[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
G06K 7/00
G11B 5/09

[12] 发明专利申请公开说明书

[21] 申请号 03120421.X

[43] 公开日 2003 年 10 月 22 日

[11] 公开号 CN 1450486A

[22] 申请日 2003.3.13 [21] 申请号 03120421.X

[30] 优先权

[32] 2002.4.11 [33] JP [31] 109052/2002

[71] 申请人 CIS 电子工业有限公司

地址 巴西圣保罗

[72] 发明人 伊豆山康夫

[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

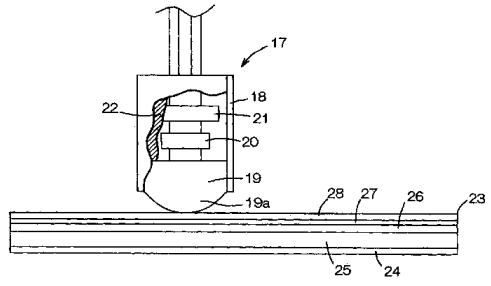
代理人 郭思宇

权利要求书 1 页 说明书 9 页 附图 7 页

[54] 发明名称 磁阅读器的磁头

[57] 摘要

本发明目的是提供一种用于磁阅读器的改进的磁头，从而可在高安全下从磁存储介质读出数据，即，不必忧虑数据可能会被非法读出，并且即使数据被非法读出，非法人员也不能利用这种非法读出的数据。 所公开的适用于读出磁卡 23 上存储的数据的磁卡阅读器的磁头 17 包括一个用于感测磁卡 23 上按模拟信号存储的数据的带有一个线圈的磁心，一个适用于把模拟信号转换成对应数字信号的模数转换器芯片 20，以及一个适用于加密数字信号的微处理器 21。 利用合成树脂 22 把模数转换器芯片 20 和微处理器 21(集成电路)固定在外壳 18 内。



ISSN1008-4274

1.一种适用于从利用磁性材料存储预定数据的磁存储介质读出所述预定数据的磁阅读器磁头，所述磁头包括：

一个适用于按模拟信号感测所述存储介质上存储的所述数据的带有一个线圈的磁心，一个电气上和所述线圈连接并适用于把所述模拟信号转换成对应数字信号的模数转换器芯片，以及一个电气上和所述模数转换器芯片连接并适用于加密所述数字信号的集成电路。

2.根据权利要求 1 的磁头，其中所述磁头还包括一个定义所述磁头的外周边表面的并在其中含有所述磁心、所述模数转换器芯片和所述集成电路的外壳。

3.根据权利要求 2 的磁头，其中利用合成树脂把所述模数转换器芯片和所述集成电路固定在所述外壳内。

4.根据权利要求 1 的磁头，其中所述磁阅读器包括一个适用于解密已由所述集成电路加密的所述数字信号的节点终端并且所述节点终端电气上和所述磁头的所述集成电路连接。

5.根据权利要求 1 的磁头，其中所述集成电路是从包括微处理器、门阵列、现场可编程门阵列和专用硬件的组中选择的。

6.根据权利要求 1 的磁头，其中所述磁存储介质是磁卡并且所述磁阅读器是磁卡阅读器。

磁阅读器的磁头

技术领域

本发明涉及磁阅读器中使用的磁头。

背景技术

适用于读出存储在磁存储介质上的数据的磁阅读器的磁头是周知的。下面参照图7说明用于磁卡阅读器70的常规磁头的一个例子，磁卡阅读器70借助和磁卡71的穿过磁卡阅读器70的引导槽(未示出)的表面相接触的磁头72从磁卡71的磁条读出数据。磁卡阅读器70包括磁头72，经接口电缆73和磁头72连接的模数转换器74以及经接口电缆75和模数转换器74连接的控制单元76。

磁头72具有一个磁心和缠绕在该磁心上的一个线圈。控制单元76是一个计算机，其具有CPU、存储器、硬盘、光盘机和软盘机。尽管没有示出，显示器(显示部件)、键盘(输入部件)以及打印机(输出部件)通过接口电缆和控制单元76连接。

当带有磁条的磁卡71沿着磁头72的末梢(磁心间隙)穿过磁卡阅读器70的引导槽时，磁心周围的磁通改变并且产生感应的电动力从而电流流过磁心以抵消磁通的变化。该电流经接口电缆73从磁心流过模数转换器74并且由该模数转换器作为模拟信号检测。模数转换器74把从磁头72输入的模拟信号转换成对应的数字信号。数字信号经接口电缆75从模数转换器74输出到控制单元76。控制单元76放大该数字信号并且通过显示器和/或打印机分别以字符数据或打印数据输出数字信号。另外，控制单元76按数字信号的形式把数据存储在它的存储器里。

磁卡阅读器通常分类为手动地沿着引导槽移动磁卡的手动送入型阅读器以及通过驱动带或驱动滚轮移动从卡入口中插入的磁卡的电机驱动插入型阅读器。

在图 7 中所示的磁卡阅读器 70，如果任何部件和接口电缆 73、75 连接，有可能非法地通过电缆 73 读出经过磁头 72 的模拟信号或者通过电缆 75 读出经模数转换器 74 转换的数字信号。还有可能通过电缆 73、75 非法地读出存储器中存储的数据。鉴于磁卡上的记录方法，磁卡上写入和从磁卡读出数据都是相对容易的。因此，利用非法读出的以模拟或数字信号为形式的数据容易复制磁卡。

发明内容

本发明的目的是为磁阅读器提供一种改进的磁读写器的磁头，从而使他人难以在从磁存储介质读出数据的过程中非法地读出数据并且加密该数据以便即使该数据被非法读出他人也不能使用该数据。

依据本发明，提供一种适用于从磁存储介质读出数据的磁阅读器磁头。

该磁头包括一个适用于感测在存储介质上以模拟信号的形式存储的数据的带有线圈的磁心，一个电气上和该线圈连接并适用于把模拟信号转换成相应的数字信号的模数转换器芯片，以及一个电气上和该模数转换器芯片连接并适用于加密数字信号的集成电路。

本发明包括以下实施例。该磁头还包括一个定义磁头的外周边表面的并在其中包含磁心、模数转换器芯片和集成电路的外壳。

通过合成树脂把模数转换器芯片和集成电路固定在该外壳内。

磁阅读器包括一个适用于解密由该集成电路加密的数字信号的并且电气上和磁头的集成电路连接的节点终端。

该集成电路是从包含微处理器、门阵列、现场可编程门阵列和专用硬件的一组中选择的。

磁存储介质是磁卡并且磁阅读器是磁卡阅读器。

附图说明

图 1 是示意示出磁卡阅读器的方块图；

图 2 示意示出卡读出台的内部结构；

图 3 是部分剖开的透视图，示出含在卡读出台内的磁头；

图 4 是一个流程图，示出在微处理器和数据控制台之间进行的加

密和解密顺序;

图 5 是示意示出磁卡阅读器的替代实施例的方块图;

图 6 是流程图，示出微处理器和主计算机之间进行的加密和解密顺序；以及

图 7 示意示出磁卡阅读器中使用的周知磁头。

具体实施方式

从以下参照各附图对磁卡阅读器中使用的磁头的说明会更完整地理解依据本发明的在磁阅读器中使用的磁头的细节。

图 1 是示意示出磁卡阅读器 1 的方块图，图 2 示意示出卡读出台 2 的内部结构，而图 3 是示出包含在卡读出台 2 中的磁头 17 的部分剖开的透视图。在图 3 中，磁头 17 的磁心 19 使它的梢端 19a 和磁卡 23 的上表面接触。图 3 通过部分地剖开在外壳 18 中装填的合成树脂 22 示出外壳 18 的内部。

如从图 1 清楚那样，磁卡阅读器 1 包括适用于感测磁卡 23 的磁化层 26 上以电信号形式存储的数据的卡读出台 2 以及经接口电缆 3 和卡读出台 2 连接的数据控制台 4（终端节点）。数据控制台 4 是一个包括 CPU（中央处理器）、存储器（辅助存储器）、硬盘、光盘机和软盘机的计算机。适用于以字符信息的形式输出数据的显示器 5（显示部件）、适用于添加和/或改变数据的键盘 6（输入部件）以及适用于以打印信息的形式输出数据的打印机 6（输出部件）经接口电缆 7、8 和数据控制台 4 连接。

如可从图 2 中看出那样，卡读出台 2 为电机驱动插入型，并且具有位于它的正面的卡入口 9、位于它的背面的卡出口 10 以及从卡入口 9 延伸到卡出口 10 的卡引导轨 11。卡读出台 2 的纵向中部设有后面会更详细说明的磁头 17。在入口 9、出口 10 和磁头 17 附近，分别设置光敏器 12、13、14，以对沿着引导轨 11 移动的磁卡 23 进行位置检测。一旦把磁卡 23 插入到卡读出台 2 的入口 9 中，磁卡 23 被自动地沿着引导轨 11 移动并且从出口 10 弹出。

在卡读出台 2 中，组成磁头 17 的磁心 19（见图 3）的梢端 19a

对着引导轨 11。卡 23 在卡读出台 2 内设置的带 15 上沿着引导轨 11 移动。通过电机 16 的转动带 15 被驱动。

如图 3 中所看出，磁头 17 包括覆盖磁头的外周边表面的外壳 18，带有线圈（未示出）的磁头 19，电气上和该线圈连接的模数转换器芯片 20，以及电气上和模数转换器芯片 20 连接的微处理器 21（集成电路）。在磁头 17 中，磁心 19、模数转换器芯片 20 以及微处理器 21 包含在外壳 18 内。在磁头 17 内，磁心 19 的梢端 19a 从外壳 18 的下端向外暴露。尽管未示出，微处理器 21 包括算术单元、控制单元和高速缓存。

通过在外壳 18 内填充的合成树脂 22 整体地把模数转换器芯片 20 和微处理器 21 固定在外壳 18 的内部。至于合成树脂 22，最好采用适当的热固合成树脂。也有可能用热塑合成树脂代替热固合成树脂。

磁卡 23 包括彩色印刷层 24、基层 25、磁化层 26、屏蔽层 27 和印刷层 28，按这个顺序这些层叠加在磁卡 23 的下表面上。在磁卡 23 中，磁化层 26 由铁磁材料构成，而基层 25 由聚对苯二甲酸乙二酯制成。

当磁卡 23 经卡入口 9 插入卡读出台 2 时，光敏器 12 检测磁卡 23 并且向数据控制台 4 输出卡插入信号。一旦接收卡插入信号，数据控制台 4 向磁头 17 的微处理器 21 输出读该卡 23 上存储的数据的命令。

当磁卡 23 的磁化层 26 通过组成磁头 17 的磁心 19 的梢端 19a（即，磁心间隙）时，在磁心 19 周围磁通改变，于是产生电动力并且电流在线圈中流过。流过该线圈的电流的值取决于磁通的变化并且以模拟信号的形式输入到模数转换器芯片 20。该模数转换器芯片 20 把模拟信号转换成对应的数字信号。接着把该数字信号输入到和模数转换器芯片 20 连接的微处理器 21。微处理器 21 加密数字信号。然后加密后的数字信号从微处理器 21 输出到数据控制台 4。

如果光敏器 13、14 检测出磁卡 23 经过磁头 17 并且接着从卡出口 10 弹出，光敏器 13、14 分别向数据控制台 4 输出卡通过信号。响应这些卡通过信号，数据控制台 4 命令微处理器 21 停止读数据。

数据控制台 4 具有一个放大器（未示出）以放大数字信号并且解

密已由该放大器放大的数字信号。数据控制台 4 可以向显示器 5 或打印机 6 输出解密后的数字信号。数据控制台 4 在存储器中存储加密或解密的数字信号。数据控制台 4 包含高速缓存，从而还可以在高速缓存中存储加密或解密的数字信号。

图 4 是一个流程图，示出在数据控制台 4 和微处理器 21 之间进行的加密和解密顺序。在依据本发明的磁卡阅读器 1 中，采纳公钥密码系统（RSA 公钥密码系统）在数据控制台 4 和微处理器 21 之间加密和解密数据。

一旦接收来自光敏器 12 的卡插入信号，数据控制台 4 产生一个用于加密磁卡 23 上存储的数据的公钥 30 和一个用于解密已在该方式下加密的数据的私钥 31。

私钥 31 输入到 CPU 的密钥管理实用程序 32，在其中按预定方式对私钥 31 分配地址。接着把私钥 31 从密钥管理实用程序 32 输入到存储器的私钥文件 33 并且存储在其中。另一方面，把公钥 30 经接口电缆 3 从数据控制台 4 输入到微处理器 21 的密钥管理实用程序 34 并且在密钥管理实用程序 34 中按预定方式对公钥 30 分配地址。把公钥 30 从密钥管理实用程序 34 输入到微处理器 21 的高速缓存并且存储在该高速缓存的公钥文件 35 中。

一旦接收来自模数转换器芯片 20 的数字信号 36，微处理器 21 从公钥文件 35 取出公钥 30 并且利用该公钥 30 形成 RSA 算法 37。微处理器 21 根据该 RSA 算法 37 加密数字信号 36 并且经接口电缆 3 向数据控制台 4 输出加密后的数字信号 36。一旦接收来自微处理器 21 的加密数字信号 36，数据控制台 4 从存储器的私钥文件 33 取出私钥 31 并且利用该私钥 31 形成 RSA 算法 38。从私钥文件 33 取出的私钥 31 和已由微处理器 21 使用的加密数字信号 36 的公钥 30 相对应。数据控制台 4 根据 RSA 算法 38 解密加过密的数字信号 36，从而得到磁卡 23 上存储的数据 39。

在依据本发明的磁卡阅读器 1 中，模数转换器芯片 20 和微处理器 21 都包含在外壳 18 内，从而，在不拆开磁头 17 下，不可能把适应

于非法地读出以模拟或数字信号为形式的数据的部件连接到磁卡阅读器 1 上。因此，难以非法读出数据。在磁卡阅读器 1 中，磁头 17 含有适用于对磁卡 23 上存储的数据进行加密的微处理器 21。从而，即使非法读出磁卡 23 上存储的数据，在不解密加过密的数据下不能使用该数据。这样实际上不可能复制磁卡 23。

图 5 是示意示出磁卡阅读器的替代实施例 40 的方块图，而图 6 是示出在微处理器 21 和主计算机 43 进行的加密和解密的顺序。

磁卡阅读器 40 包括一个卡读出台 41。卡读出台 41 中含有和图 3 中相同的磁头 17，该磁头适用于把磁卡 23 上存储的数据转换成对应的数字信号并且加密该数字信号。磁卡阅读器 40 的卡读出台 41 的结构和图 2 中示出的结构相同，从而省略对它的详细说明。磁卡阅读器 40 通过接口电缆 42 外部连接到主计算机 43（节点终端）。

安装在卡读出台 41 上的磁头 17 包括外壳 18，带有线圈的磁心 19，模数转换器芯片 20 和微处理器 21（MPU）。磁头 17、磁心 19 和模数转换器芯片 20 包含在外壳 18 之内，其中利用合成树脂 22 把模数转换器芯片 20 和微处理器 21 整体地固定在外壳 18 内（见图 3）。

主计算机 43 是一个具有 CPU、存储器、硬盘、光盘机和软盘机的计算机。通过接口电缆 44、45，显示器 46（显示部件）、键盘 47（输入部件）和打印机（输出部件）和主计算机 43 连接。

在卡读出台 41 中，若光敏器 12 检测出磁头 23 经卡入口 9 插到卡读出台 41 中，光敏器 12 向主计算机 43 输出卡插入信号。一旦接收卡插入信号，主计算机 43 命令磁头 17 的微处理器 21 读卡 23 上存储的数据。

若光敏器 13、14 检测出磁卡 23 通过磁卡 17 并从卡出口弹出，光敏器 13、14 分别向主计算机 43 输出卡通过信号。响应这些卡通过信号，主计算机 43 命令微处理器 21 停止读数据。

该磁卡阅读器 40 采纳为公钥密码系统（RSA 密码系统）和公用钥(common key)密码系统（DES 密码系统）的组合的 MIX 密码系统在微处理器 21 和主计算机 43 之间加密和解密数据。

MIX密码系统是一种利用分别由RSA密码系统和DES密码系统提供的好处的加密系统。更具体地，在有利方面上基于DES算法的数据处理速率快到大约是基于RSA算法的数据处理速率的1/100，但在不足方面上DES算法难以安全地分发密钥并且要管理的密钥的数量大。RSA密码系统优点是不仅不必传送公钥并且要管理的密钥的数量远少于由DES密码系统管理的密钥的数量。从而MIX密码系统利用DES密码系统提供的高数据处理速率的优点并且利用RSA密码系统提供的简易密钥管理的优点。按照MIX密码系统，微处理器21根据DES算法58解密数据并且根据RSA算法56解密用来形成另一个DES算法64的公用钥57（DES钥）。

一旦接收来自光敏器12的卡插入信号（见图2），如图6中所示，主计算机43产生一个用于RSA算法的公钥50和一个用来解密加过密的公用钥57的私钥51。私钥51输入到CPU的密钥管理实用程序52并且由密钥管理实用程序52按预定方式分配地址。从密钥管理实用程序52把私钥51输入到存储器的私钥文件53并存储在其中。公钥50经接口电缆42从主计算机43输入到微处理器21的密钥管理实用程序54并且由密钥管理实用程序54分配地址。从密钥管理实用程序54把公钥50输入到高速缓存的公钥文件55并存储在其中。

一旦接收来自模数转换器芯片20的数字信号59，微处理器21从公钥文件55取出公钥50并且利用该公钥50形成RSA算法56。微处理器21生成用于DES算法58的公用钥57（DES钥）并且接着根据RSA算法56加密该公用钥57。微处理器21利用该公用钥57形成DES算法58并且根据DES算法58加密数字信号59。把公用钥57输入到密钥管理实用程序60并且由密钥管理实用程序60按预定方式分配地址。把公用钥57从密钥管理实用程序60输入到微处理器21的高速缓存中的公用钥文件61并存储在其中。微处理器21通过接口电缆42向主计算机43输出加过密的公用钥57以及加过密的数字信号59。

一旦接收来自微处理器21的加密公用钥57和加密数字信号59，主计算机43对加密公用钥57分配地址，接着在存储器的临时文件62

中存储公用钥 57，从存储器的私钥文件 53 取出私钥 51 并且利用该私钥 51 形成 RAS 算法 38。主计算机 43 根据 RSA 算法 63 解密加过密的公用钥 57。主计算机 43 利用解密的公用钥 57 形成 DES 算法 64。主计算机 43 根据 DES 算法 64 解密加过密的数字信号 59，从而得到磁卡 23 上存储的数据 65。

从私钥文件 53 取出的私钥 51 一方面对应于微处理器 21 用来加密公用钥 57 的公钥 50，并且对应于微处理器 21 用来加密数字信号 59 的公用钥 57。

主计算机 43 以字符数据的形式向显示器 46 输出解密的数字信号 59 并且以打印数据的形式向打印机 47 输出解密的数字信号 59。主计算机 43 在存储器中存储加密的数字信号 59 以及解密的数字信号 59。

利用该磁卡阅读器 40，除非拆开磁头 17，不能把任何适用于非法地读出模拟或数字信号形式下的数据的部件连接到其上。在该磁卡阅读器 40 的情况下，即使非法读出磁卡 23 上存储的数据，由于数据已被磁头 17 的微处理器 21 加密不能立即使用该数据。

公钥密码系统不受 RSA 密码系统的限制，而是可以采用 EPOC 密码系统、Rabin 密码算法、Diffie-Hellman ElGamal 密码系统和 Elliptic Curve Diffie-Hellman Elliptic Curve ElGamal 密码系统中的任一种。还可以只采用公用钥密码系统。在这种情况下，公用钥密码系统不限于 DES 密码系统，而是可以是 FEAL 密码系统、IDEA 密码系统、MISTY 密码系统、MULTI 密码系统和 RC2/4/5 密码系统中的任一种。

除了微处理器，磁头可包含门阵列、现场可编程门阵列或专用硬件。

卡读出台不受电机驱动插入型的限制，而是可以是手动送入型。接口电缆可以从包括 RS－232C 电缆、RS－422A 电缆和 RS－423A 电缆的组中选择。

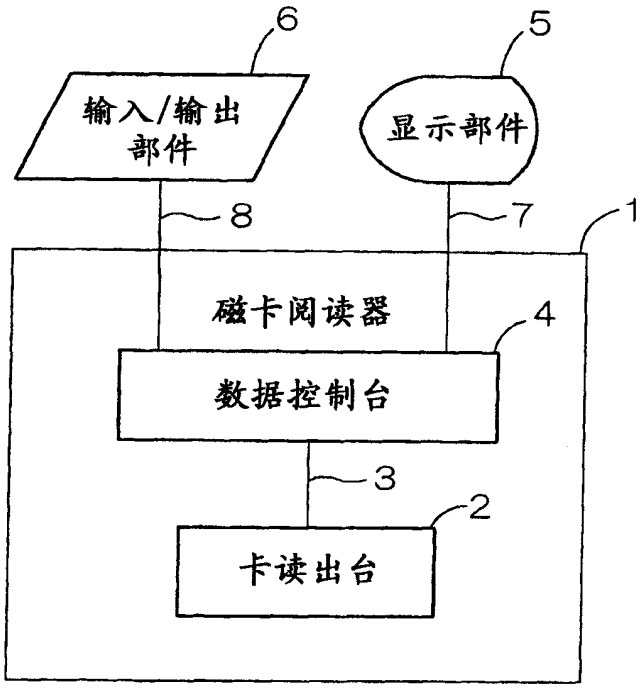
依据本发明的磁头还可以应用于用来读涂上磁墨水的文件夹的磁墨水字符阅读器。

依据本发明的磁头能加密从磁存储介质读出的数据，从而即使非法读出加密数据，除非解密该加密数据仍不能使用该加密数据。在这种方式下，可靠地防止复制该磁存储介质。

通过该在外壳内包含磁心、模数转换器芯片和微处理器的磁头实施例，除非磁头本身被拆开，不可能连接任何适用于在模数转换之前或之后非法读出数据的部件。同时鉴于该特性，几乎不可能非法读出数据。

通过该利用合成树脂把模数转换器芯片和微处理器固定在外壳内的磁头实施例，可以先去掉该合成树脂后拆开该磁头。但是，去掉合成树脂必然破坏模数转换器芯片和微处理器。这种特性进一步可靠防止连接任何适用于对模数转换器芯片和微处理器非法读出数据的部件的企图。

图1



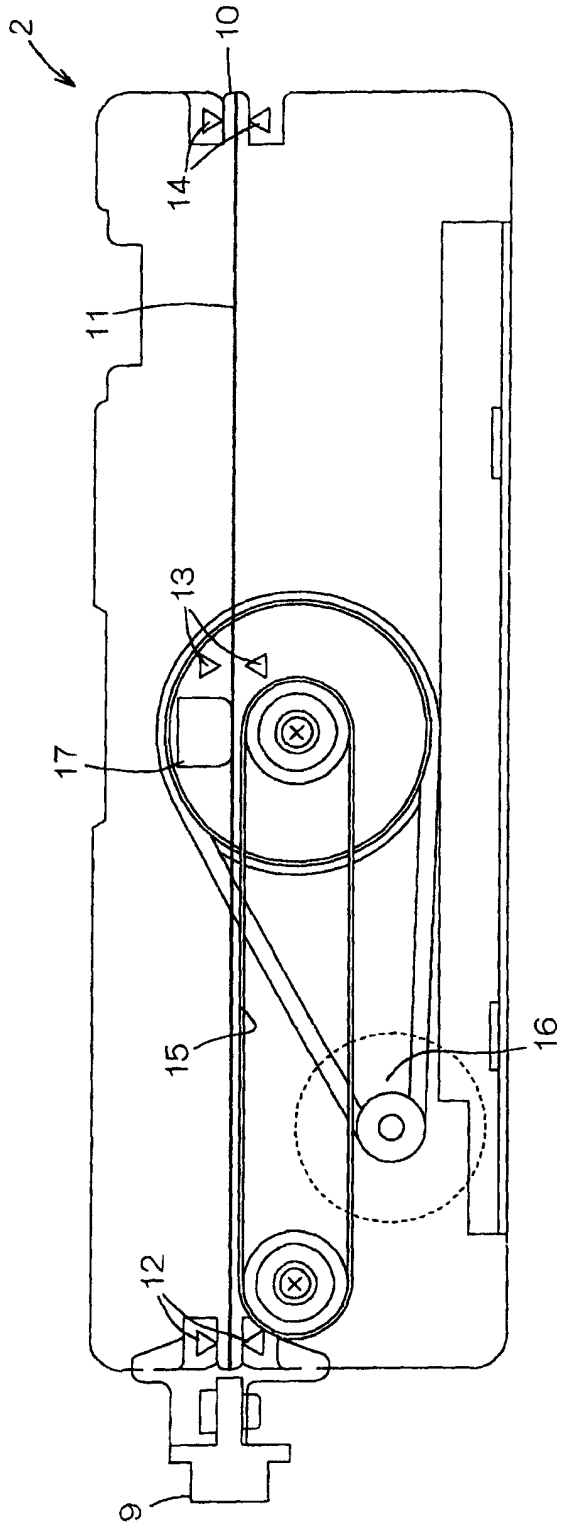


图 2

图 3

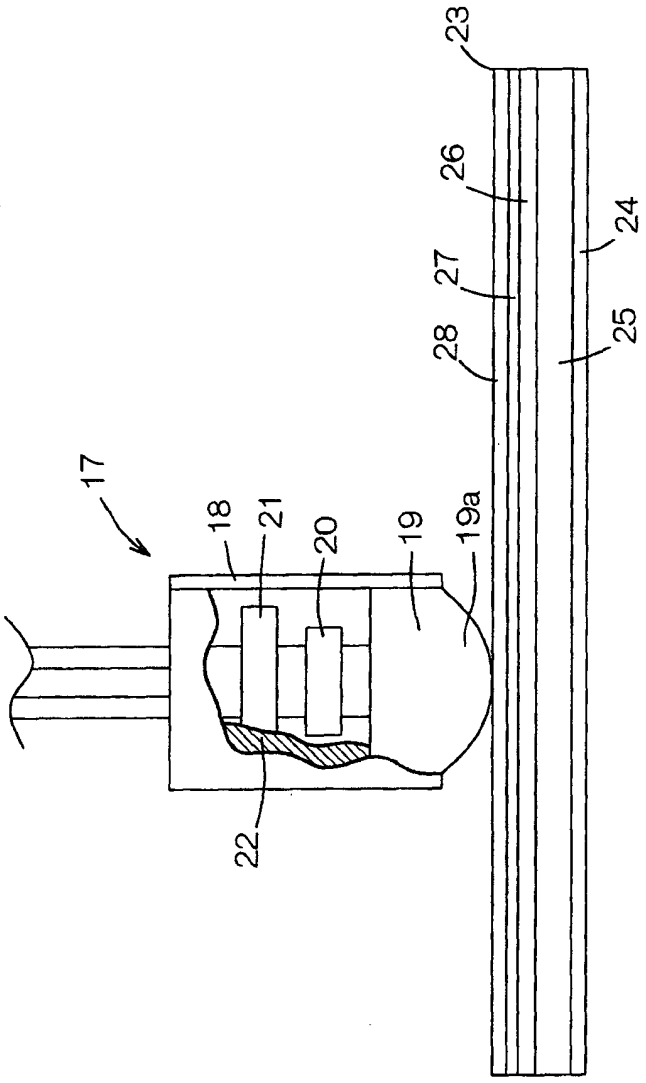


图4

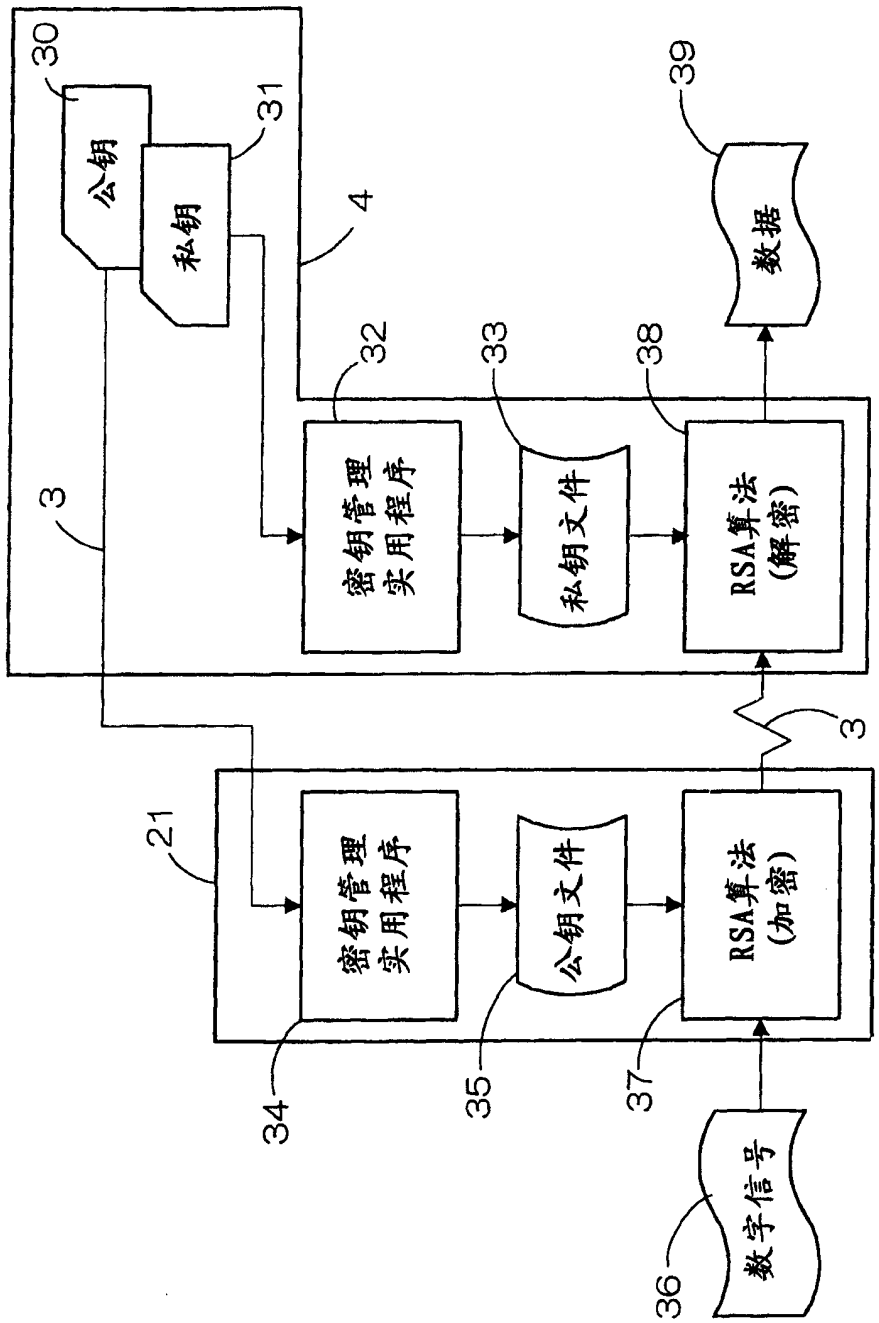

30
公钥
31
私钥
4
3
32
密钥管理
实用程序
33
私钥文件
38
RSA算法
(解密)
39
数据
3
21
密钥管理
实用程序
公钥文件
RSA算法
(加密)
34
35
37
36
数字信号

图5

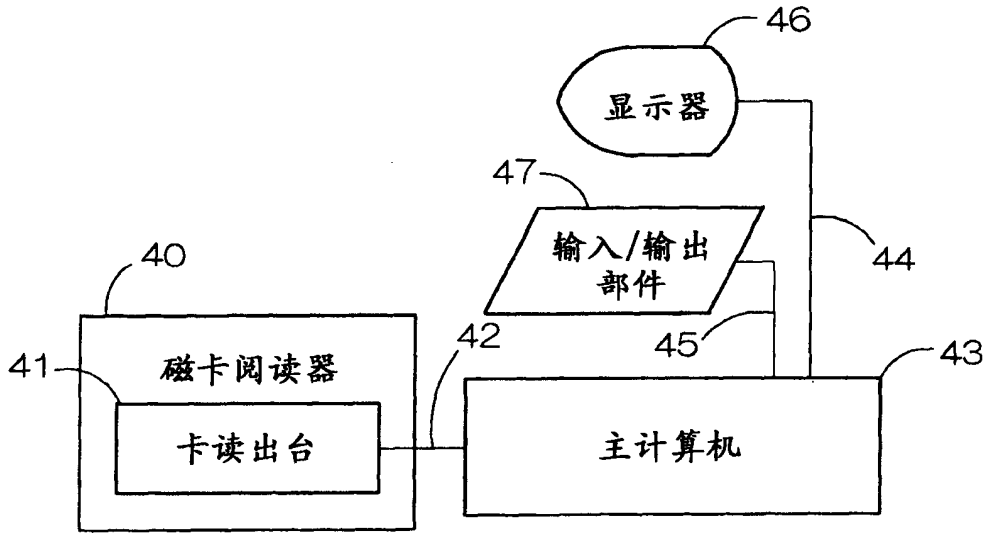


图6

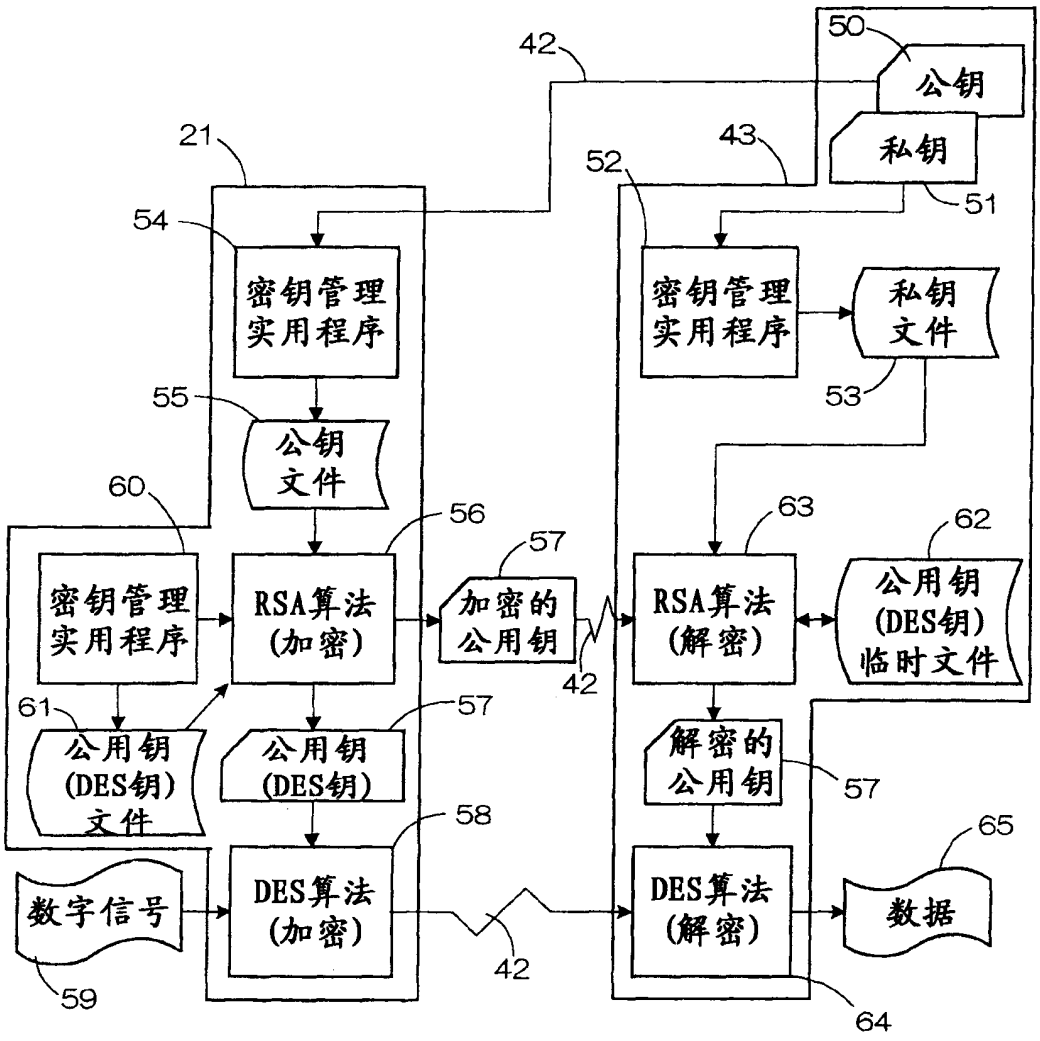

42
50
公钥
私钥
21
43
52
51
54
密钥管理
实用程序
密钥管理
实用程序
私钥
文件
55
53
公钥
文件
60
56
63
62
57
密钥管理
实用程序
RSA算法
(加密)
加密的
公用钥
RSA算法
(解密)
公用钥
(DES钥)
临时文件
42
61
57
公用钥
(DES钥)
文件
公用钥
(DES钥)
解密的
公用钥
57
58
65
数字信号
DES算法
(加密)
DES算法
(解密)
数据
42
59
64

图7