[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04B 5/00

[12] 发明专利说明书

[21] ZL 专利号 97120093.9

[43] 授权公告日 2003 年 6 月 4 日

[11] 授权公告号 CN 1110910C

[22] 申请日 1997.10.13 [21] 申请号 97120093.9

[30] 优先权

[32] 1996.11.14 [33] US [31] 749865

[71] 专利权人 国际商业机器公司

地址 美国纽约

[72] 发明人 邓·考普斯密斯

普拉哈卡·拉格哈万

托马斯·G·兹莫尔曼

审查员 袁红霞

[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

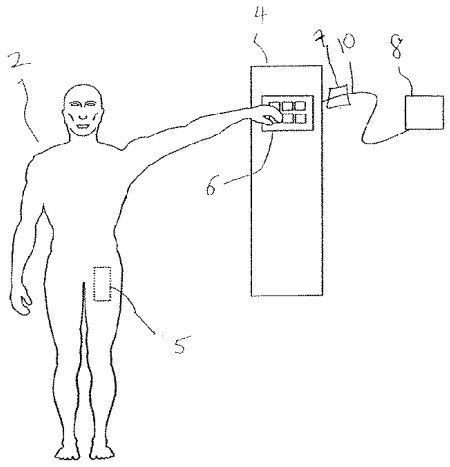
代理人 吴丽丽

权利要求书 3 页 说明书 20 页 附图 11 页

[54] 发明名称 用于和标识卡进行加密通信的近场人体耦合的系统及方法

[57] 摘要

公开了一种装置和方法，用于编码和从发射机向接收机传送数据，并使用人体作为传输介质。 发射机包括一电场发生器、通过调制电场来操作的数据编码器、以及耦合通过人体电场的电极。 接收机包括在物理上接触或靠近人体一部分的电极，以检测通过人体的电场，还包括解调器以从被调制电场中抽取数据。 与接收机相连的认证器处理编码的数据并确认传输授权的有效性。 该装置和方法用于识别和认证一个发射机的持有人。



ISSN1008-4274

1. 一种用于进行加密通信的系统，其组成是:

一个由用户个人携带或戴着的便携发射机，该发射机包括:

(i)存储一项信息的装置，

(ii)产生代表该项信息的加密电信号的装置，以及

(iii)把来自产生装置的信号耦合到用户身体上的物理接口；以及

一个接收机，包括:

(i)在接收机和用户身体之间建立电耦合的物理接口;

(ii)通过该物理接口从用户身体接收加密信号的装置;

(iii)对信号解密以得到该项信息的装置；以及

(iv)响应该项信息以完成动作的装置。

2. 如权利要求 1 中所述的一种系统，其特点在于:

发射机包括调制装置；以及

接收机包括解调装置。

3. 如权利要求 2 中所述的一种系统，其特点在于调制和解调装置包括调制和解调用的直接序列扩频装置。

4. 如权利要求 3 中所述的一种系统，其特点在于:

发射机有唯一的标识（ID);

加密电信号有相位；以及

发射机的直接序列扩频装置包括(i)与加密电信号的相位同步的装置，以及(ii)根据发射机的 ID 进行延迟的装置。

5. 如权利要求 2 中所述的一种系统，其特点在于解调装置包括通－断键控装置。

6. 如权利要求 1 中所述的一种系统，其特点在于还包括一个服务器。

7. 如权利要求 6 中所述的一种系统，其特点在于服务器包括一个接收机。

8. 如权利要求 6 中所述的一种系统，其特点在于该服务器包括一个认证器，它对每个单独用户都有一个公共 ID、一个专用密钥、以及一个时间

偏移值。

9. 如权利要求 8 中所述的一种系统，其特点在于发射机包括周期性发送认证信息的装置。

10. 如权利要求 9 中所述的一种系统，其特点在于该周期性发送认证信息的装置包括发送每日时间信息、用户公共 ID、以及随机数的加密码文本。

11. 如权利要求 6 中所述的一种系统，其特点在于该服务器包括为一群用户提供集中的唯一标识（ID）认证的装置，这群用户中的每个用户具有发射机。

12. 如权利要求 11 中所述的一种系统，其特点在于:

每个用户有一个唯一标识（ID）; 以及

发射机包括周期性发送关于用户标识（ID）和时间的消息的装置，该消息被一个加密函数加密，这个加密函数对于有发射机的用户而言是唯一的。

13. 如权利要求 12 中所述的一种系统，其特点在于产生加密电信号的装置包括:

移位寄存器 A，用于输出有第一和第二可能状态的一位; 以及

移位寄存器 B，它对应于移位寄存器 A 的位输出的第一可能状态;

移位寄存器 C，它对应于移位寄存器 A 的位输出的第二可能状态; 以及

向物理接口提供移位寄存器 B 的输出（该输出是响应移位寄存器 A 的有第一可能状态的输出位）及移位寄存器 C 的输出（该输出是响应移位寄存器 A 的有第二可能状态的输出位）的装置。

14. 如权利要求 13 中所述的一种系统，其特点在于:

移位寄存器 A、B、C 包括为所有用户公用的各自的抽头(tap)组; 以及

该装置还包括向各寄存器装载初始设置值的装置，该初始设置值是秘密的而且对每个用户是唯一的。

15. 如权利要求 12 中所述的一种系统，其特点在于加密函数是数据加

密标准（DES）。

16. 如权利要求6中所述的一种系统，其特点在于服务器包括为自主接收机提供本地认证的装置。

17. 如权利要求1中所述的一种系统，其特点在于包括一个卡，所述发射机位于该卡中。

18. 如权利要求17所述的一种系统，其特点在于所述卡可以是下列之一：

信用卡；

用餐卡；

电话呼叫卡；

保健卡；

驾驶执照；

录象带店卡；

汽车进入卡；以及

计算机进入卡。

用于和标识卡进行加密通信的近场人体耦合的系统及方法

一般地说，本发明是关于电子通信系统领域的。更具体地说，本发明是关于应用个人电磁编码标识介质来获取信息的服务。本发明特别适用于信用卡、标识卡等。

在当今社会，使用电磁场作为通信介质是无处不有的。通过物理介质（如导线）的通信及无线通信（如无线电广播和电视）两者都是分布广泛的而且是很平常的。这种通信可以在长距离上进行，包括与距地球几百万公里的空间探测器的无线电通信；或在短得多的距离上通信，如闭路电视或客户人使用终端与本地服务器的通信。

在一些情况里，在一项事务处理的过程中使用者实际上在终端或通信系统旁边。该终端对所有感兴趣的使用者都是可使用的，而需要由该终端提供服务的使用者找到该服务并用它进行一项事务处理。这种终端的实例是公共收费电话和自动付款机（ATM）。

许多事务处理涉及使用可移动手段来验证使用者的标识，授权该项事务，对服务收取费用等。这种手段经常做成卡片形式，上面带有可由终端读出的磁编码条。例如，一个要从ATM取现金的使用者站在ATM前面，插入他/她的卡片，并键入一个个人标识号（PIN），然后出现菜单提示的事务指令。对该事务的授权是根据对该使用者身份的确认，这基于（i）使用者具有授权卡及(ii)使用者知道PIN这二者的组合。

由于ATM通常被置于户外，对使用者而言这有许多缺点。其中一件事是使用者必须在事务处理开始时键入他/她的PIN。即使在较为偏僻的ATM那里，也极大可能有闯入者会在PIN被键入时看到它。对其他形式的事务处理，如在公共电话亭中使用电话卡通话，也存在这同样的缺点。

还有，当用户进行一项事务时会受到攻击，或者他/她的卡片或现金被抢或被偷。再有，许多ATM操作时，在第一个事务之后把卡片从槽口退除

一部分。这时用户或者可以把卡片取出，表明他/她不需要做另一项事务，或者把卡片留在那里并为另一个事务继续键入指令。在第二个事务过程中，卡片刚好放在开口中，任何人都能取走它，这个人可能想拿到它，抓住它，并跑掉。所以，当用户拿着 ATM 卡片或使用 ATM 卡片时卡片可为他人拿到，这表现出明显的易丢失或易被偷的缺点。

所以，需要一种通信形式，它通过使所用手段不易被主人以外的其他人接触到而减小用户被偷或被攻击的可能性。

最近出现的一种实现电子通信的新途径利用了这样一个事实，即人体主要由电解液构成的，因而它本身能携带电信号。

在一项由 David Allport 、 Neil Gershenfeld 及 Thomas Zimmerman 提出的待决美国专利申请“用外部感应的体内电流进行传感和发送信号的非接触系统”（尚无序列号）中描述了一种无线系统，其中通过用户身体以接触或靠近使发射机和接收机耦合。（是借助与地面靠近而完成电路的，地面被作为电路地）。

发射机产生低频、低功率信号，它通过电容耦合，作为位移电流进入或流出用户的身体。用户的身体起到导体介质的作用。与用户身体电容耦合的接收机响应从用户身体传送给它的位移电流以检测出低频信号。

由发射机发出的信号最好是载波信号，用伪随机码把要传送的信息调制到载波信号上，以产生扩频信号。这种调制具有抗干扰性，而且允许多个发射机同时操作，每个使用不同的调制代码。

电极最好是小而平的，用于把电子装置与人体耦合。可以把电极组合到常规与人体接触的物品中，例如手表、衣服、或鞋。也可把电极放在不与人体直接接触但很靠近的物品中，如放在钱包中的信用卡。

这种系统的某些其他方面在报纸文章“能触到它”中描述（ San Jose Mercury News, 1996 年 10 月 21 日），还在 Zimmerman 的文章“个人域网络：近场体内通信”，（ IBM 系统杂志， 35 卷， 3 、 4 期， 1996 ）中描述，它们在这里引用作为参考。在前一篇文章中，引用被采访者的话说，有待解决的一个问题是隐私问题，其中用户要控制和限制由这种设备发送的信息。

这样，这些先有技术系统没有说明如何避免不希望的被对手窃听和复制。如何使身体间电场（EF）通信能用于对侵入敏感的应用当中，特别是在货币兑换或标识确认方面应用，这一问题在上述参考资料中没有处理，成为留待解决的问题。

所以，本发明的一个目的是提供一种装置和方法，用于利用人体作为通信介质传送与用户有关的信息，它允许用户保护其隐私。

本发明的又一目的是提供一种装置和方法，用于利用人体作为通信介质传送与用户有关的信息，它保护信息的秘密，使未经用户授权或用户不希望的人不能接触这些信息。

本发明的又一目的是提供一种装置和方法，用于利用人体作为通信介质传送与用户有关的信息，它不允许未授权方产生出显然源于该用户的消息。

为实现这些目的和其他目的，根据本发明提供了一种通信系统，它在人体中产生小电流，该电流是由静电耦合外部感应产生的，该系统提供了近距离设备之间的无线识别和认证。

本发明提供一种装置和方法用于对数据加密供通过人体传输，它使用调制的电场，它提供了容易和快速的接收和认证，而且它有足够大容量去处理数以百万计的唯一发送机代码。

本发明的目标是使以可接受的价格和高度安全性和性能在百万计的人口中配备这种装置是现实的。为这些目标，本发明解决如下问题：加密，动态范围，低功率运转，多功能，多发射机，以及有效的解密。

加密最好足够简单以能在低价位微计算机上完成。在一个最佳实施例中，这种微计算机每秒执行10万到1百万条指令的量级。本发明的最佳实现使用的编码装置产生的代码以少于8000条指令足以标识出十倍于地球上的人口。

对于发射机丢失或被偷的可能性采取了措施。解密最好应在合理的时间内完成，通常在一秒以下。本发明的一个目的是提供一种解密方案，它能以几秒或更短的量级的响应时间来处理数千用户。

接收机检测到的信号强度会有急剧的变化，因为它取决于发射机和接

收机的位置和取向，发射机通常在人体上，所以不能对其限制。一个可靠的耐用的认证系统必须假定所收到的信号有大的变化，通常超过60dB。本发明的一个目的是提供一种系统，它能处理通常遇到的动态范围。

为了最大限度的方便性，在人体上的装置不应要求由人干预。认证过程应自动发生，不需人的干预。例如，如果手段是放在用户钱包中的一张卡，那么用户不必把卡拿出来采取任何其他物理动作使卡进行所要求的通信。

该装置还应有一个比较合理的使用寿命，最好至少一年或数年，极少需要由或不需要维护、修理或更换。如果是由电池供电的，那么它应消耗足够小的功率以允许电池寿命适当地长。本发明的一个目的是提供这种低功率、免维护的装置。

一个人在他/她的钱包中带有6到10个卡是不足为奇的。这样，根据本发明可以带几个卡，每个包含文本形式的数字信息或磁条。由于本发明需要电子电路，所以要比一片塑料的价格贵，因此希望使一个钱包中携带的这种装置的数量要最少。理想情况是用一个装置代替一个人的钱包中所有卡的功能。另一种情况是，如果在一个钱包中装有几个这种卡，它们的工作方式应不妨碍它们的相互操作。本发明的一个目的是提供一个卡来代替多个卡的功能。本发明的又一目的是提供一种系统，其中几个发射机可由一人携带而不会妨碍它们的相互操作。

虽然本发明主要是作为一个装置提出的，但一般掌握本门技术的人们会理解，如传统的数据处理机（包括CPU、存储器、I/O、程序存储器、连接总线及其他适当部件）之类的系统能被编程或被设计成利于把本发明实施为一种方法。这种处理器将包括适当的程序装置来执行本发明的方法。

再有，用于数据处理系统的制成品（如预先记录好的磁盘或其他类似的计算机程序产品）能包括一个存储介质及在上面记录的程序以指导数据处理系统顺利实现本发明的方法。人们将会理解，这种装置和制成品也附合本发明的精神和范围。

图1是根据本发明的个人域网络的典型应用图，它包括一个远程认证

器（authenticator），图中的人在启动一个自动付款机（ATM）。

图2是发射机和接收机模块的功能框图。

图3是发射机和接收机模块的功能框图，这里由接收机模块唤醒发射机模块。

图4A、4B和4C是设计成适于装入一个厚的信用卡中的典型发射机的顶视、底视、侧视截面图。

图5是典型接收机电路的电路略图。

图6和7是由根据本发明的装置执行的加密过程的流程图。

图8、9、10、11、12和13是在其中实施本发明是有好处的各种环境。

图14是本发明一个部分的伪代码实现。

图15和16是以移位寄存器实现本发明的密码编码的示意图。

用人体做为通信介质的一般性讨论

本发明的特殊优点在于通过人体的通信与无线通信相比，较为不易被偷听。下面关于无线通信技术中平行发展领域的评论，说明由根据本发明的人体通信克服了的缺点。

在无线网络方面当前的工作集中于红外（IR）光技术和无线电传输。基于光的通信系统要求从发射机到接收机的直的瞄准线。基于光的通信系统还要求一个光孔径。这排除了把使用这种技术的装置放入用户的口袋中或把它隐藏在用户的身上。

通常红外（IR）发射机用于无线网络，其功耗达到1瓦，超过了一个由电池供电装置（如手表或寻呼机）的耗电量。电池供电手表的一般标准是电池应能维持3年。所以最好是通信系统消耗足够少的电能，使其具有相匹的寿命。

也使用射频（RF）徽章。这种徽章通常采取带有RF发射机的卡的形式，如在共同转让美国专利5,5238,222（1996年6月18日发出）中描述的那样。

无线电发送引出一系列问题。无线电使用天线把电波转换成传播的电磁波。为了有效地发送和接收，天线的长度需要是波长一半左右。考虑到

位于人体处的装置通常要小于100mm长，则必须使载波频率超过1GHz，这达到微波范围的频率。这样的高频需要电路消耗很大功率。

天线需要特别的几何形状，或者是扁长的以捕获电场，或者是线圈状的以捕获电磁辐射的磁场。一个最好的通信系统应与它被嵌入的对象的几何形状一致并利用被嵌入对象的形状。

在GHz范围的射频开始具有光的方向性。身体能作为电导体是由于在血液中存在离子电解质。这给位于身体两侧的两个装置进行通信带来了困难的问题，例如一个电子表在右手上而由电池供电的微芯片呼叫卡放在左后口袋中就是这种情况。一个最好的通信系统应能在位于身体上任何位置的装置之间进行通信。

另一个考虑是无线电传输受到FCC（联邦通信委员会）的场强和频率限制。它的条例会在发布产品方面造成长时间的延迟。一个最好的通信系统不应受到FCC的许可证限制。

天线有最佳方向，按射束方向图发射能量，而不是全方位的。然而，要放在身体上的电子装置的设计者并不总是知道该装置可能放在何处。该装置可能得在常规产品的位置和取向范围内进行通信。例如，手表随着用者手的运动而运动和改变取向。一个最好的系统应在取向上有大的灵活性，能在一个运动和位置范围上运行。

辐射信号能在任何距离上以足够大的天线截听。这是广播具有的性质。某些在个人电子装置之间传送的数据可能具有敏感性，例如信用卡和电话的号码，客户记录，个人日记条目，商务通信，以及计算机标识口令等。其消息不能被截听的通信系统是最安全的。需要的是截听消息很困难的一种通信方法。

有许多人聚集在一块小地方的情况是常见的，例如在公共交通运输装置，电梯，排队队列，会议，以及听众。在这些情况下，由于来自近邻通信系统的干扰而使其失灵的通信系统是不能接受的。由于这些个人电子装置的通信是在一个有限距离（例如2米以下）上进行的，使通信系统具有有限的范围是有利的。

所以，一个所希望的个人域网络通信系统的目的可概括如下：

1)当前还没有标准方法来互连这些个人电子装置。静电耦合（ESC）可用于一类装置。

2)需要某种无线网络供这些传感器和其他电子装置来共享数据，但最好不是在空中的无线通信（RF），这类似于计算机使用的那一类，例如无线局域网（LAN）。ESC能提供网络结构的物理接口。

3) 一个最好的通信系统应消耗很少能量。由于ESC以比无线电低的频率工作，没有能量幅射，因而是低功耗的。

4)一个最好的通信系统应在取向上有大的灵活性，在一个运动和位置范围上工作。一个最好的系统应能在位于身体上任何部位的装置之间通信、ESC使用身体作为通信电路的一部分，并使用环境中的每种材料作为返回电流路径。

5)一个最好的通信系统不应受FCC的许可证限制。在本发明的最佳实施例中使用的电场强度低于FCC设定的电场强度几个量级。例如，典型ESC装置尺寸为80mm × 50mm × 8mm（一个厚信用卡），在330KHz以30V发射（通常用于谐振发射机），在300m处场强为344pV/m，比FCC条例第15部分规定的FCC允许场强低86dB。

6)所需要的是一种使得难于截听其消息的通信方法。因为电场以立方随距离衰减，在十倍距离上的场强为原强度的1/1000。随着到发射机距离的增大，信号强度迅速下降到环境热噪声以下，使偷听越发困难直至不可能。

7)没有来自近邻系统的干扰。静电通信系统的通信范围有限。而且电场强度随距离成立方衰减，所以近邻装置只能听到它们的近邻。来自更远些的装置的信号迅速衰减到背景噪声之下而不可听见。

8)天线尺寸小而且是扁平的，或者能采取它所嵌入的物体的形状。电极的有效性依赖于投射的表面面积。它不依赖于特定的严格形状和几何构成。手表带满足这一要求。信用卡特别好，因为它们呈现出较大的表面面积。鞋底也有大的表面面积，而且与地（外电极）和用户身体（内电极）都有特别好的接触，使它们成为与位于用户身体周围的其他装置进行通信的主要候选者。

密码术

本发明提供一种对数据加密的方法，用于以调制的电场通过人体传送数据，从而使它能被接收和快速认证，并以足够的容量处理数以百万计的唯一发射机代码。为了以可接受的费用和高度的安全性和性能来实现在数百万计的人口中布设，本发明解决了如下问题：加密/解密，动态范围，低功率运转，多功能，多发射机，及有效解密。

加密最好是在计算上足够简单以能在低价位微计算机上完成，这种微计算机运行在10万至1百万指令每秒的量级。加密的最佳算法不利用乘、模的指数、或其他在便宜的处理机上难于完成的操作。本发明使用的编码装置产生的代码足以以少于8000指令来识别地球人口的十倍。

最好应针对发射机可能丢失或被丢失来采取措施。解密应能在一个合理的时间内完成，通常应在1秒以下。本发明的一个目的是提供一种解密方案，它能以秒的量级或更少的响应时间来同时处理数千个用户。

在接收机处检测到的信号强度有急剧的变化，因为它取决于发射机和接收机的位置和取向，发射机通常位于人体上，所以不能被限定。一个可靠的耐用的认证系统必须假定收到的信号有大的变化，一般超过60dB。本发明的一个目的是提供一个系统，它能处理通常遇到的动态范围。

为了最大限度地方便，在人体上的装置不应要求人的干预。认证过程应自动发生，不受人的干预。该装置还应能工作一年或多年，最小的维护和修理或替换。如果该装置是电池供电，所以它应该是低功率装置以最大限度延长电池寿命。本发明的一个目的是提供一种低功率和免维护装置。

一个人在他/她的钱包中带有6到10个卡是不足为奇的。每个卡包含文本格式的数字信息或磁条，由于本发明需要电子电路，所以要比一片塑料的价格贵，因此希望使一个钱包中携带的这种装置的数量要最少。理想情况是用一张卡代替一个人的钱包中所有卡的功能。或者，如果在一个钱包中装有几个这种卡，它们的工作方式应不妨碍它们的相互操作。本发明的一个目的是提供一个卡来代替多个卡的功能。本发明的又一目的是提供一种系统，其中有几个发射机可由一人携带而不妨碍它们的相互操作。

图1是一典型环境图，其中使用了根据本发明的个人域网络，包括一个远程认证器。应理解，许多其他环境也可以利用本发明。这种其他环境

包括接受呼叫卡通话的公用电话，在加油站的油泵，复印机，邮件机，以及通过建筑物或汽车门的入口。还有，本发明可与计算机键盘连接使用作为一种口令机制。当用户把手从键盘上拿开时，机器便被锁住。

现在参考图1，一个人（或称用户）2正在启动一台自动付款机（ATM）4。个人2携带了一个个人域网络（PAN）设备5，如一个EF卡（下文中详细讨论）。ATM4包括一个控制面板6，它又包括适当的键，允许用户2键入适当的信息，如PIN（个人标识码）及所需处理的事务。该控制面板包括一个触点，用于建立与个人2的电连接。

ATM4由通信链路10与接收机模块7及处理机8相连。通常，处理机8位于远处，链路10包括适当的介质，如电话网。处理机8有处理用户2的事务请求所需的全部装备，如访问用户2帐户数据库等。

PAN卡5和处理机8通过用户2身体的导电介质和链路10进行通信，以确认用户2的标识。

根据本发明，通信是加密的，以建立认证的安全性。在下文中将详细讨论最佳加密技术。

再有，如果该用户带有多个PAN型发射机，如嵌在卡中、手表中或鞋中的设备，它们可以被分别检测以得到认证。

根据本发明（如图1所示），发射机和接收机联合工作以提供通信。对于双向通信，使用二个发射接收机。它们位于例如图1中的卡5和处理机8中。

图2和图3是这些发射机和接收机模块的二个最佳实施例的功能方框图。

在图2中，在一发射机和接收机之间发生单方向通信。该系统支持一种情况，其中卡5连续地或以规律的时间间隔（如每隔1秒）发送一个信号，例如一个标识码（ID）（见下文）。其假定是：每当用户2接触在一个适当的短时间内接触控制面板6，则规则发送的ID信号传送到控制面板供处理器8接收。这样，不需要提示或信号交换。

在这个实施例中，卡5包括一个发射机模块，图中已详细画出。如下文要讨论的那样，发射的信号是根据本发明加密的。因此，卡5包括一个

信号发生器12，它最好是根据一个随机数、一个时间表示和一个用户ID来产生加密的信号。所产生的信号用一低频调制器14调制，并发送给用户2的身体组织，这是由于卡5与用户2的身体靠近。在图2中用户身体2用一单方向通信线来代表。

因为用户2物理上与控制面板6上的接收电极18接触，所以接收机4被连成接收信号。信号被解调器20解调，并通过网络链路10传送给处理机8。在处理机8内，认证器根据下文中详细描述的加密协议来认证信号，并把信息提供给应用程序24，例如处理ATM事务的程序。

在图3，在卡5中的发射接收机和ATM4中的接收机之间发生双向通信。这另一种系统所支持的方案中只在请求时才发射信号（例如标识码（ID），见下文），从而使卡5节省能量。其假定是：每当用户2接触控制面板6并开始一项事务时，控制面板6请求信号，于是卡5以发送信号作为响应。这样，便完成了提示或“握手”序列。

图3中的一些部分等效于图2中相同标号的部分；然而，一个单独的通信信号26，即前面提到的请求，从控制面板6通过用户2身体向卡5传送。这个请求由ATM4中的唤醒电路28产生，由卡5中的唤醒接收机电路30接收。唤醒电路30最好能控制卡5上的节能功能，以在空闲时减少耗能，而一旦收到请求便恢复完全供电。

当恢复供电时，微处理器电路32产生一个加密的信号，其产生方式与图2中的发生器12在很大程度上是相同的。ID信号象前一种方案一样传送给ATM4，那里微处理器34象前面一样指示通过网络10把解调后的信号传送给处理机8。

为了低功耗，微处理器特别是在卡5上的微处理器32最好是低频部件，如CMOS微处理器，由于卡5的数量相对于ATM4的数量而言是很大的，微处理器及总体电路的价格最好是不对称的。就是说，使用大量便宜的发射机（每人一个），但少量昂贵的接收机（每个ATM机、汽车、门等有一个接收机）。同样，最好是发射机利用比较简单的电路，而接收机可以更复杂。

该系统最好利用由卡5产生的密码（例如由不持久的（perishable）

口令随机数发生器（下文中详细描述）来产生）和由用户 2 键入的 PIN 的组合。

EF 卡的最佳实施例

图 4A、4B 和 4C 分别是设计成适宜厚信用卡形式的卡 5 的一个最佳实施例的切顶、切底和切侧面后的视图。卡 5 包含一个如图 3 的发射机。

发射机 5 有一个顶部电极 100 和底部电极 102。发射机足够大能包括 6 个硬币大小的锂电池 104，通常能有 2 年以上的电池寿命。电子电路 106 包括一个微处理器 32，位于电池 104 之间，以有效地利用卡片的面积。

环形天线 108 检测通信信号 26，后者唤醒微处理器 32 以在数据通信之间最大限度地节省能量消耗，选择环形天线 108 的尺寸和通信信号 26 使卡 5 和 ATM4 之间有最佳的信号耦合效率。

通过使天线环的周长基本上接近通信信号 26 的 1/2 波长，使环 108 的辐射方向图没有空区，使卡 5 对取向的敏感性为极小。通信 26 的频率最好在 100MHz 和 500MHz 之间。通信信号 26 可以简单到是一种总是连续的恒定载波。

当卡 5 达到足够近时，在环 108 中产生的电压将足以使微处理器 32 接通。如果有几个人在 ATM4 附近，而且他们的卡 5 被接通，那么只有接触 ATM 接收机电极 18 的人将被检测。

可以提供一个通/断开关，用于不需通信时使该单元断掉。最好是绕卡 5 滑动一个金属盒。这将挡住 RF 达到该装置。在卡 5 上还可放置附加的按钮（未示出），以便允许在例如由一人所有和携带的多个信用卡当中选择几种功能。一种最佳方法是让 ATM4 显示用户 2 可用的几个卡（实际是帐户），并让用户在控制面板 6 上选择所希望的帐户。

图 5 给出典型接收机电路的电路略图。接收机检测在接收机电极 18 上的小位移电流。放大器 200 放大该位移电流并将其转换成电压。放大器 202 和 204 提供进一步放大的放大级。一个由微处理器 208（如 Microchip technology 公司(Chandle, Arizona)出售的 PIC 16C 57）控制的数控开关 206 选择放大器输出之一，并将被放大的信号 210 加到快速模拟一数字转换器 212，例如 Maxim Corporation (Sunnyvale, CA)出售的 MAX 153，它

能在8比特位下每秒完成一百万次转换。

其结果是动态范围超过60dB的通用的位移电流数据获取。一旦在微处理器208中俘获了数据取样，便可以采用多种通信解调技术。

一种最佳通信解调技术是直接序列扩频，如Leon W. Couch在“现代通信系统”一书（Prentice Hall, N. J.,1994，380－387页）中所描述的那样。使用扩频以允许有选择地检测多个发射机的最佳方法是让每个发射机与通信信号26的相位同步，并根据每个发射机的唯一标识（ID）号来延迟伪随机序列。为在多个发射机之间进行选择，接收机将移动相关函数的相位，寻找自相关函数的峰值（见Couch的书的第384页）。

通信解调技术的另一实施例是通断键控，这里由载波通代表1，载波断代表零。这种振幅调制（AM）方案比扩频简单，而且可以根据信号强度来选择多个发射机。

在一个最佳实施例中，EF卡产生一个总是变化的加密输出，以防止窃听者截获输出并在以后回放。卡中的微控制器含有用户的唯一公共标识号（64二进位）、唯一专用密钥（64二进位）、唯一专用时间偏移（64二进位）以及产生DES加密输出的程序。每秒钟EF卡发送三段信息；EF卡的当日时间，用户的公共标识号，以及由EF卡当日时间和专用密钥的偏移文本产生的随机数的加密文本（结果为64二进位）。读出器检测这三个值，并把它们送到安全认证器，由它确认代码的有效性。

认证器包含每个用户的公共标识、专用密钥、以及时间偏移值的数据库。认证器使用公共标识号来查找时间偏移和专用密钥，并用相同的DES算法对时间偏移加密，以检验EF卡的有效性。

微控制器使用便宜的手表晶体来保持一个误差在每年几分钟之内的时基。这个时基用于靠一个反馈移位寄存器（对移位寄存器的多个抽头(tap)进行异或（XOR）操作）来产生伪随机数。一个专用偏移被加到传输的当日时间上，于是即使窃听者知道随机数表也不能知道所产生的随机数是什么。

在该系统中唯一已知的弱点是认证器必须允许EF卡的守时器中的变化，这种变化是由于EF卡时间基准晶体对温度的依赖性，从－10℃到60

℃范围内这种变化是50ppm。这就产生了一个脆弱的时间窗口。在这个时间窗口内窃听者能记录一个EF卡的输出并在一个暂时的可接受窗口内重播这个输出。误差的可接受窗口随时间而增大，在每次EF卡认证时被复位。

理论上最坏的情况是每年26分钟，但由于EF卡通常是由用户个人携带，因此假定用户身体通常保持室温因而EF卡也通常保持室温是合理的。如下事实表明了这种假定的合理性：低价位（10美元以下）的电子手表的变化小于每年几分钟。

通过对窗口大小设定限制，需要周期性的认证，从而限制了安全脆弱性。

在一个最佳实施例中，EF卡包含的一个微控制器在低频（32KHz）下运转，在2.5V用28μA（微安）。发送(振荡信用卡的板)消耗大约500μA，但只占用时间的10％（假定每秒一次以2400波特传输3字节（24位），造成平均电流50μA。通常的CR2430锂钮扣电池(直径24.5mm，厚3mm）约为一个25美分的硬币大小，容量为200mAh（毫安小时）；足以运行微控制器和发射机约3.5个月。一个信用卡上能装6个这种电池(和电子电路一起)，得到的1.2年的寿命。把报告次数降到每5秒一次，可使寿命延长到3年。使EF卡的电池数和厚度加倍，也会使EF卡的寿命加倍。由用户2启动的通/断开关会进一步延长电池寿命（假定8小时通，16小时断，每周5天）。

最佳加密技术评述

下面的讨论给出上述EF卡的两种安全实现的细节及认证服务器的细节。这些可概括如下：

1. 对大量人口的集中化唯一标识（ID）认证

服务器唯一地识别卡的持有者，拒绝假冒的企图。一个应用实例是用于以百万计的人口的唯一ID，他们中的每个人能把卡用于ATM访问，驾驶员证，护照，电话卡，信用卡或其他服务。系统的难点在于小心地选择服务器用于有效认证的偏移参数。选择参数的细节取决于实施例，并在下文中给出。

2. 在自主锁中的本地认证

在上面给出的实现中，假定多个接收机连于一个集中的认证服务器。而这里代之以每个接收机有它自己的处理器，但不与任何中央服务器连网。例如，在汽车中的门锁可以由这种独立的处理器来实现。一个用户卡可被编程来访问这种锁的任何子集合。

下面将详细描述这两个最佳实施例

1. 集中的唯一 ID 认证

每个用户有一个唯一标识（ID） X，由一个位串来代表，通常为 32 位长，允许（在本例中为 32 位）约 4 百万用户有唯一位串 IDS。

卡以 1 秒间隔发送 f(X,t)（以位串表示），这里 f( )是为 X 所专用的加密函数，t 是从初始同步起点起测量的时间（以秒为单位）。下文中描述加密函数和认证服务器的两个实施例。再有，对每个实施例都会表明，加密函数是不能被破译的，除非通过穷尽的（这是不实际的）计算。

2. 自主接收机的本地认证

在不希望用网络把所有接收机（例如锁）连到一个中央服务器的情况下，可以使用不同的方案，其中对每个 EF 卡的 EPROM 编程（在一中心站）使其能访问全部接收机的一个子集合。

假定在每个接收机（锁）处有一个中等计算能力的处理机。

参考图 7 中的流程图，对每个卡给一个密钥 X。多个卡可以共享同一个密钥 X，如果它们被授权访问相同一组接收机的话。X 的第 i 位表明第 i 个锁是否允许以密钥 X 访问该卡。这样，在一个有 500 个锁的建筑物中，密钥 X 就会由 500 位组成。

用随机选取的长度约 1000 位的串散插到 X 中，从而得到新的密钥 Y。这用来对专用函数 f(Y,t)中的时间加密，这里的 t 和前文中一样代表时间。这个专用函数对全部锁都是知道的，因为借以从 X 导出 Y 的随机图样是知道的。当试图打开锁 r 时，在锁中的处理机对传输内容进行解密，即转换 f 并在验证随机插入位之值正确之后把这些位去掉，如果在 X（解密之后）中对应于 r 的位为零或者时间 t 不匹配（在锁偏移窗之内，并根据编码方案附加一个长度为 4 倍于 t 的平方根（sqrt(t))的秒值的时间窗）。

最好是，由EF卡传送的信号（由ID、时间等构成）用对全部卡都知道的公共密钥来加密，并只能由服务器能得到的专用密钥来解密。潜在的能力是，位于一个地理区域的根据本发明的接收机网络能用于跟踪一个人的行踪。

由于根据本发明的装置发送的信号看起来是随机数，所以窃听者看到的是无意义的东西（随机数），它不能揭示出关于卡的携带者的任何信息。只有当这些数被送到一个认证器时，它们才与一种服务链接，如ATM、驾驶执照、电话呼叫卡等。

在一个实施例中，发射机卡放在个人的钱包、衣袋或手提包中，而接收机被集成于各种应用当中。发射机包括微处理器电路、电场发生器、电池、以及时间参考。微处理器电路包括识别数据、控制软件、和加密技术。接收机包括电场接收机、微处理器和时基。发射机被装在一个大约信用卡大小的塑料套内，装在用户的手提包或衣袋中。接收机被集成于适合应用的装置中。

加密的第一实施例：移位寄存器

一个实施例涉及移位寄存器，参见图15和图16。

关于本实施例的其他背景信息，可参见如下参考文献：

参考文献（1）：

C. G. Gunther,“由移位寄存器控制的交替阶跃发生器”，计算机科学中的文献注释304，密码术的进展：87'加密文集，柏林，Springer-Verlag, 1988, 第88－92页。

还可参见

参考文献（2）：

Don Coppersmith, Hugo Krawczyk，及Yishay Mansour,“收缩（shrinking）发生器”，密码术进展，－CRYPTO 1993年会，Douglas R. Stinson（编者），Springer LNCS卷773，1994，第22－39页

D. Coppersmith, A. Herzberg, H. Krawczyk, S. kutten, Y. Mansour，“收缩发生器：用于流密码加密系统的一种新型伪随机发生器”，在ITL发表，1992年10月。

在参考文献（1）中，使用3个移位寄存器，每个的长度约为100。第一个寄存器A操作和输出1位。这一位决定是否使用第二个或第三个寄存器B或C。接下来，这个寄存器B或C操作和输出1位，它用作为系统的输出。在这一时间步长，另一个寄存器C或B是空闲的。

三个寄存器的抽头（tap）（决定多项式）对所有用户可以是共同的，而初始设置值对各用户是变化的而且保持为秘密值。用户会广播他的ID、他的卡输出的最后128位、以及他得知的时间t。服务器将把时间t与实际时间做比较；调出用户寄存器的初始设置，并使寄存器A向前t步（这能迅速完成）并使寄存器B和C分别向前大约t/2步。

寄存器A的输出中的各0位会指出系统输出的128位中哪些位来自寄存器B。

服务器将检验在时间间隔 $t/2-2\,t^{1/2}$ 和 $t/2+2\,t^{1/2}$ 之间寄存器B的输出，以找出对应于这些输出位的位图象。确切位置U取决于寄存器位的各0位输出的个数，因而难于快速算出。服务器也对寄存器C完成类似计算，以找出它的位置V。

如果用户是合法的，则二个位置应满足 $U+V=t$。

这个实施例对于EF卡是简单的，只需大约300位RAM和几百位ROM。服务器所需计算略多些，需要对约为 $4\,t^{1/2}$ 的位串进行求值，或者说每个寄存器有大约100,000位输出。

服务器计算的这种新颖实现比蛮力检验显著地高效率，能当（潜在的）数百万EF卡并发访问资源时切实可行地实现一个服务器系统。

再有，由于时钟漂移，服务器通常不会严格地与每个卡同步。所以它允许在一个δ秒的“漂移窗口”内认证。就是说，如果t是根据服务器得到的时间，那么只当对某个t'收到信号 $f(X,t')$ 而且 $|t-t'|$ 最大为δ时它才给予确认。

参考文献（2）描述了一种类似的配置但只用二个移位寄存器。第二种配置的安全性减小了，但实现起来较简单（只用二个移位寄存器而不是三个）。

必须在大约 $t^{1/2}$ 个时间步长接收给定的信号，它应减至最小以限制窃听

者具有的操作时间。

加密的第二实施例：数据加密码标准（DES）

第二个实施例要涉及众所周知的数据加密标准（DES）。

参考图6的流程图，每个用户将有一个秘密的DES密钥X。每秒一次由卡发送用户ID及在对应于这个ID的密钥X之下消息t的DES加密，对此我们可用f(X,t)表示。服务器将接收ID，查找对应的密钥X，并检验f(X,t)的计算结果。

EF卡需要大约96位RAM作DES加密，需要另外64位用于t，还需要几千位ROM用于DES。（更快地实现DES会需要约32k位ROM）。

图6还给出按上面所说明的数据包的典型格式。

图14是图6中同步器的伪代码实现。

这里再次利用了漂移参数来调整同步。漂移参数（用δ表示）的选择受如下约束：

（1）它要足够大，以复盖时钟漂移和$4t^{1/2}$之和（对于上述第一实施例）

（2）它要足够小，以使窃听者的“机会窗口”不能重新使用相当长时间的传输。

不能期望在服务器和EF卡上的时钟保持绝对同步。所以服务器允许有一个时钟同步窗口（通常可为8秒）（这是卡和服务器的时间表示之间允许的差异），在此窗口内将进行认证。这一功能是在服务器的同步器中实现的。一旦收到了卡的信号，服务器的同步器便检验卡的时间表示是否在它自己时间的8秒之内，如果是，再检验该卡是否被允许访问服务器。

每次成功认证之后，δ时间即被复位为零。漂移有二个原因：(a)一个特定卡的时间基准快于或慢于认证器的时间基准，(b)通常由于温度变化造成的一个特定卡的时间基准发生了变化。

第一种情况是可以预测的，在一个最佳实施例中，认证器根据相继的认证来计算每个卡的频率。由于温度变化造成的漂移通常很小，因为卡通常由人携带处于室温。廉价的数字手表的守时能力表明实际的时间基准的稳定性，这种表能使时间误差保持在每年几分钟之间。

本发明（嵌入由用户携带的卡中）能应用的场合

本发明的一个目的是用一个通用电子卡代替个人钱包中的多个塑料卡。本发明能代替许多塑料卡的功能，包括信用卡、用餐卡、电话呼叫卡、自动付款机（ATM）现金兑换卡、保健卡、驾驶执照、录象带店卡、飞机乘客卡、汽车和计算机的允许进入卡。下面是表明EF卡在多种应用中的可用性的一些场合。

信用卡

读出电极可放在现金收入记录机附近的毯子或面板上。当顾客站在现金记录机旁时，来自个人EF卡的标识信息便被传入接收机。当购买的物品项目都汇总相加之后，顾客可按一下按钮，以认可这次购物。

用餐卡

参考图8，读出图放在由服务员带给顾客的盘子300中，盘中有餐馆帐单302。顾客触摸接收电极18以认可付款。如果此人有几个信用卡，则会出现代表各卡的图符，此人便可选择他/她希望记入的那张卡。为增加安全性，可在纸帐单上留下签名。把接收电极18放在纸帐单下面，便可在顾客签名时收集电子识别信息。

电话卡

参考图9，接收机电极18放在公共付费电话的送受话器310上。当个人拿起送受话器310时，此人的识别信息便从EF卡5通过此人的手和身体以及在送受话器310上的接收机，加载到网络计算机上进行认证。加载可与手工拨号同时进行，从而使认证的完成没有延迟，也不会中断呼叫过程。

因此，卡5使得使用付费电话如同家中电话一样方便，顾客只需拿起电话和拨号，无需忙于使用电话卡或进入号码。

保健卡

参考图10，接收机电极18位于放在设施全部入口处的地板垫子330中，以及放在所有楼梯的电梯前面的地板垫子330中。接收电极也可以位于病人在进入设计时可能遇到的其他固定物或物体上。

当某人进入设计时，由检测模块7来检验个人的标识信息。该信息及

垫子的位置被送到设计计算机中。这一信息与预约信息进行比较，以通知一个适当的部门病人到达。

在机场，可以类似地使用飞机常客卡，用于飞机预订信息。

驾驶执照

警官携带一个根据本发明实现个人域网络的个人数字辅助器，它还包括一个无线电链路连到警官巡逻车中的计算机上。接收机电极位于一个交通传票记录仪（traffic citation log）内部。该记录仪包括一个通到警察局的无线电链路。如象前面一般性讨论的那样，通信能迅速确认驾驶执照的有效性和访问驾驶员的记录。

录象带店卡

参考图 11，接收机电极 18 位于出口通道附近的门垫中。卡 5 标识信息将用于指出个人的账号。

本发明能与无线电标签技术结合，该技术能电子识别每盘录象带。顾客从架子上选取他/她想要的录象带 400，然后只要走出该商店即可。包装在每个录象带 400 上的无线电标签 402 会识别由顾客拿走的那些录象带，而卡 5 会识别出要付的账单。

汽车进入卡

参考图 12，接收电极 18 位于金属门把手 410 中。当受权的卡 5 持有者把他/她的手放到门把手上时汽车门自动打开。在一固定时间段内（例如 15 秒）接触门把手而不拉开门闩，则使所有车门锁住。

计算机进入卡

参考图 13，接收电极 18 位于计算机键盘下面。计算机键盘通常处于不能用状态。当受权卡 5 持有人的手接近键盘时，键盘变为能用状态。这种安排防止未受权人使用该计算机。在餐馆和零售商店的收款机可以使用类似的系统。

实施例的法定（statutory）分类

利用前面的说明，本发明能以标准的编程和/或工程技术来实现，使用计算机编程的软件、固件、硬件或它们的任何组合或次级组合。任何这样产生的程序连同计算机可读的程序代码手段，可以在一种或多种计算机可

读或可用介质中实现提供，这类介质如固定（硬）盘驱动器、磁盘、软盘、光盘、磁带、半导体存储 （如只读存储器（ROM））等，或者通过任何发送/接收介质，如因特网或其他通信网络或链路来提供，从而构成一个根据本发明的计算机程序产品，即制成品。可以通过直接执行一个介质体中的代码、或把代码从一个介质体拷贝到另一个介质体中、或通过网络传送代码，来制作和/或使用这个含有计算机程序代码的制成品。

为了制作、使用、或销售本发明所使用的装置可以是一个或多个处理系统，这些系统包括但不限于中央处理器（CPU）、存储器、存储设备、通信链路、通信设备、服务器、I/O（输入/输出）设备；或者是一个或多个这种处理系统的任何二级组成部分或单个部件，包括软件、固件、硬件或它们 任何组合或二级组合，由它们实现在权利要求书中提出的本发明。

可以通过键盘、鼠标、笔、声音、触模屏、或其他任何能由人向计算机输入数据的手段，包括通过其他程序（如应用程序），来实现接收用户输入。

精通计算机科学的人将能容易地把按所描述方法生成的软件与适当的通用或专用计算机硬件结合，以产生一个实现本发明的计算机系统和/或子系统，和产生一个实现本发明方法的计算机系统和/或计算机子系统。虽然已详细描述了本发明的最佳实施例，但显然，对于精通本门技术的人而言，可以对实施例进行修改和调整而不偏离如下面的权利要求书中提出的本发明的范围。

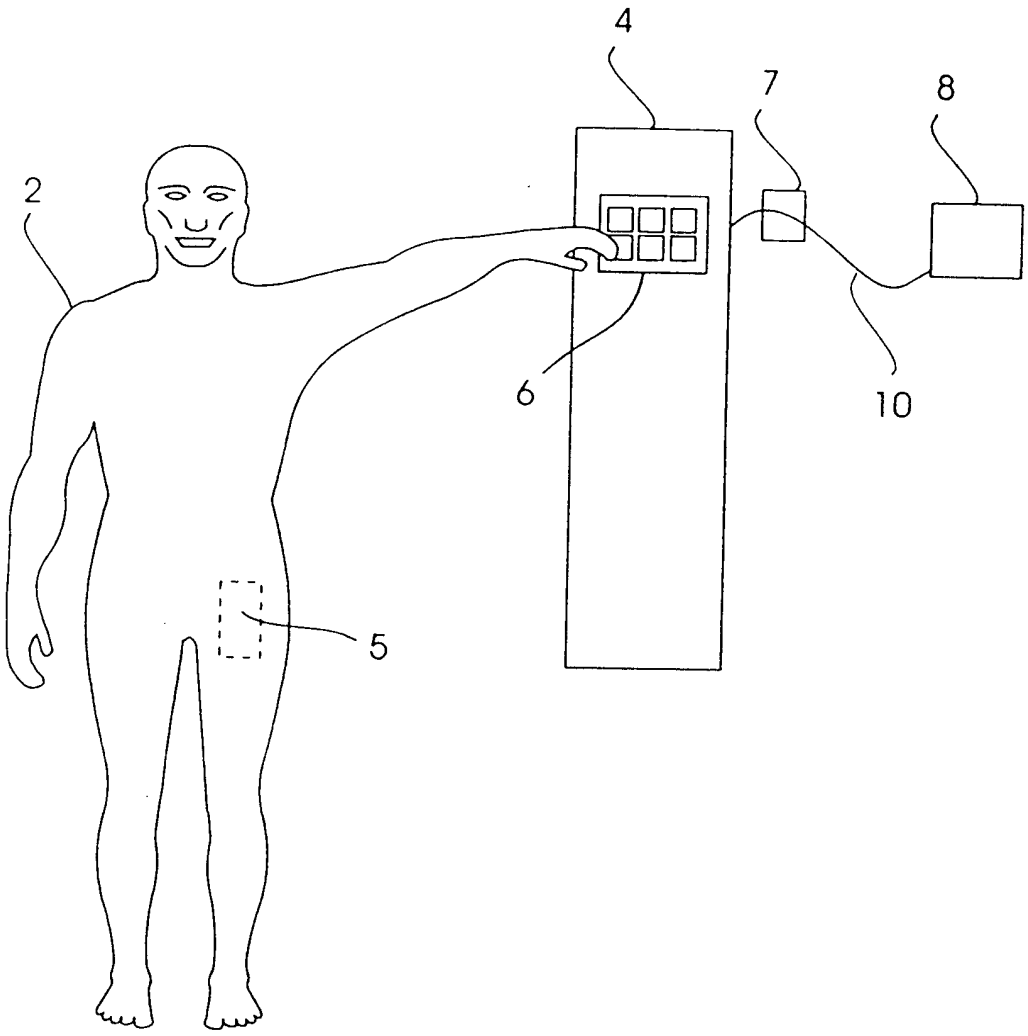


图1

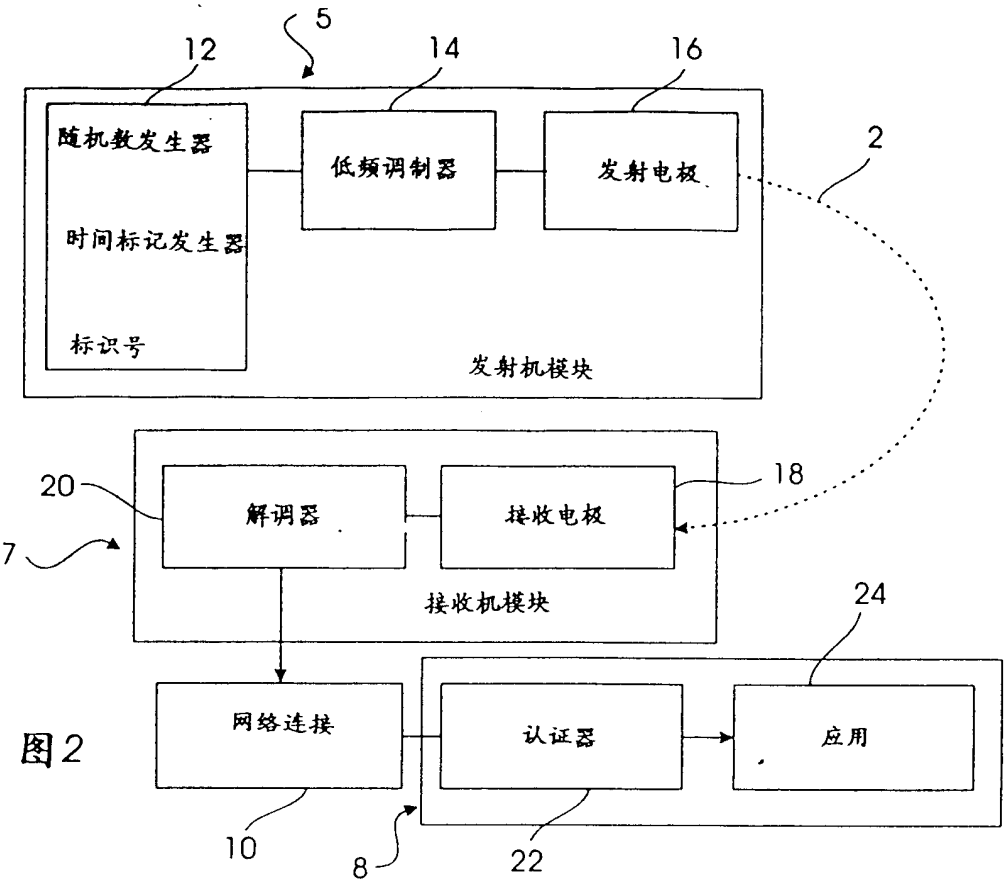

5
12
14
16
随机数发生器
时间标记发生器
标识号
低频调制器
发射电极
2
发射机模块
20
解调器
接收电极
18
7
接收机模块
24
网络连接
认证器
应用
10
8
22

图2

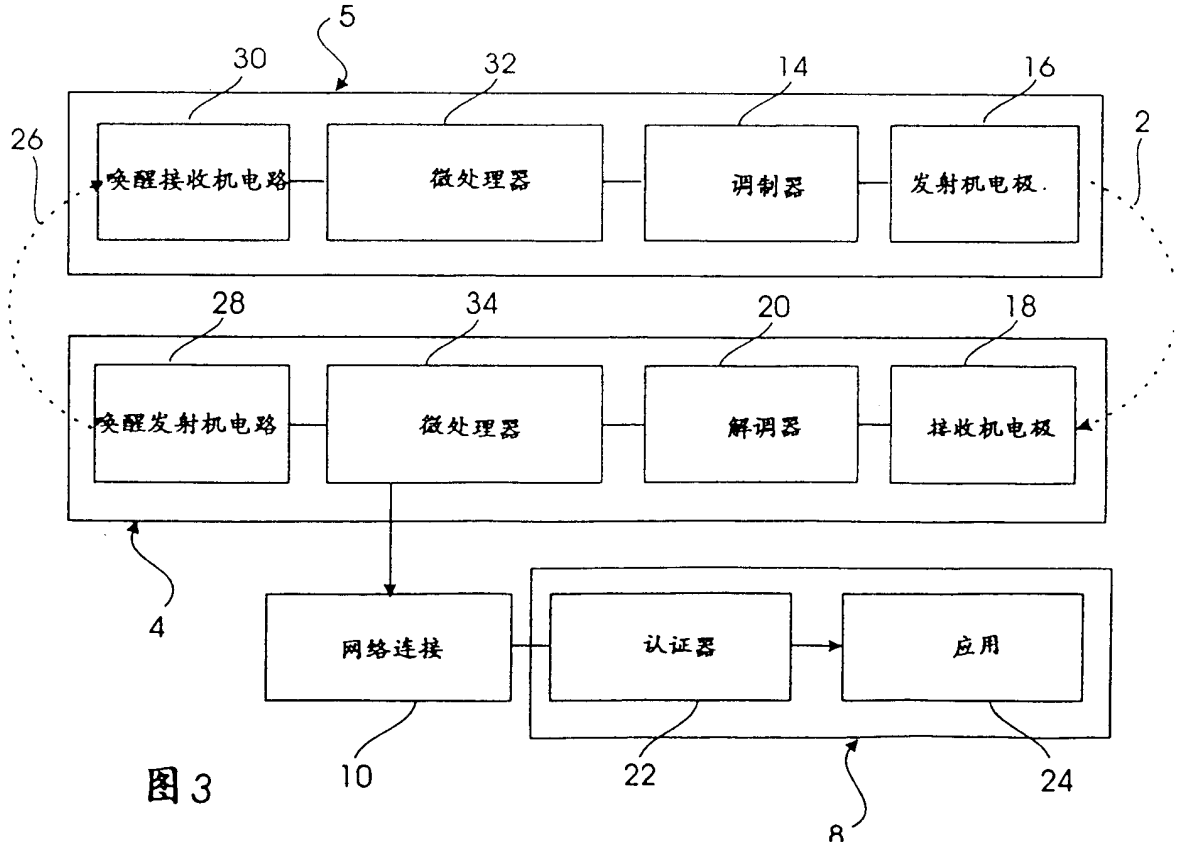

5
30
32
14
16
26
唤醒接收机电路
微处理器
调制器
发射机电极
2
28
34
20
18
唤醒发射机电路
微处理器
解调器
接收机电极
4
网络连接
认证器
应用
10
22
24
8

图3

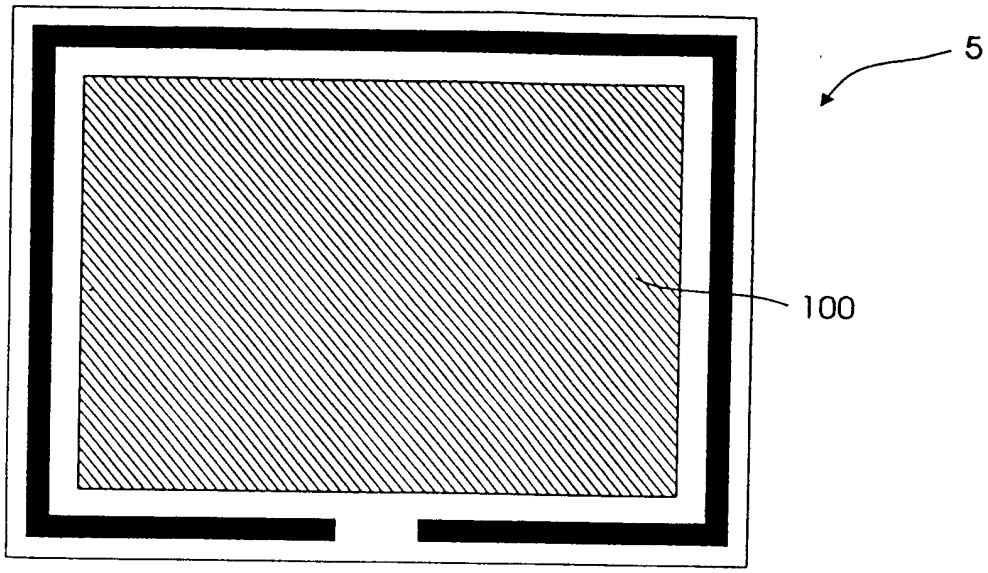


图 4A

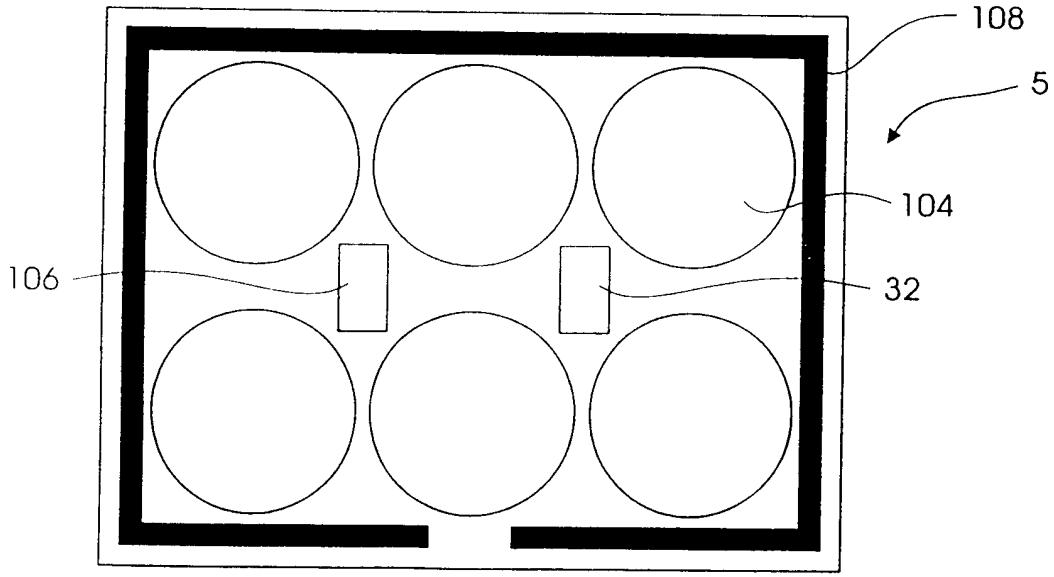


图 4B

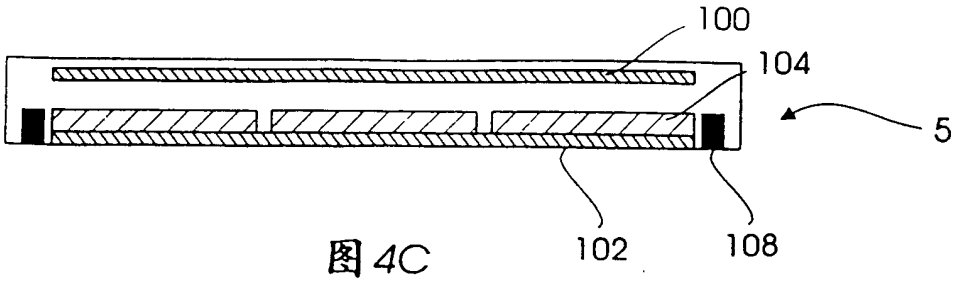


图 4C

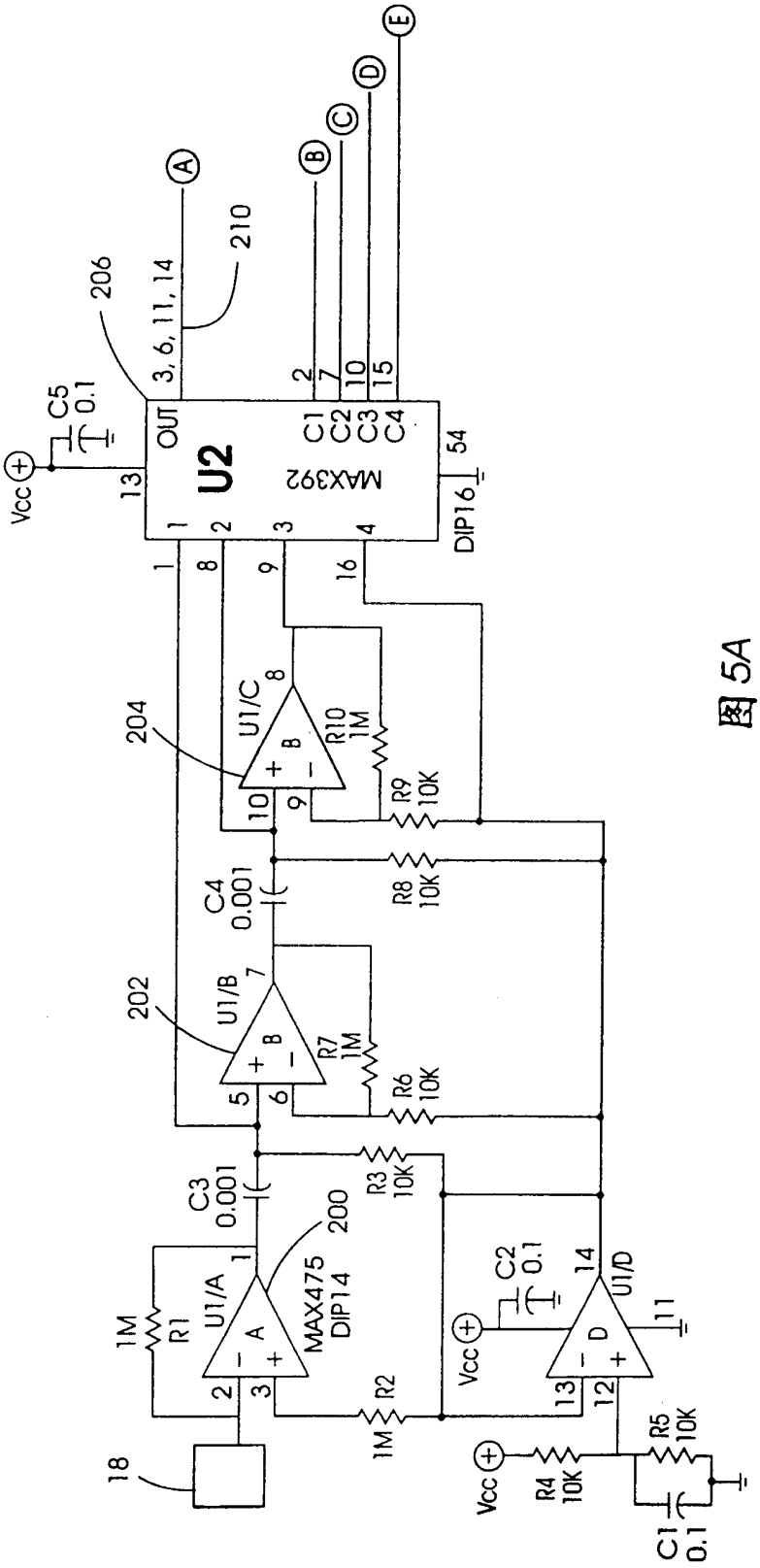

U2
MAX392
DIP16
OUT
C1
C2
C3
C4
A
B
C
D
E
210
206
204
202
200
C5 0.1
U1/C
U1/B
U1/A
U1/D
MAX475
DIP14
R1 1M
R2 1M
R3 10K
R4 10K
R5 10K
R6 10K
R7 1M
R8 10K
R9 10K
R10 1M
C1 0.1
C2 0.1
C3 0.001
C4 0.001
Vcc
18

图 5A

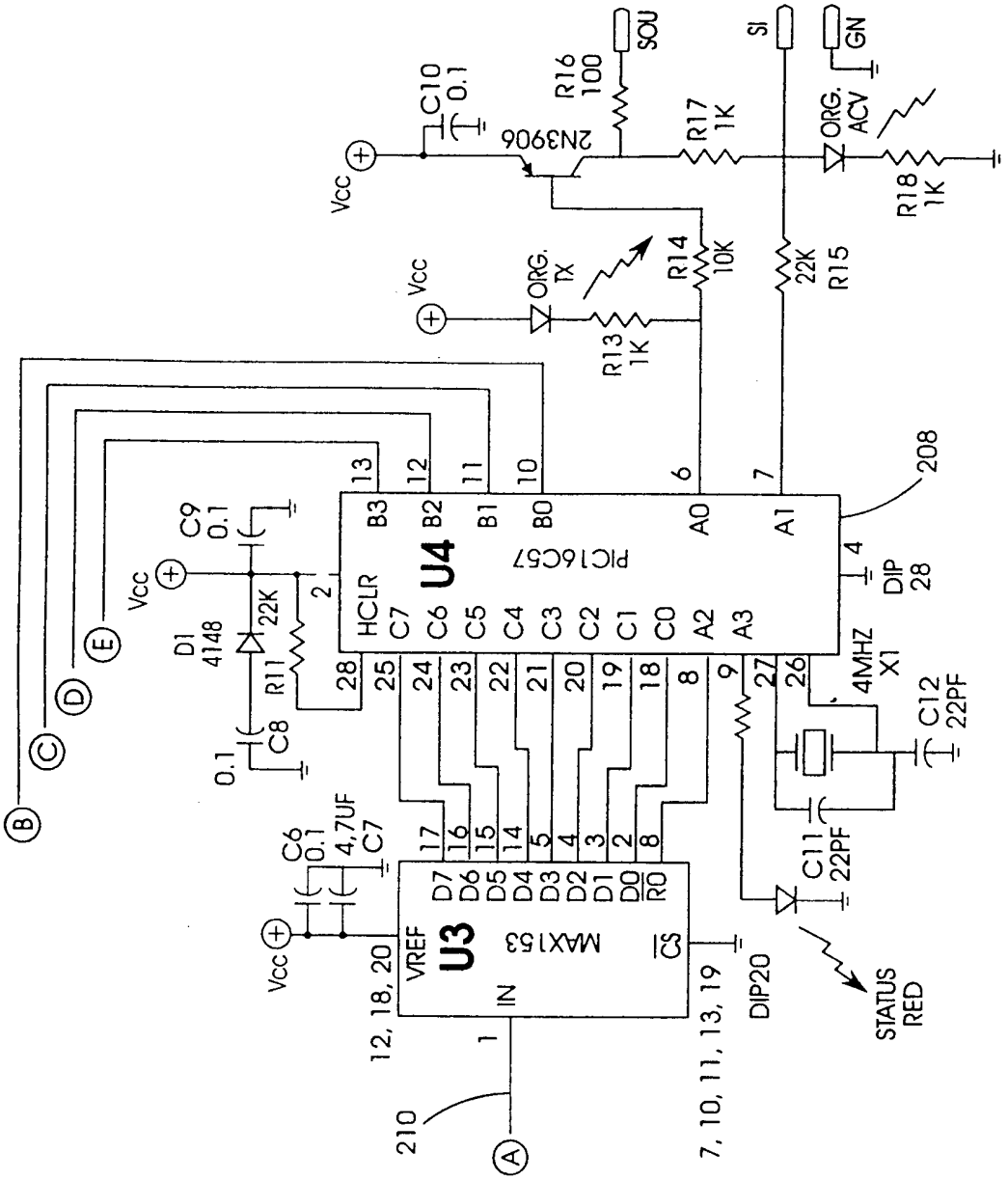

U4
PIC16C57
U3
MAX153
Vcc
SOU
SI
GN
ORG. ACV
ORG. TX
2N3906
R16 100
R17 1K
R18 1K
R13 1K
R14 10K
R15 22K
C10 0.1
C9 0.1
C8 0.1
C6 0.1
C7 4,7UF
C11 22PF
C12 22PF
D1 4148
R11 22K
4MHZ X1
DIP 28
DIP20
STATUS RED
208
210
12, 18, 20
7, 10, 11, 13, 19
HCLR
VREF
IN
CS
A
B
C
D
E

图 5B

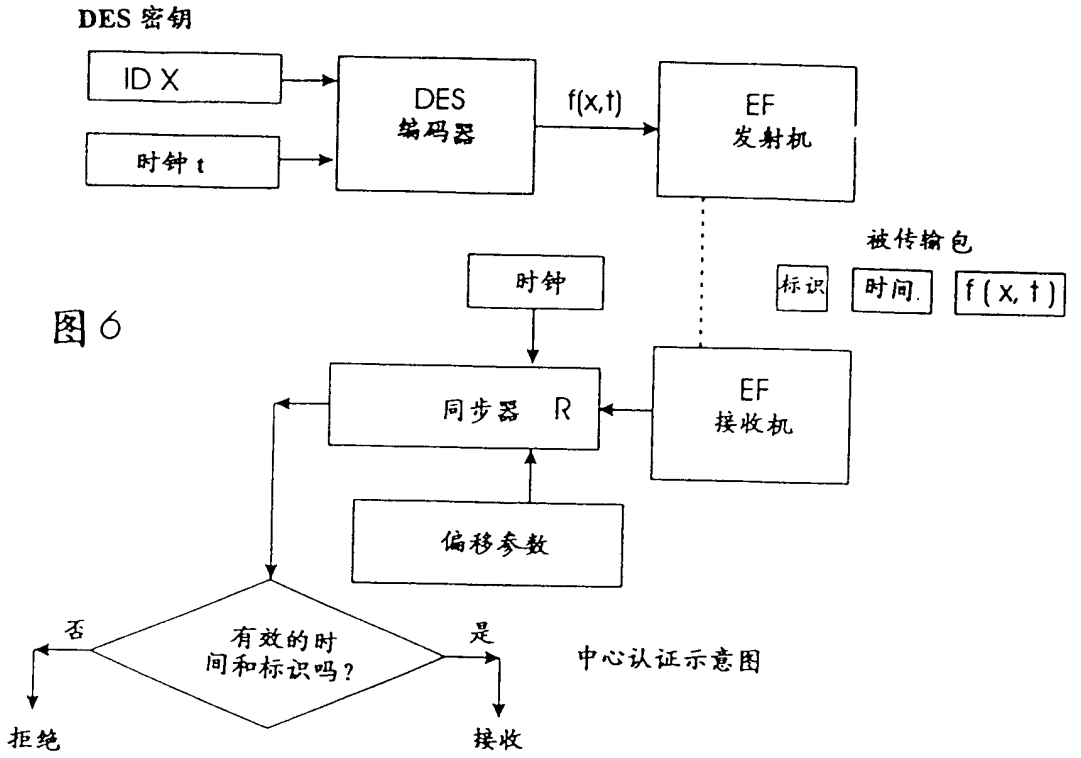

DES 密钥
ID X
时钟 t
DES
编码器
f(x,t)
EF
发射机
被传输包
标识
时间
f(X, t)
时钟
同步器 R
EF
接收机
偏移参数
否
有效的时
间和标识吗?
是
拒绝
接收
中心认证示意图

图 6

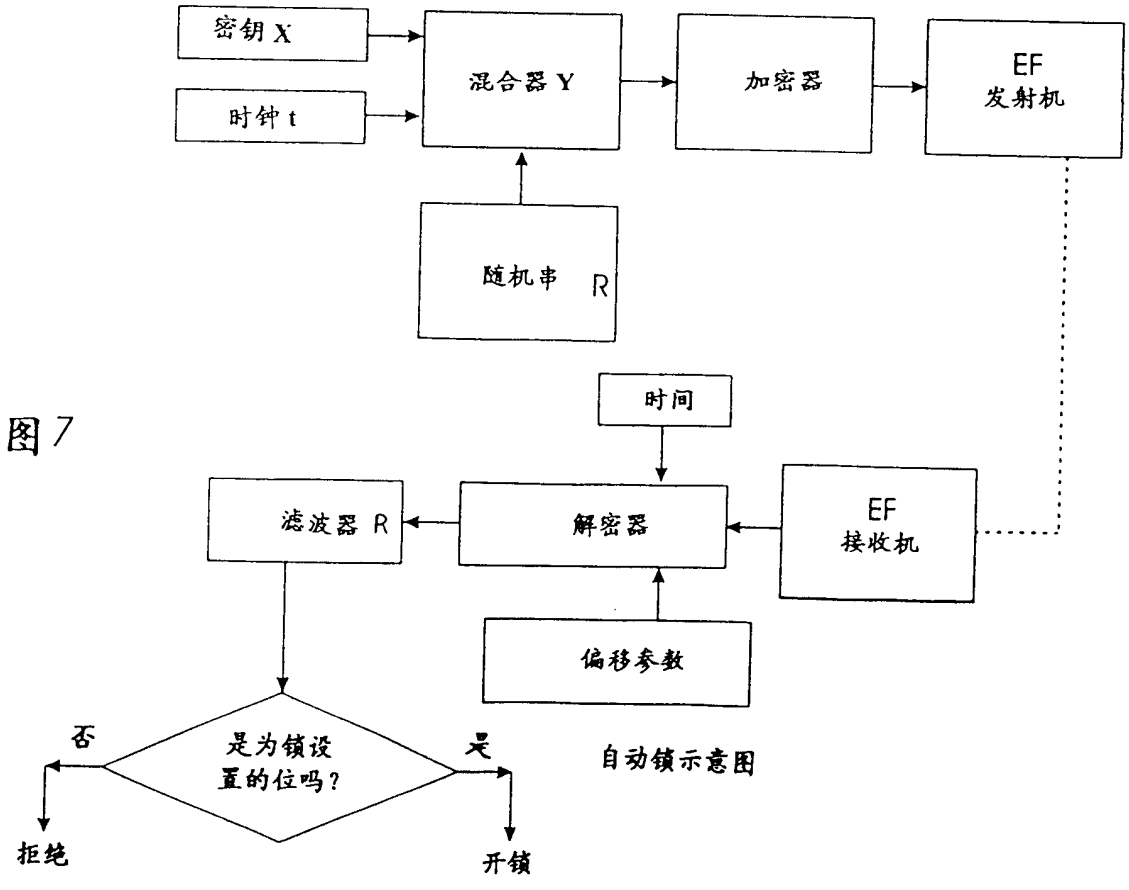

密钥 X
时钟 t
混合器 Y
加密器
EF
发射机
随机串 R
时间
滤波器 R
解密器
EF
接收机
偏移参数
否
是为锁设
置的位吗?
是
拒绝
开锁
自动锁示意图

图 7

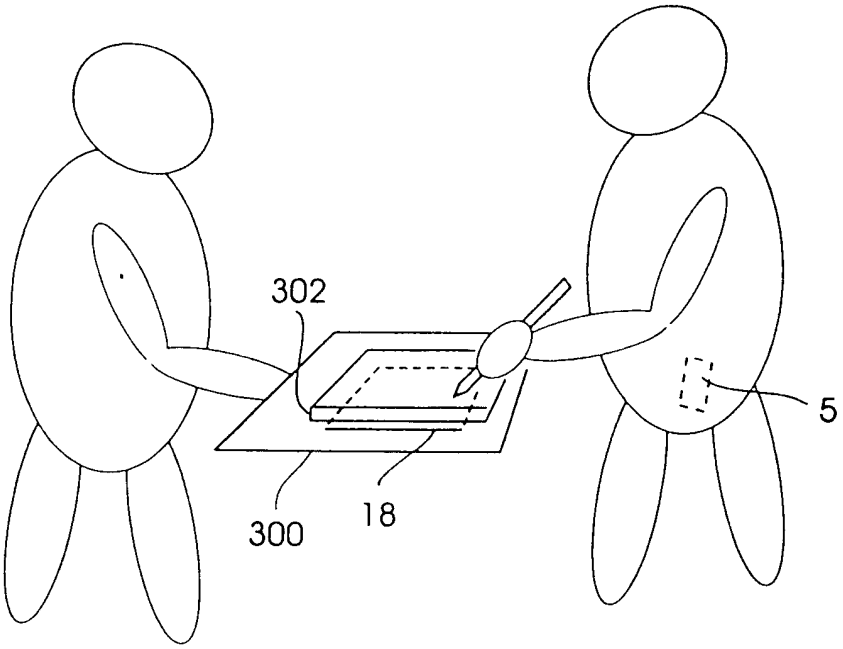


图8

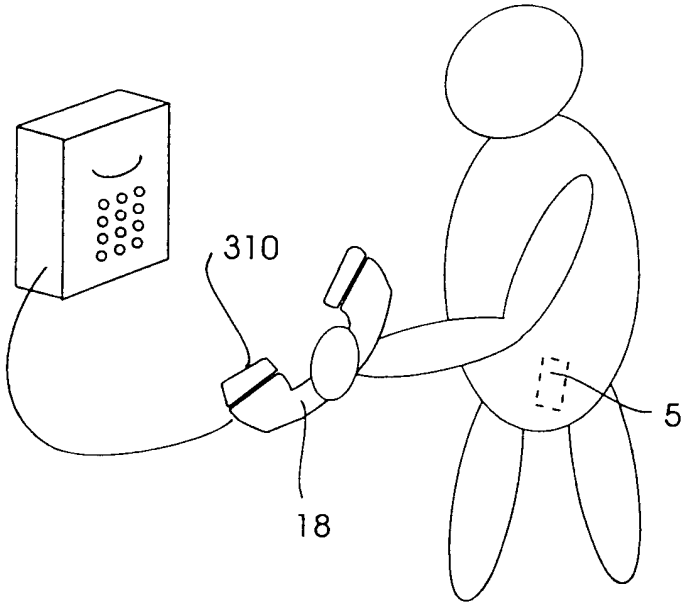


图9

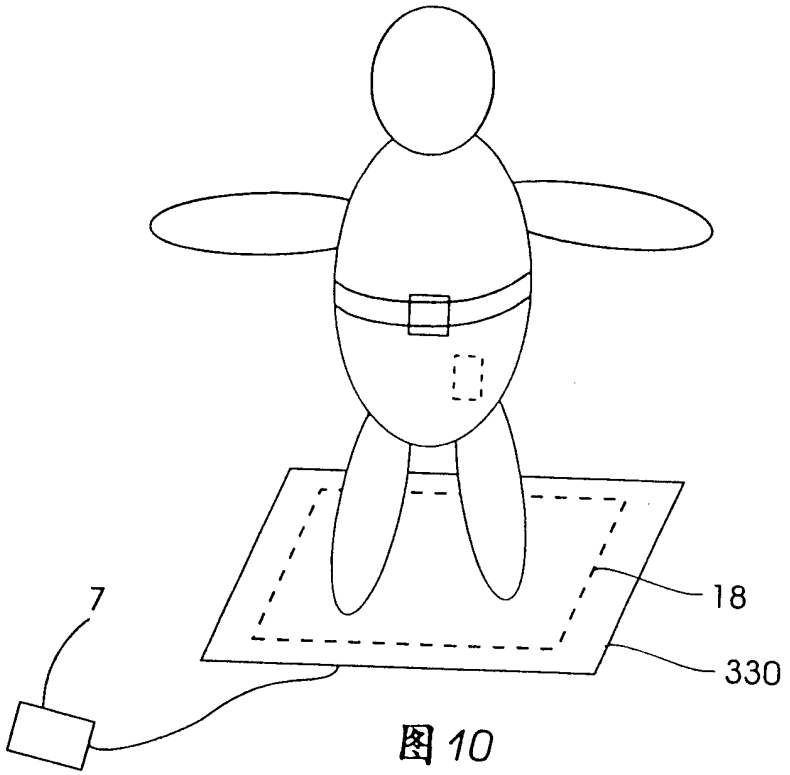


图 10

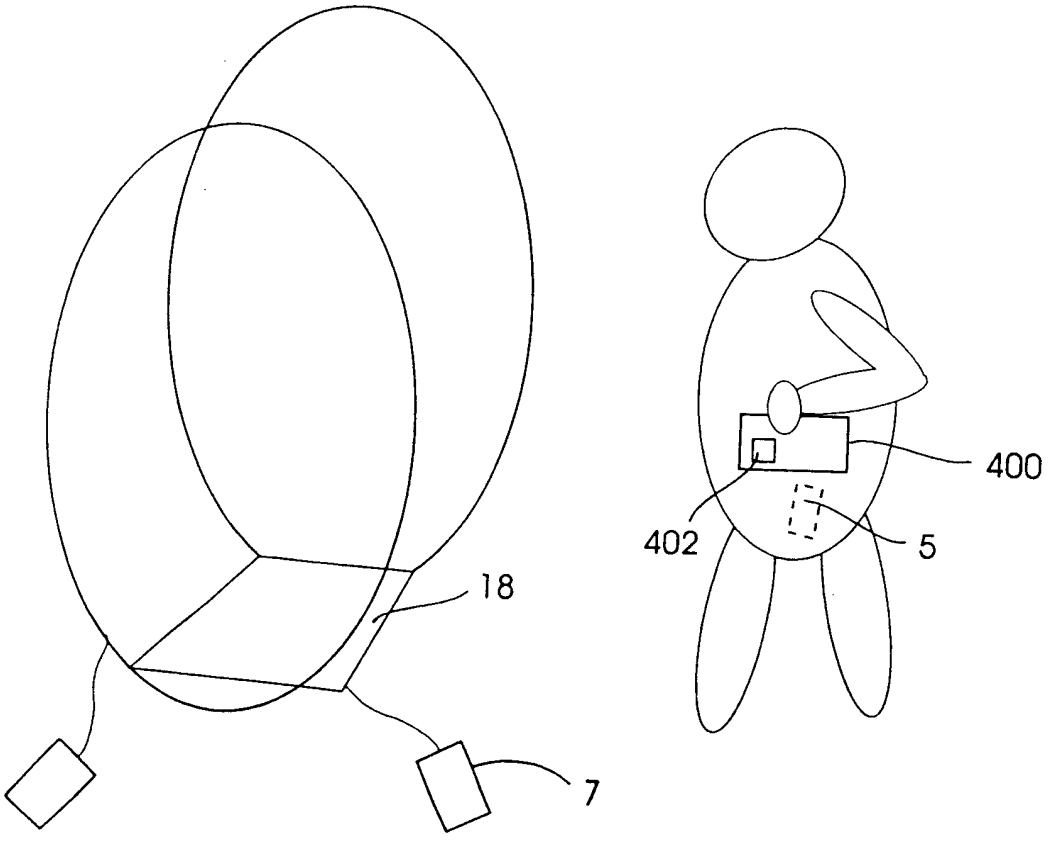


图 11

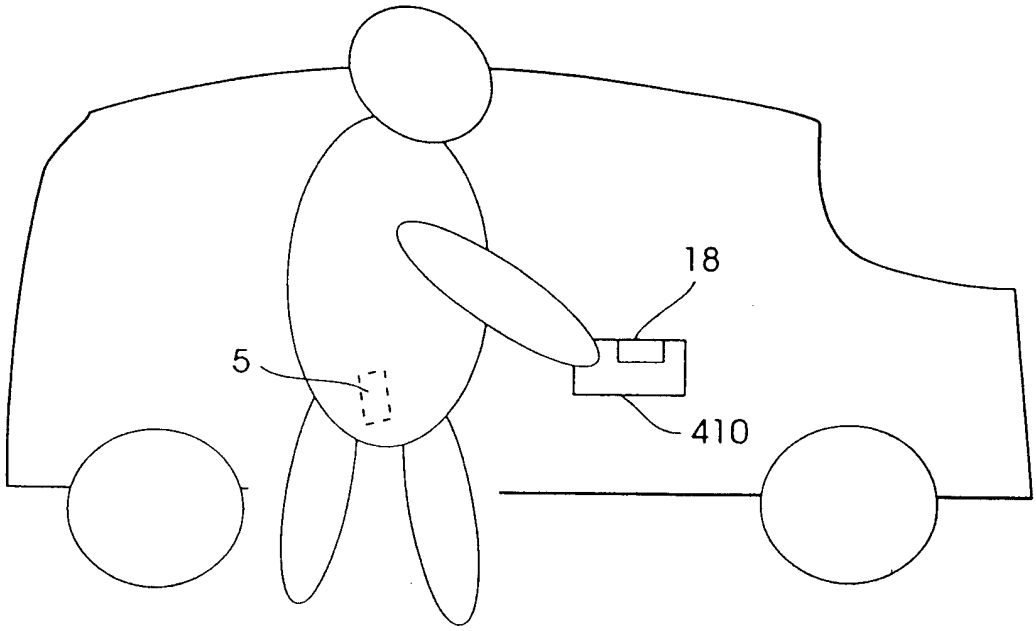


图 12

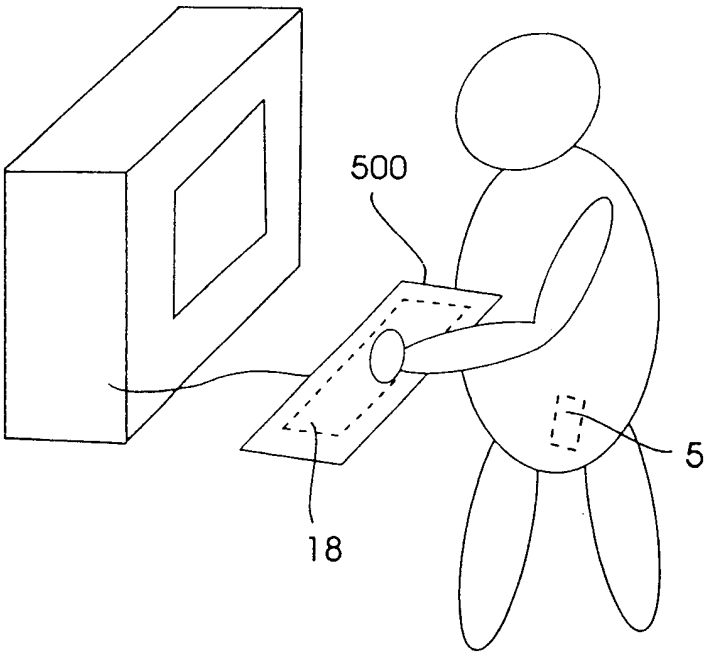


图 13

; 同步器的伪C代码

```
; Given T,PUBLIC_ID,CARD_SEQUENCE from the Card
; Determine if CARD_SEQUENCE is valid.

; CARD_SEQUENCE is the bit sequence transmitted from the Card to the Authenticator, representing
; the content of one of the two registers (Register B or Register C) in the card. The register is selected
; in the Card based on the LSB of Register A.
;
; The length, number, and location of taps of the Card registers (Register A, B, and C) are known
; to the authenticator, by table lookup, using the public identification (PUBLIC_ID) as an index. The
; authenticator does not know the content of registers A, B, and C.
;
; The SYNCHRONIZER uses three independent Feedback Shift Register (FSR), labeled FSR_A, FSR_B,
; FSR_C, with the length, number, and location of taps specified by table lookup, indexed by PUBLIC_ID.
; Feedback shift register (FSR) reference page 655-657 The Art of Electronics, Horowitz and Hill,
; Cambridge University Press, Second Edition 1989.
;
; The SYNCHRONIZER creates the content of the card register (Register B or C) and authenticates by
; comparing the content of the created register (FSR_B or FSR_C) to the received sequence
; CARD_SEQUENCE.

K=T/2-2(square root(T));              // define constant
A_COUNT=0;                            // number of times FSR_A LSB is one
AUTHENTICATION_VALID=0                // reset authentication results

for (=0;i <T;i++)                     // bring FSR_A up to time T
{       Clock FSR_A;
        if (FSR_A & 1)                // count number of times LSB of FSR_A is one
                A_COUNT++;
}
for (=0;i=K;i++)                      // bring FSR_B and FSR_C up to time K
{       Clock FSR_B;
        Clock FSR_C;
}
if (FSR_A & 1)                                  // LSB of FSR_A selects FSR
{       for (i=0;i<A_COUNT-K;i++)               // bring FSR_C up to time T
                Clock FSR_C;
        if (FSR_C=CARD_SEQUENCE)                // check for authentication
                AUTHENTICATION_VALID=1          // match so valid
}
else
{       for (i=0;i<T-A_COUNT-K;i+)              // bring FSR_B up to time T
                Clock FSR_B;
        if (FSR_B=CARD_SEQUENCE)                // check for authentication
                AUTHENTICATION_VALID=1          // match so valid
}
```

图 14

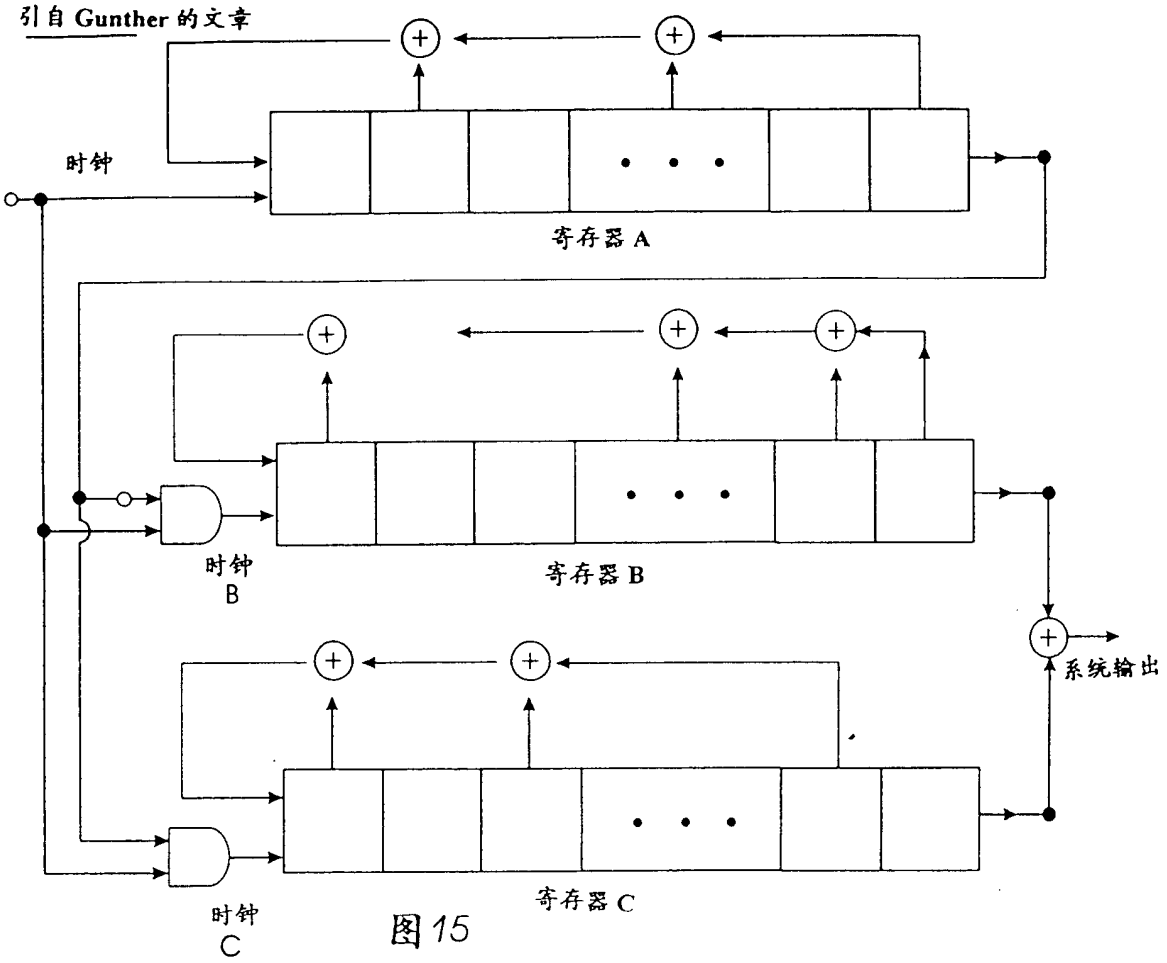
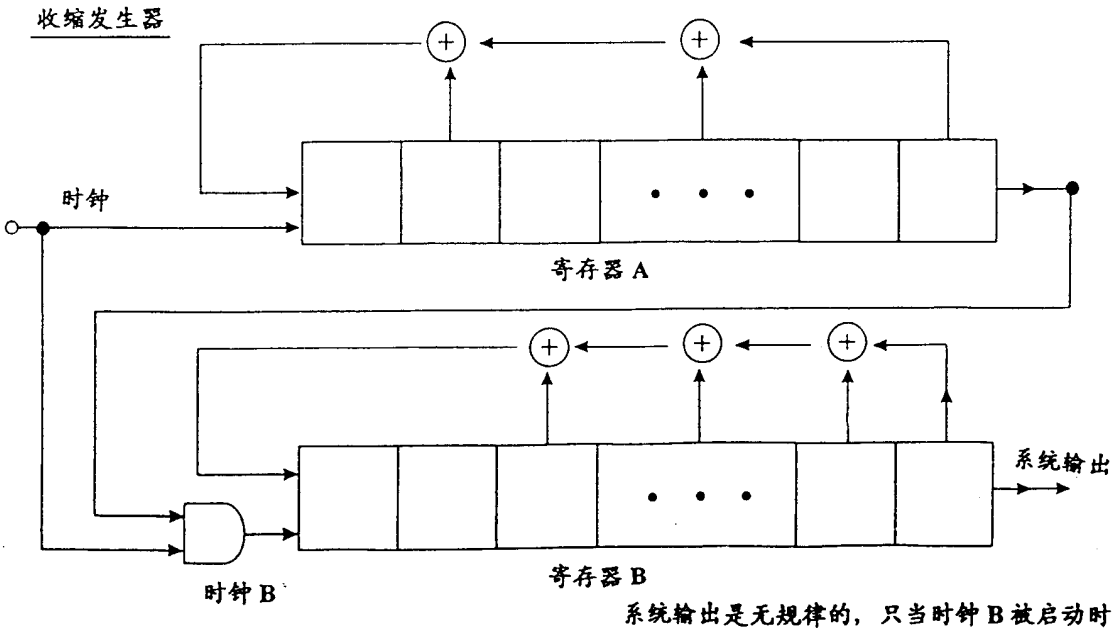


图 15



系统输出是无规律的，只当时钟 B 被启动时才产生系统输出。

图 16