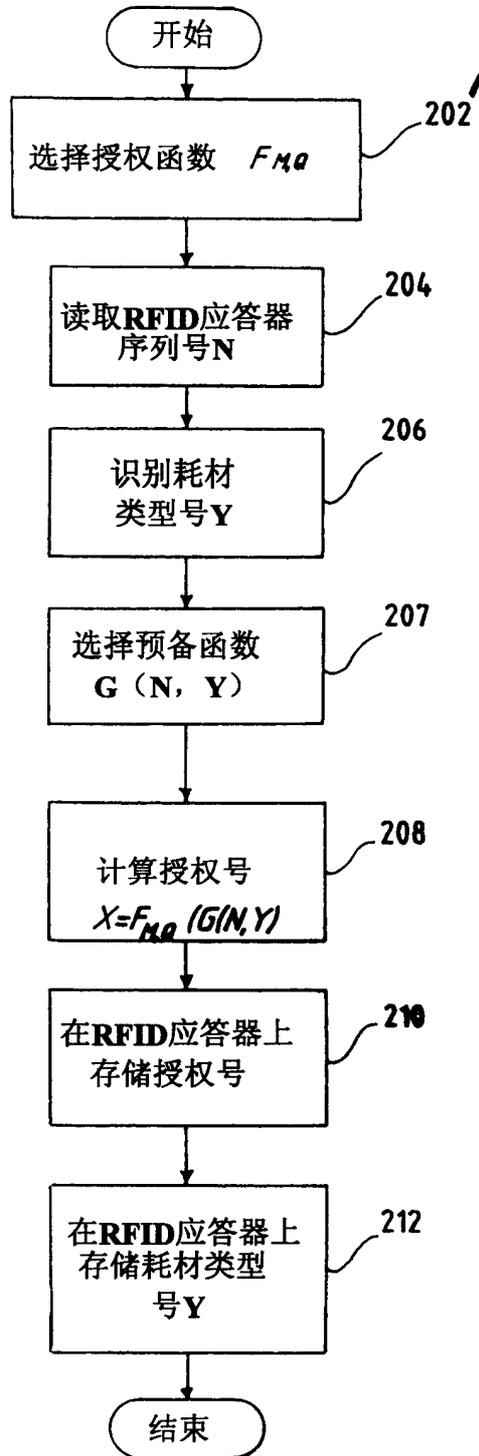
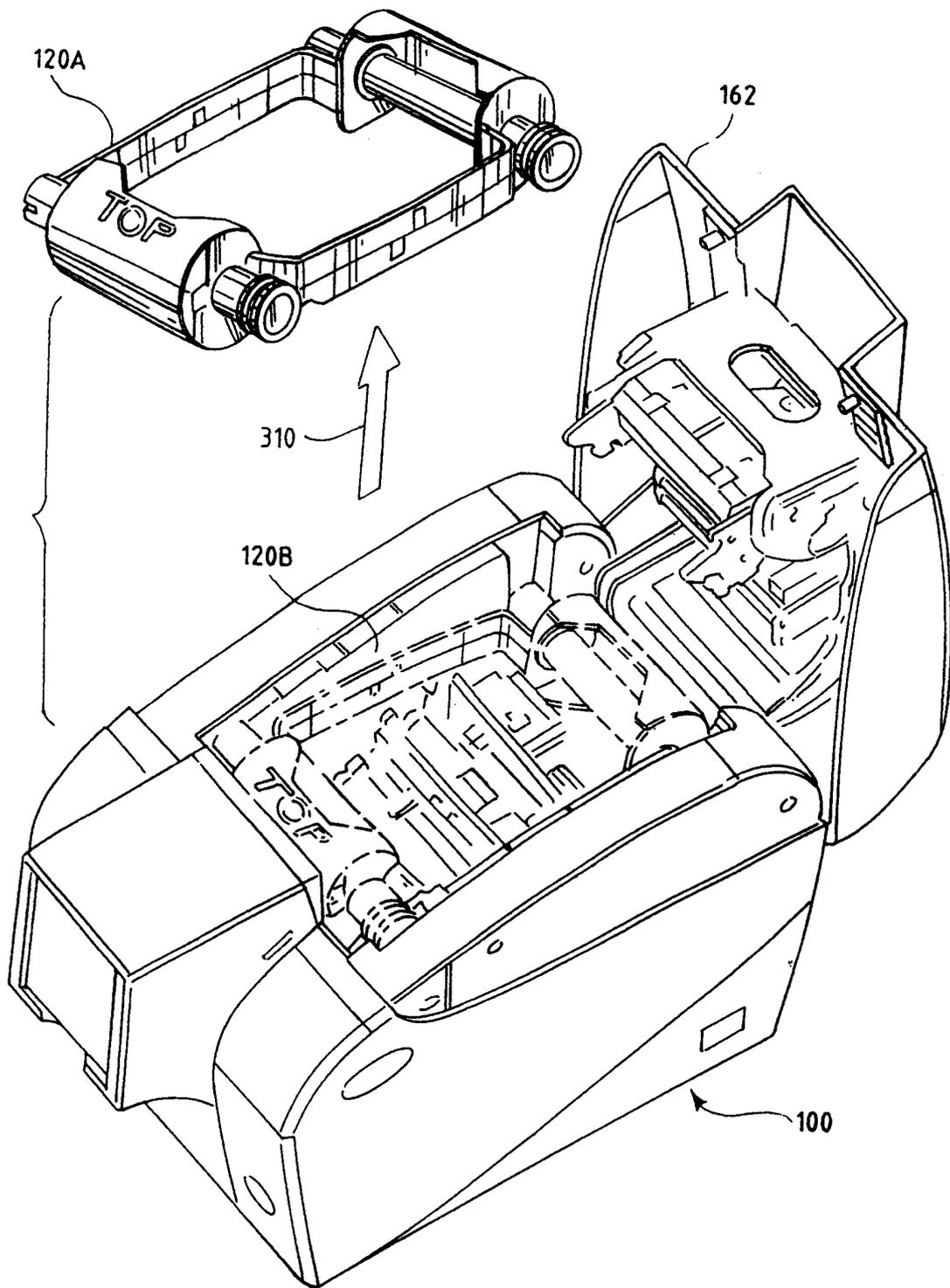


图3A



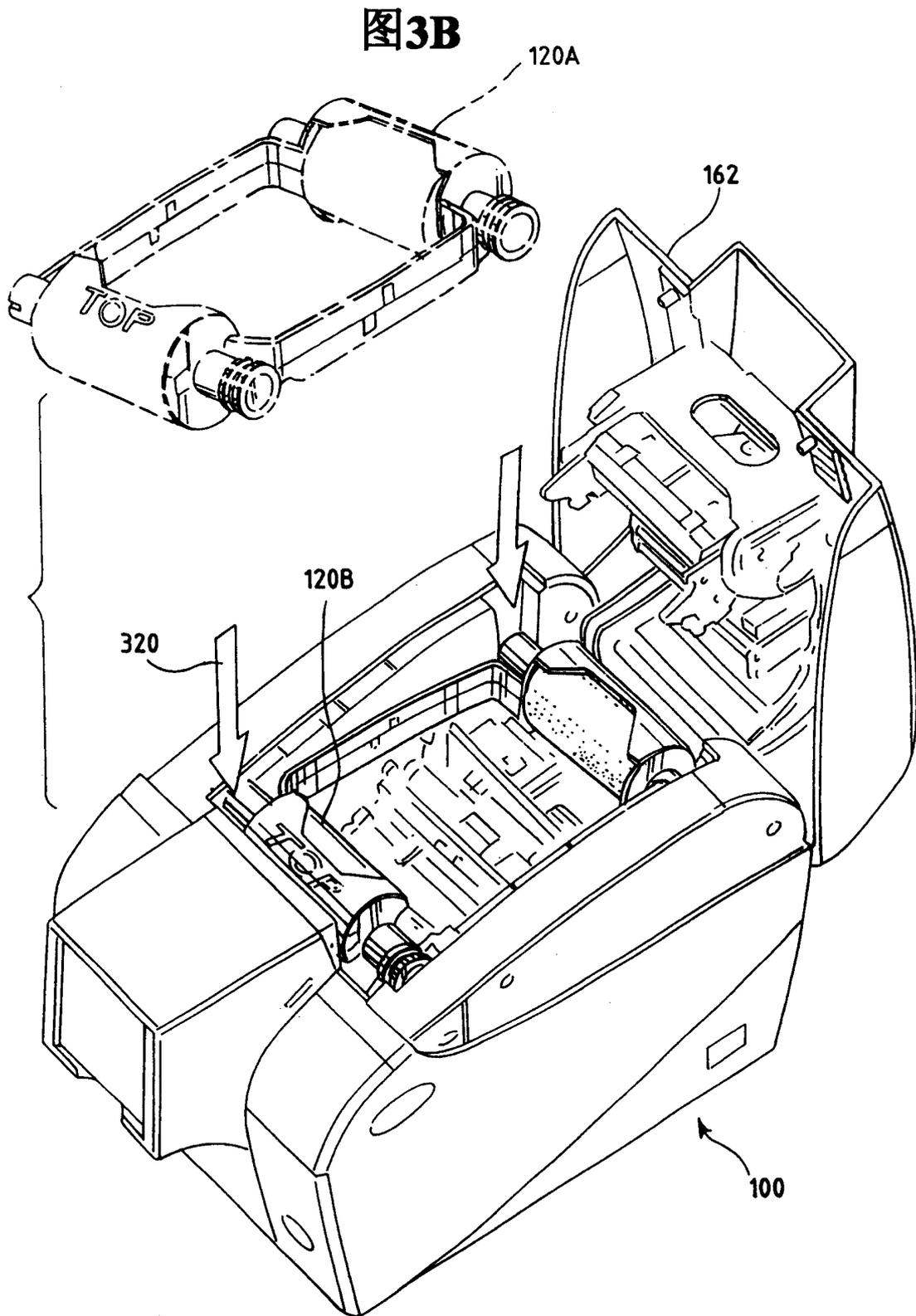


图4

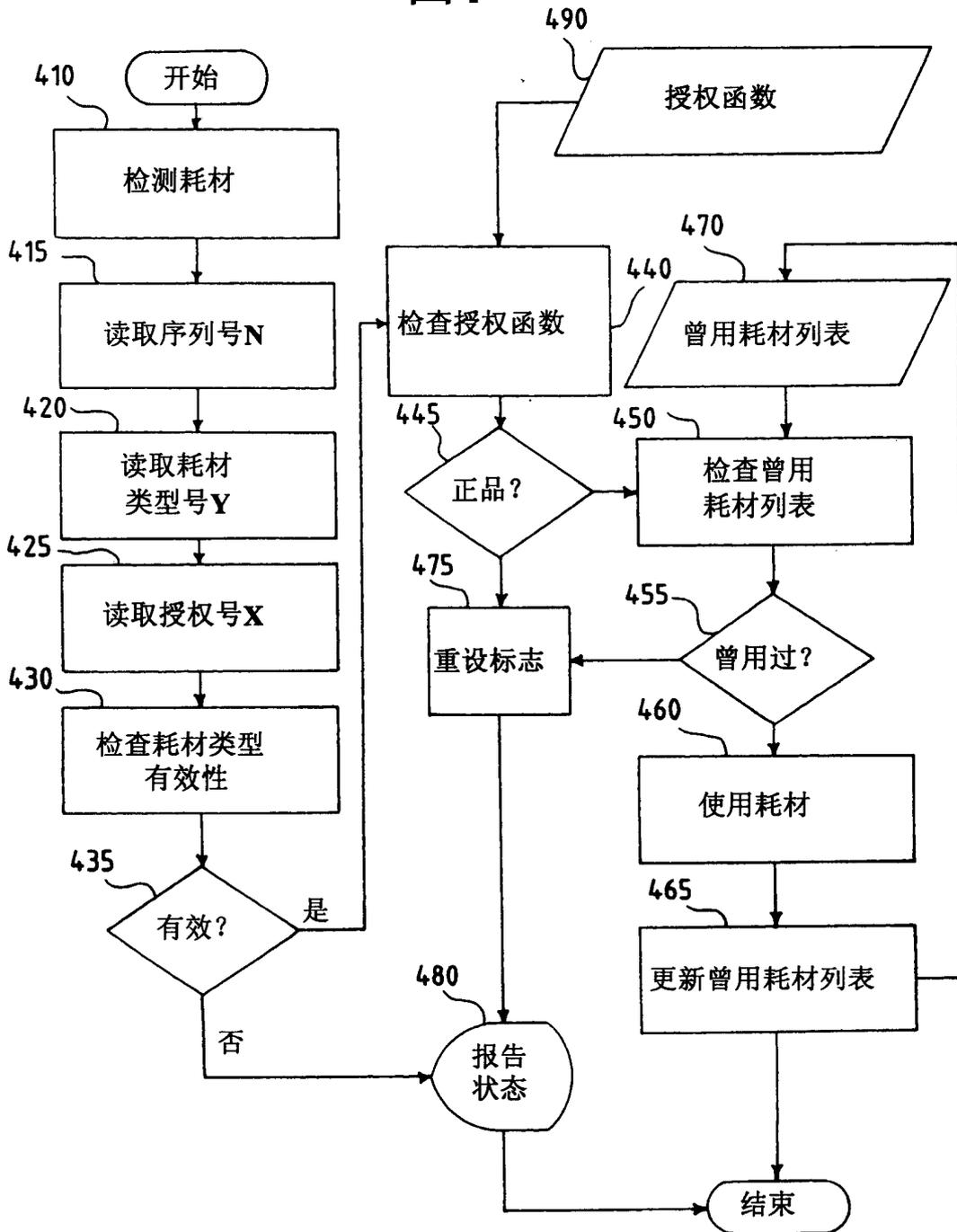


图5

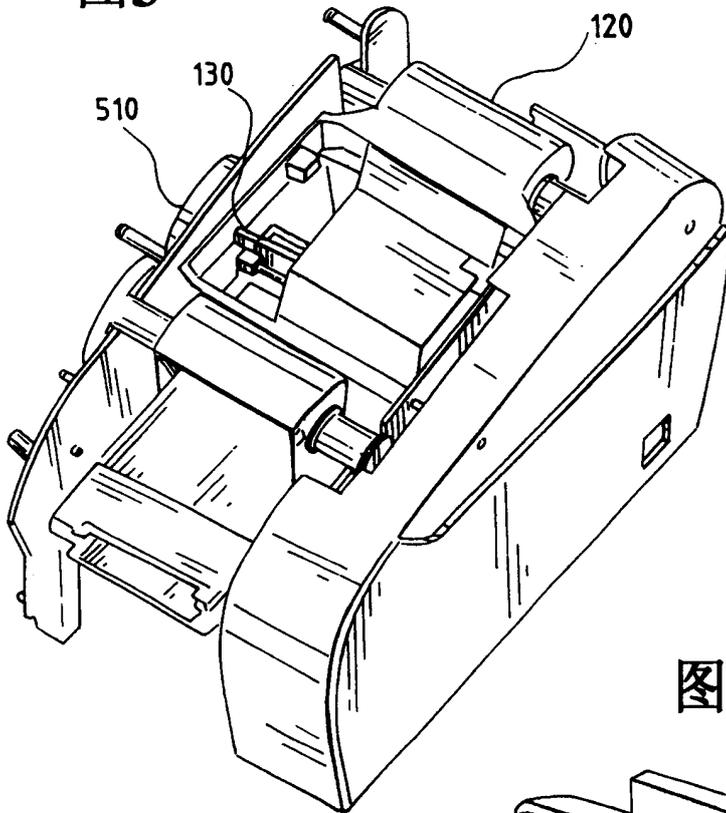


图6

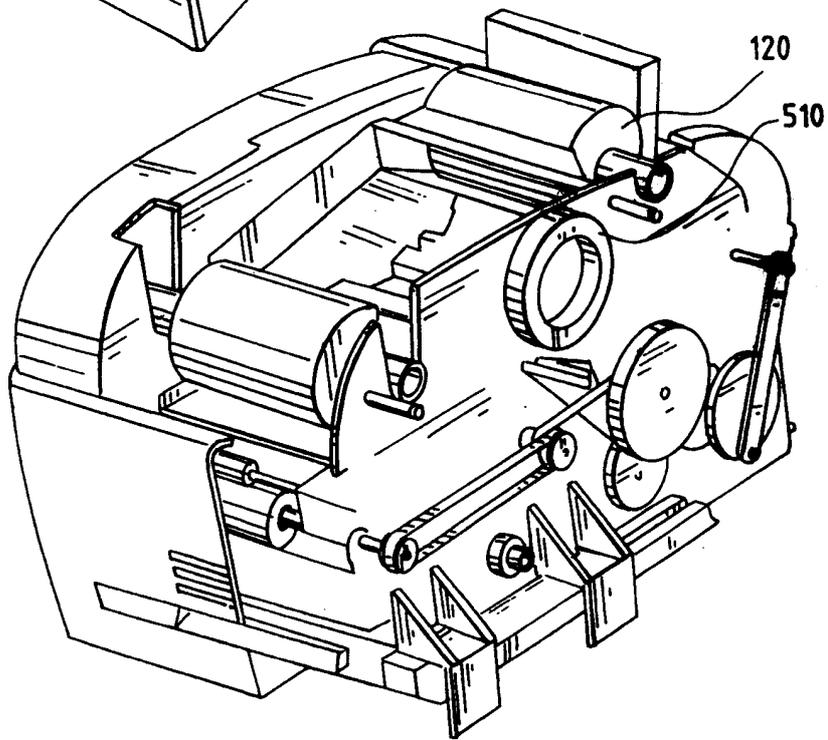


图7A

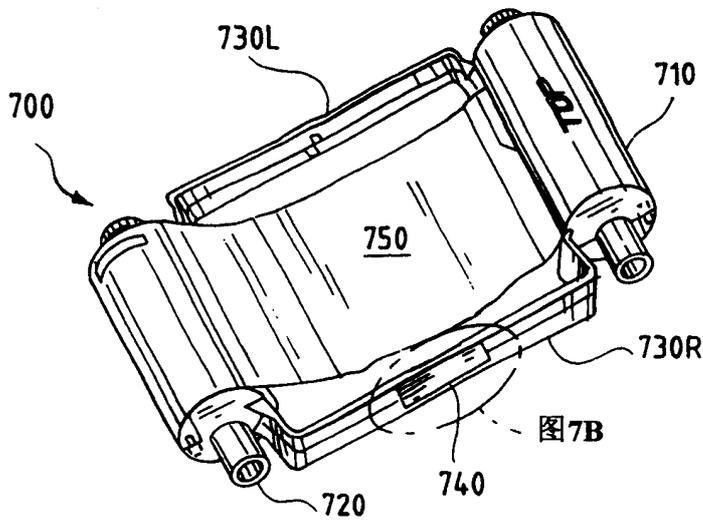


图7B

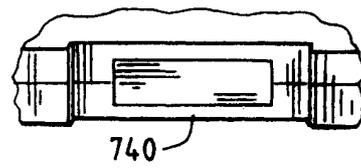


图7C

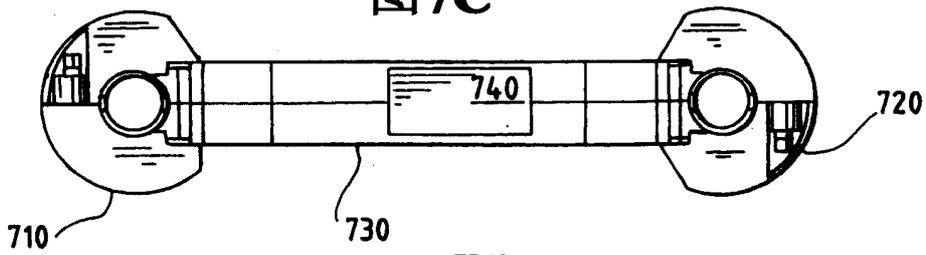


图7D

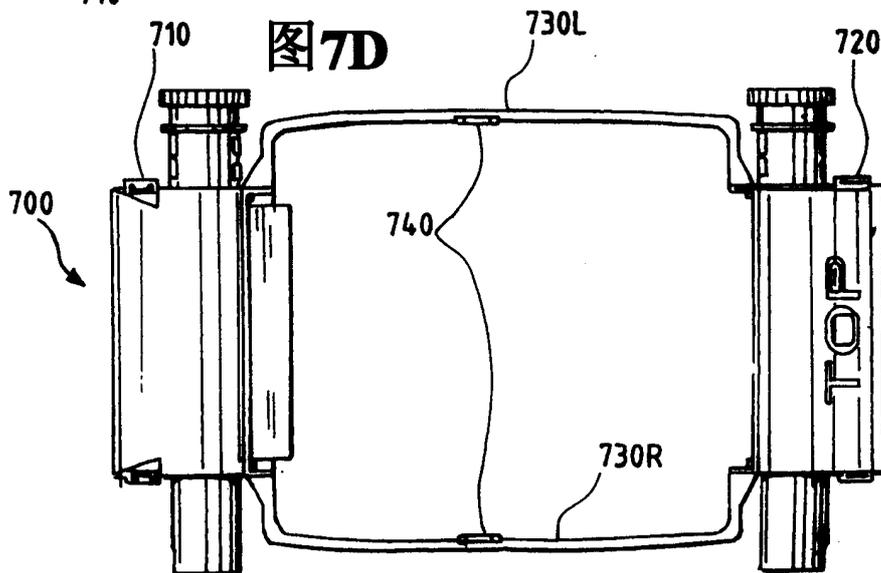


图8

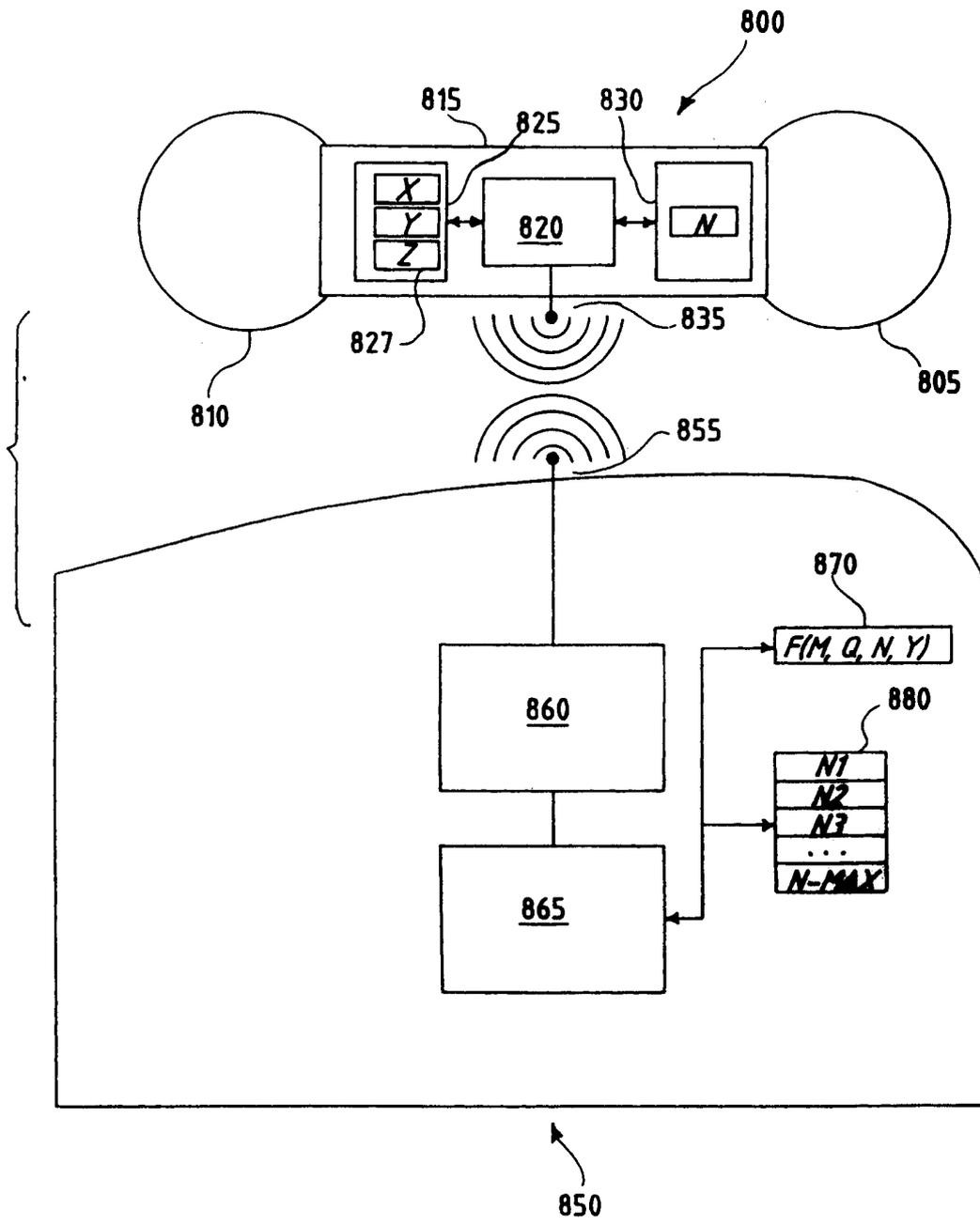


图9

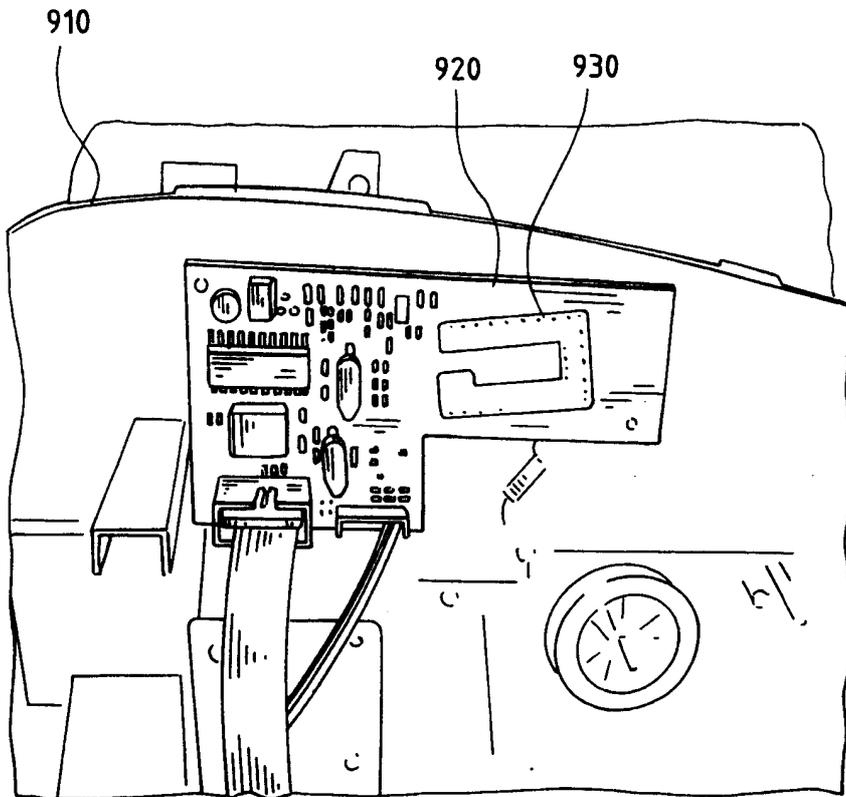


图10A

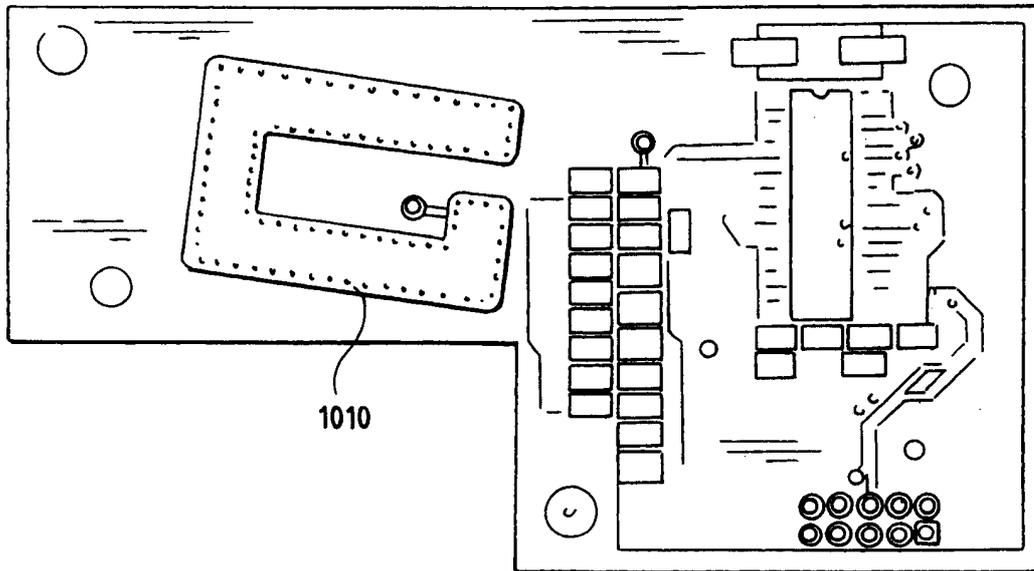


图10B

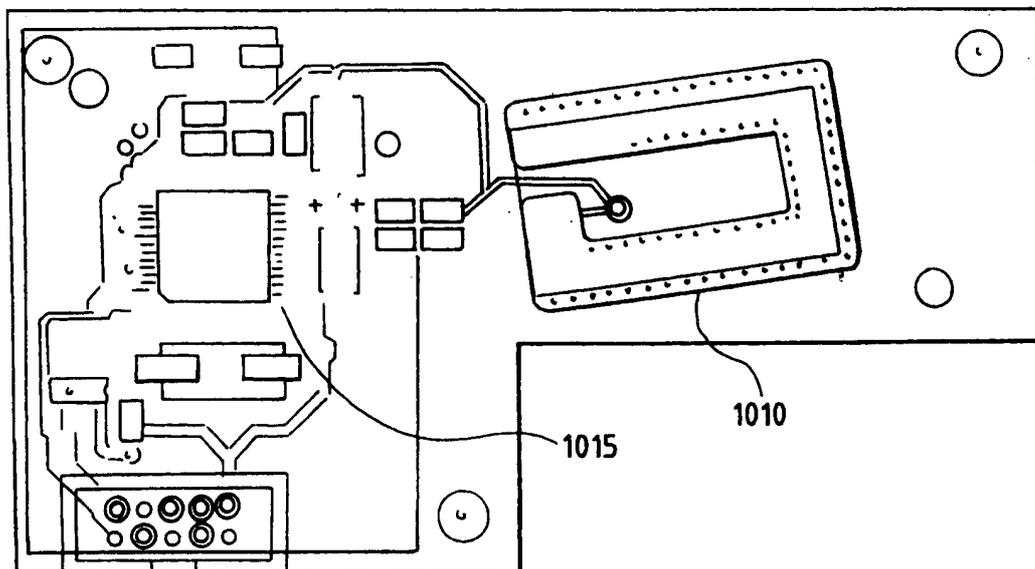


图11

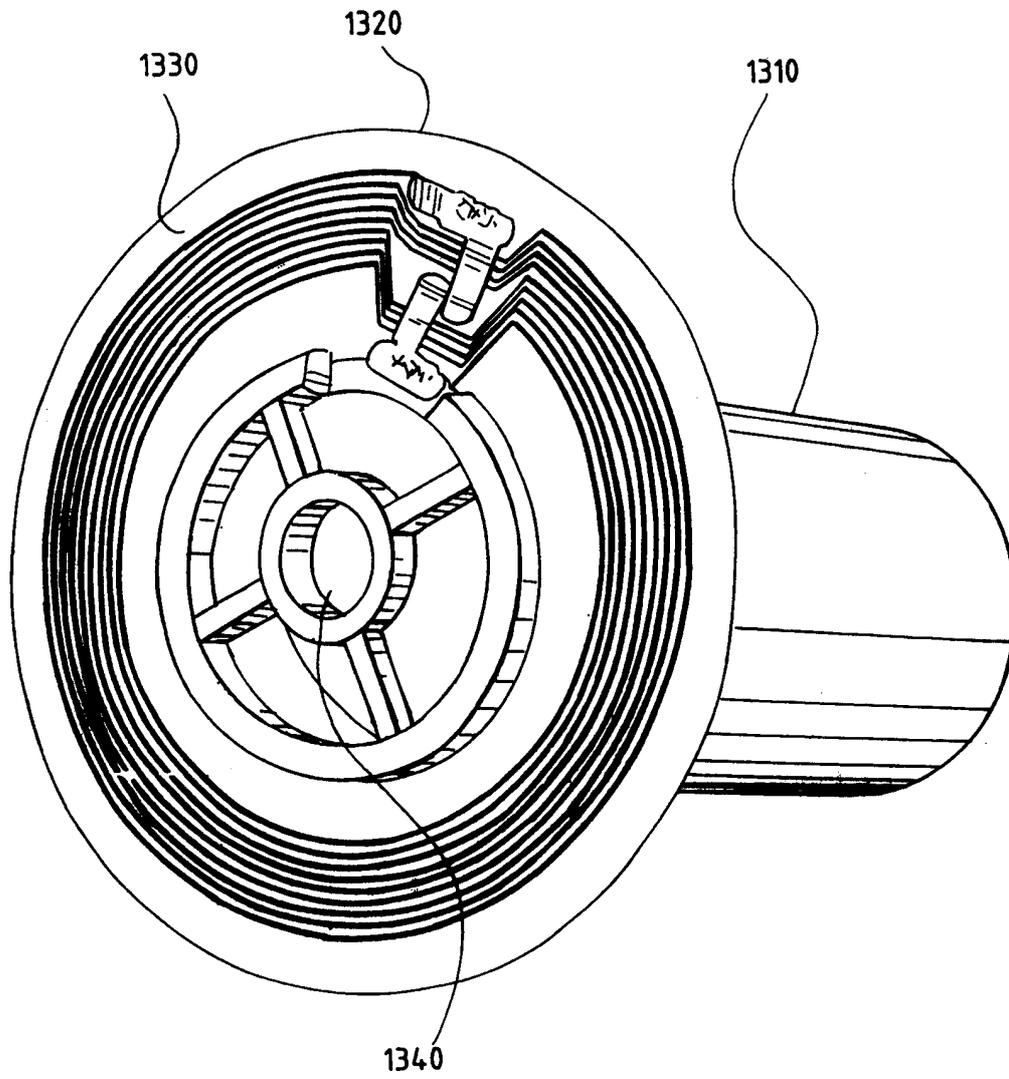


图12A

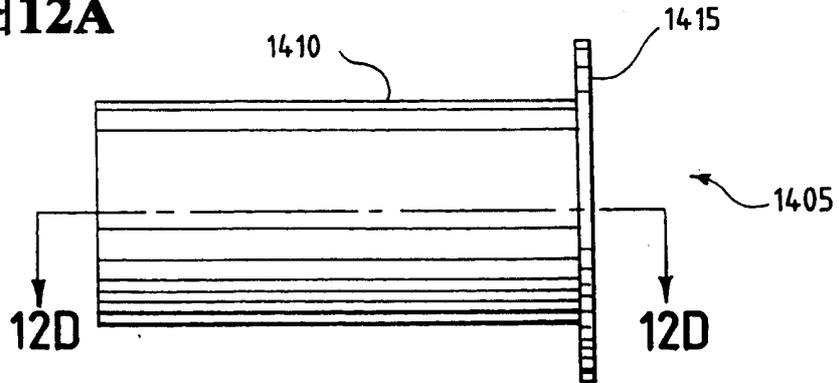


图12B

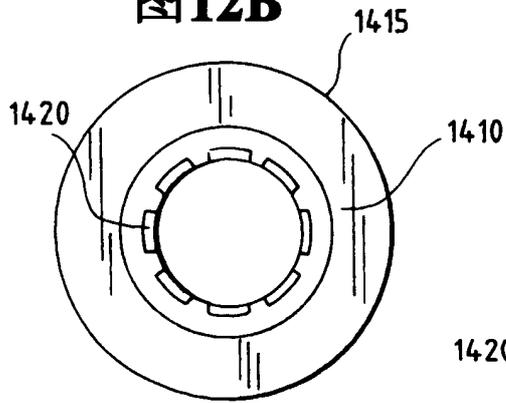


图12C

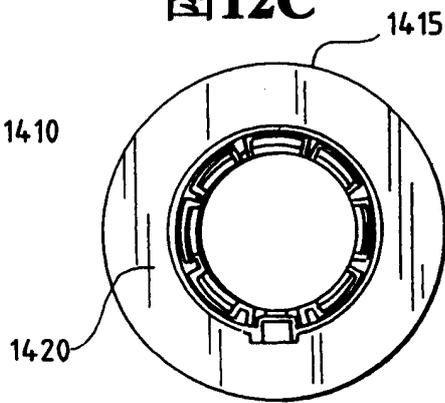


图12D

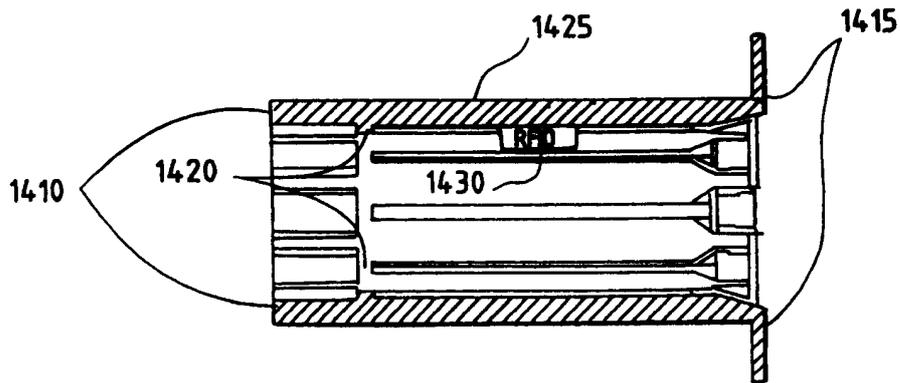


图13

