[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06K 19/073 (2006.01)
G06F 1/00 (2006.01)
G07F 7/10 (2006.01)

[12] 发明专利说明书

专利号 ZL 200580026938.X

[45] 授权公告日 2009 年 10 月 28 日

[11] 授权公告号 CN 100555316C

[22] 申请日 2005.5.31
[21] 申请号 200580026938.X
[30] 优先权
[32] 2004.6.9 [33] EP [31] 04102617.0
[86] 国际申请 PCT/IB2005/051768 2005.5.31
[87] 国际公布 WO2005/122071 英 2005.12.22
[85] 进入国家阶段日期 2007.2.8
[73] 专利权人 NXP 股份有限公司
地址 荷兰艾恩德霍芬
[72] 发明人 S·范里恩斯沃 J·R·布兰德斯
[56] 参考文献
EP0552392A1 1993.7.28
WO9512852A 1995.5.11
CN1433555A 2003.7.30
US5719560A 1998.2.17
US5237609A 1993.8.17
US5644638A 1997.7.1
审查员 张 岩
[74] 专利代理机构 中科专利商标代理有限责任公司
代理人 王波波

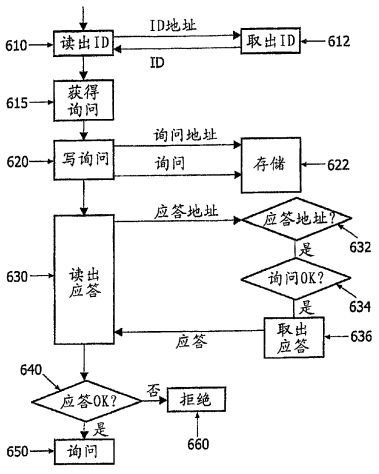
权利要求书 2 页 说明书 13 页 附图 6 页

[54] 发明名称

一次验证系统

[57] 摘要

一种验证系统，包括多个电子标签(120，122，124)，其中每个都与各自的唯一标识 ID 相关联。所述标签包括具有第一存储单元(222)和第二存储单元(224)的存储器(220)，其中所述第一存储单元用来存储预先计算的询问，所述第二存储单元用来存储与所述询问相关联的预先计算的应答。 所述第一存储单元(222)不能从标签外部读取。 存取电路(210)只在已经收到的与第一存储单元中所存储的询问相匹配的询问后才提供应答。 读出站(110)获得与标签相关联的标识。 接着，确定相应的询问并向标签发送所述询问。 从标签接收应答并通过比较所收到的应答和与所述询问相应的应答来验证标签的真实性。



1. 一种验证系统，包括多个电子标签和至少一个验证电子标签真实性的读出站；每个电子标签都与各自的唯一标识相关联，并包括：存储器，所述存储器包括第一存储单元和第二存储单元，其中第一存储单元存储预先计算的询问，第二存储单元存储与该询问相关联的预先计算的应答；第一存储单元不能从标签外部读取；以及存取电路，用于只响应于收到的与存储在第一存储单元中的询问相匹配的询问，提供存储在第二存储单元中的应答；

操作每个用于电子标签的读出站，以便：

获得相关联的唯一标识；

为标识确定相应的询问；

将询问发送给标签；

从标签接收应答；以及

通过对收到的应答和与所述询问相关联的应答进行比较来验证标签的真实性。

2. 根据权利要求 1 的系统，其中电子标签的存储器包括第三存储单元，用于存储与标签相关联的唯一标识；第三存储单元是只读型的；操作所述读出器，用于通过从标签的存储器中读出标识符来获取与电子标签相关联的唯一标识。

3. 根据权利要求 1 所述的系统，其中存储器包括存储询问的第四存储单元；第四存储单元可从标签外部写入；配置存取电路，用于响应从标签外部对第二存储单元的读取访问，比较第四存储单元中所存储的询问和第一存储单元中所存储的询问，并且只在比较后匹配的情况下，提供第二存储单元中所存储的应答。

4. 根据权利要求 1 的系统，其中第一和第二存储单元是一次写入型的；所述系统还包括用于电子标签的激活器，操作该激活器以便：

获取相关联的唯一标识；

为该标识确定相应的询问；

在电子标签的第一存储单元中存储该询问；

确定与该询问相关联的应答；以及

在标签的第二存储单元存储该应答。

5. 根据权利要求 1 或 4 的系统，其中采用至少对标识和密码密钥运行预定密码算法来确定所述标识的相应询问。

6. 根据权利要求 1 的系统，其中配置所述存取电路；用来提供从标签外部对第二存储单元中所存储的应答的最多一次的访问。

7. 根据权利要求 1 所述的系统，其中所述存储器包括多对存储单元；每对包括存储预定询问的各自的第一存储单元和存储与同一对中的第一存储单元中的询问相关联的预定应答的各自的第二存储单元；每个第一存储单元都不能从标签外部读取；配置存取电路，用来响应收到的与一对中的第一存储单元中所存储的询问相匹配的询问，提供存储在同一对中的第二存储单元中的应答。

8. 根据权利要求 6 或 7 所述的系统，其中按顺序配置所述存储单元对，并且操作存取电路从存储器对中的第一对开始，每次响应于收到的询问提供应答时，就为随后的存取操作按顺序选择下一对。

9. 一种电子标签，用于如权利要求1所述的验证系统，所述电子标签与唯一标识相关联，并包括：存储器，所述存储器包括第一存储单元和第二存储单元，其中第一存储单元用于存储预先计算的询问，第二存储单元用于存储与所述询问相关联的预先计算的应答；所述第一存储单元不能从标签外部读取；以及存取电路，用来只响应收到的与第一存储单元中所存储的询问相匹配的询问，提供在第二存储单元中所存储的应答。

一次验证系统

技术领域

本发明涉及一种验证系统，包括多个电子标签和至少一个验证电子标签真实性的读出站。本发明还涉及用于这种系统中的电子标签。

背景技术

目前，智能标签系统得到了广泛应用，从公共运输、公路通行税以及乘客车票到航空行李标记。预期将来会有更多商品需要配置智能标签，诸如服装或超市的商品。在这类应用中，标签读出器和智能标签之间以非接触的方式进行通信愈加频繁。这就提高了处理时间以及准确性并降低了排队的时间。这种标签有时也被叫做RF-ID(射频识别)。

市场上各种智能标签的硬件性能差异很大。有些电子标签只能存储可由标签读出器读出的数据（相当于条形码）。这种标签的一个例子是飞利浦半导体公司的MIFARE® ultralight。这种标签可以使用不同类型的存储器，包括只读、一次写入、以及可重写（例如，EE-PROM闪存）存储器。其他标签提供了先进的密码保护。例如，飞利浦半导体公司的MIFARE®PROX系列就是基于安全的8位80C51核心。其提供了具有定制参数的复杂的存储器保护机制，以便保护片上存储器，还提供了先进的存储器管理单元，以便保护应用的安全。MIFARE®PROX IC基于高度集成的生产工艺以及设计方法，使芯片能经受得住任何物理分析。利用三重DES协处理器保护数据。MIFARE®PROX PKI控制器也包括优化了诸如RSA或ECC这样的公开密钥算法的嵌入式32位密码协处理器。

不同种类的智能标签之间处理能力的差异导致了成本上的明显不同。简单的标签所提供的保密性相对较低，因为数据没有用密码保护。这就使得诈骗团伙能够伪造/仿制真标签，例如，通过获取原始读出器和标签，从标签读出数据并观察读出器和标签之间的交互。因而仿制真标签相对来说比较简单，例如，利用配置诸如天线这样的硬件的PDA（个人数字助理）以及程序，其中天线用于与读出器进行RF通信，程序使PDA表现为真标签。如果使用这种伪造的标签所获得的优点变低

和/或检测的几率较高，就不值得这样做。通过象目测标签这样的附加的保密性测量，能够增加检测的几率。然而，这种检测系统大多相当费事并因此总是不太合适。

对于某些应用来说，简单标签所提供的保密性就不够了。另一方面，不能证明带有密码处理器的标签的附加成本是必要的。例如，象在足球比赛或流行音乐会的入场券这样的应用中的情况。在这种应用中，电子标签能用于控制活动的入场，即，只有买了票的人才允许进入。另外，对保证每个人安全的保密性要求相当严格。

一种进行验证的公知方法是利用密码询问－应答协议。这需要在标签读出器和智能卡本身处执行一种（或多种）密码算法。这样做将使简单的智能标签变成复杂的、价格更贵的智能标签。

发明内容

本发明的一个目的是提供一种验证系统以及这种提出的能够区分伪造的和真的智能标签的电子标签，即在标签中不需加密处理器就能验证标签。本发明的又一个目的是提供一种用于这种系统的电子标签。

为了实现本发明的目的，验证系统包括多个电子标签以及至少一个用于验证电子标签真实性的读出站；每个电子标签与各自的唯一标识相关联并包括存储器，所述存储器包括第一存储单元和第二存储单元，其中，第一存储单元用于存储预先计算的询问，第二存储单元中用于存储与该询问相关联的预先计算的应答；第一存储单元不能从标签外部读取；以及存取电路，用于只响应收到的与存储在第一存储单元中的询问相匹配的询问，提供在第二存储单元中存储的应答；操作每个用于电子标签的读出站，以便获取相关联的唯一标识；为标识确定相应的询问；将询问发送给标签；从标签接收应答；并通过对收到的应答和与所述询问相关联的应答进行比较来验证标签的真实性。

基于密码询问－应答系统，通过向智能标签添加可执行的简单的验证协议，标签读出器能够区分伪造的智能标签和真的智能标签。密码检查所需的值是预先计算的并存储在标签中。这些预先计算的值必须保密以起到验证作用。为了防止智能标签意外泄漏保密数据，只在读出器发给智能标签正确的询问的情况下，智能标签才发送应答。因此恶意读出器不能容易地获得应答以生成标签副本。所述询问基于与标

签相关联的唯一的标识（ID）。通过确保只有真正的读出器能够生成该 ID 的询问，实现了智能标签和标签读出器两者的相互验证。在所述标签中不需要密码处理，这就使得标签的成本很低。通过传统的询问－应答协议，所述应答能够与询问相关联。在询问和应答之间还可以有其他关联。例如，两者都可以是随机数。随机数存储在标签中，读出器对随机数进行访问并能根据标签 ID 确定它们。

所述系统给出了密码保密性的常规级别:与给定 ID 相关联的第一标签是真的。通过窃听标签和读出器之间的通信，随后就能制造/仿制假标签。如果标签只能用一次（例如，在进入大门处），系统就能完全用密码保密。这很容易实现，例如利用入口系统记录哪些标签已经使用过并拒绝复制品（即，与同一 ID 相关联的标签）进入。对于保密需求中等的系统来说，能够接受可以在理论上产生一些复制品的情况。可以采取一些额外的步骤来降低这种情况发生的几率。例如，如果标签将用于重大活动的入口，第一个有效标签进入与最后一个人进入之间的时间非常有限，这就排除了大规模复制的机会。利用对标签进行简单的目测，能够降低利用诸如 PDA 等设备来仿制标签的几率。

根据从属权利要求 2 方法，电子标签的存储器包括存储与标签相关联的唯一标识的第三存储单元；第三存储单元是只读类型的；操作所述读出器，用于通过从标签的存储器中读取标识，获取与电子标签相关联的唯一的标识。以这种方式，读出器能够以简单可靠的方式获得唯一的 ID，并根据所述 ID 执行询问－应答。优选地，所述 ID 以不能篡改的方式（确保标签保持唯一性，在这种意义上讲，没有普通的标签能够例如通过写入 ID 被轻易地修改 为具备其他标签的 ID）在制造期间被载入标签。可以使用获取唯一 ID 的任何方案。作为制造绝对唯一的 ID 的另一种选择，标签还可以带有对于每组标签来说是唯一的分组 ID，例如，用于一个活动。通过添加更进一步的标识，诸如在集合内能唯一标识标签的序列号，能够使这种分组标签绝对唯一。这种附加 ID 可以写入标签中，随后以只读形式锁定带有该附加 ID 的存储单元。两个 ID 的组合能够产生对于所有集合的所有可能标签来说都是唯一的 ID。

根据从属权利要求 3 的方法，所述存储器包括存储询问的第四存储器单元；第四存储单元可从标签外部写入；配置存取电路，用来响应

于从标签外部对第二存储单元的读取访问，比较第四存储单元中所存储的询问和第一存储单元中所存储的询问，并只在所述比较后认为匹配的情况下提供存储于第二存储单元中的应答。在这种配置中，标签完全像个存储器，这就使得操作非常简单。将询问写入存储单元并从存储单元读取应答。只有在写入的询问与已经存储的询问相匹配时，预先计算的询问才是真正提供的应答。

根据从属权利要求 4 的方法，第一和第二存储单元是一次写入型；所述系统还包括用于电子标签的激活器，操作该激活器以便：

获得相关联的唯一标识；

为标识确定相应的询问；

在电子标签的第一存储单元中存储询问；

根据预定密码算法确定与询问相关联的应答；以及

在标签的第二存储单元中存储应答。

通常，在制造期间已经激活了。在优选实施例中，激活是单独的步骤，例如针对每个活动进行激活。在这种情况，对于每个活动都可选择相关联的询问－应答对。例如，利用一个认为保密的询问－应答算法，为每个活动选择不同的密钥。在这种方法中，每个活动中 ID 都是唯一的（即，用于一个目的的标签集），这就足够了，询问－应答算法能够使应答对于该活动和询问来说是唯一的。应该理解，询问应该一次写入而应答如上所述那样可有条件的读取。这能够通过在存储单元中存储询问和应答来实现，所述存储单元对于不需要的操作能够由激活器锁定。优选地，响应写入存储单元中的值来自动锁定。在这种方法中，能够降低由于不完全激活所述询问和/或应答就可读取的几率。

根据从属权利要求 5 的方法，利用至少对标识和密码密钥运行进一步的预定密码算法，确定标识的相应询问。这不仅产生了保密询问还能够只在读出器中存储这种算法和密钥以使读出器能够被系统的所有标签操作。密码还能用来产生两个唯一数（询问和应答），例如通过产生两个伪随机数，利用这些数来作为询问和相关联的应答。一种存储所述算法和密钥的可选方法（例如，利用表格）是在与 ID 相关联的系统中存储所有可能的询问（或者甚至是所有的询问－应答对）。对于具有大量标签的系统来说，后一种方法需要更多的存储器。优选地，

能够以保密方式，例如利用密码智能卡，执行任何敏感数据/操作。

根据从属权利要求 6 的方法，配置存取电路，用来提供从标签外部对第二存储单元中所存储的应答最多一次的访问。在这种方法中，产生了用密码保密的一次验证系统。应该理解，对于某些系统来说，不需要如此严格的要求。这种系统可以使用计数器（例如在读出器和/或标签中），这就把使用次数限制到了预定的次数，例如 3 次。这种系统不是完全保密的（不能防止被假标签在实际上执行标签的第二次或进一步的使用），但是，在考虑到了其他条件（例如，目测、活动的有限期限等等）的同时，在某些应用中能够被接受。

根据从属权利要求 7 的方法，存储器包括多对存储单元；每对包括存储预定询问的各自的第一存储单元和成对存储预定应答的各自的第二存储单元，其中所述预定应答与同一对中的第一存储单元中的询问相关联；每个第一存储单元都不能从标签外部读取；配置存取电路，用来只响应收到与同一对中的第一存储单元中所存储的询问相匹配的询问，提供同一对中的第二存储单元中存储的应答。在该方法中，对于几个操作来说标签的产生都是保密的（因为有多少操作就有多少存储器对）。很多应用都能从这种标签中获益。一种用处可以是电子公共交通票，其能够在相同类型的行程中使用几次（每次都用掉一个存储单元对），或者使用区域机制，其中用户在每个区域支付一次。在后者的系统中，每个存储单元对都对应一个用户走过的区域。其他的很多应用也能从这种标签获益，例如，用户必须为所获得的每件商品/服务付钱时。例如，用户每次在酒吧购买饮料时使用一个存储器对。然后，用户在夜晚结束时在收款处结帐。收款处检查已经使用了多少存储单元并收取相应的费用。还能在预先付费的应用中使用这种标签，其中每次用户使用产品/服务时使用一个存储器对。高保密级别与低成本的标签相结合，这就展开了很多新的应用。

根据从属权利要求 8 的方法，按顺序配置存储单元对，并且存取电路是可操作的，从存储器对中的第一对开始，每次响应收到的询问提供应答时，就为随后的存取操作按顺序选择下一对。以这种方式，读出器不需管理哪个存储器对能够使用或者检查哪个存储器对未使用。标签自己处理。应该理解，标签所需的任何数据（例如，账户）都必须保密存储在标签中，防止从标签外部重新写入。

为了实现本发明的目的，在验证系统中使用的电子标签与唯一的标识相关联，并包括：

存储器，包括第一存储单元和第二存储单元，其中第一存储单元用来存储预先计算的询问，第二存储单元用来存储根据预定密码算法对应于所述询问的预先计算的应答；第一存储单元不可从标签外部读取；以及

存取电路，用于只响应收到与第一存储单元中所存储的询问相匹配的询问，提供第二存储单元中所存储的应答。

附图说明

通过下面描述的实施例本发明的这些和其他方面是很清楚的。

在附图中：

图 1 示出了根据本发明的系统的方框图；

图 2 示出了根据本发明的电子标签的实施例的方框图；

图 3 示出了根据本发明的读出站的实施例的方框图；

图 4 示出了根据本发明的电子标签的第二实施例的方框图；

图 5 示出了能够用于读出站的表格；

图 6 示出了优选实施例的流程图；

图 7 示出了根据本发明的系统的实施例的方框图；以及

图 8 示出了根据本发明的电子标签的第三实施例的方框图。

具体实施方式

图 1 示出了根据本发明的系统 100 的方框图。所述系统包括读出站 110 和多个电子标签（表示为 120，122，和 124）。如果需要，可以采用不止一个读出站。读出站和电子标签可以彼此通信。数据能够双向交换。优选地，象飞利浦的 Mifare 系统一样，以从无线/非接触 ID 卡所获知的方式或与无线/非接触式 ID 卡相类似的方式进行无线/非接触式通信。在这种系统中，读出站和标签都配置天线。通常，读出站还通过天线向标签提供电源。有利的是，采用了允许多个标签在读出站附近而不阻塞通信的通信技术。这种通信系统和通信技术是公知的，并不是本发明的主题，但是可以将其用于根据本发明的系统。如果需要，所述通信还可以基于进行接触的方式，例如采用传统的智能

卡接触。因此，可以使用基于非接触式或接触式的通信系统作为选择或者二者同时使用。

图 2 示出了根据本发明的电子标签 200 的方框图。应该理解，只有与本发明相关的元件才显示得更加详细。诸如天线、电源电路、通信电路等等的元件采用方框 230 示出并且是完全公知的。每个电子标签 200 都包括存储器 220。存储器 220 包括第一存储单元 222 和第二存储单元 224，其中第一存储单元 222 存储预先计算的询问，第二存储单元 224 存储与所述询问相关联的预先计算的应答，例如基于预定密码询问－应答算法，或者利用通过系统彼此相关联的两个（伪）随机数。标签 200 还包括存取电路 210，用于只响应收到与存储在第一存储单元 222 中的询问相匹配的询问，提供存储在第二存储单元 224 中的应答。存取电路 210 可以采用任意合适的方式实施。例如，标签可以由命令驱动。一旦收到带有作为参数的询问的“提供应答”命令，存取电路就可以使用比较器根据存储单元 222 中的询问检查收到的参数。如果匹配，就使用常规读出电路从存储单元 224 读出应答值，并将其作为对命令的应答提供。命令解码/应答编码可以是存取电路的组成部分或者在标签 200 的不同部分中。命令/应答的编码/解码是公知的，因此不再进一步描述。第一存储单元 222 不能从标签外部读取。例如，这可以采用例如保证存储单元不被连接/切换到标签之外的接口的任一合适的方式实现。优选地，存取电路 210 还负责控制第一存储单元的存取，例如使用状态机。这种状态机使用永久存储的状态参数来操作。为此，存储器 220 可以扩充几位来存储这些状态。应该理解，所述数据需要存储尽可能长的时间。为此目的，优选使用非易失性存储器，诸如 EEPROM 或闪存。还可以使用其他合适的存储器类型，例如 MRAM。

图 3 示出了典型读出站 300 的方框图。方框 310 示出了诸如天线、电源电路、通信电路等元件，用于与电子标签通信和有选择地为其供电。象这样的方框 310 是图 2 的方框 230 的对应部分。这种元件是完全公知的，因此将不再进一步描述。例如，读出站 300 通过执行所选的询问－应答协议或者通过检查收到的应答是否与根据系统与所述询问相关联的应答相匹配来提供询问－应答验证。为此目的，读出站 300 可以配置在合适的程序控制下运行的处理器 320。可以使用任一合适的处理器，例如象个人电脑中所用的处理器。所述程序可以存储在存储

器 330 中，例如硬盘、光学存储介质（例如，CD-ROM，DVD-ROM，DVD+RW 等等），诸如 ROM、闪存或其他合适的非易失存储器的固态存储器中。重要的密码计算和数据（例如，密钥）优选在诸如密码智能卡的保密模块 340 中执行/存储。读出站本身可以基于传统计算机，诸如使用模块 310 和 340 增强的桌面 PC 或膝上型 PC。

每个电子标签都与唯一的标识（ID）相关联。这种 ID 的用处是使标签在系统范围内能够被唯一识别。这能够通过使用一般来讲对于每个标签是唯一的 ID 来实现。在图 4 的实施例中，这种 ID 存储于标签本身，在存储单元 402 中 。这就使得读出站能够很容易地获得 ID（例如，通过仅执行对应于存储单元 402 的预定存储地址的读取操作）。不能从外面对该存储单元进行写访问。原则上，所述 ID 能够被自由读取。优选地，在标签的制造期间，唯一的 ID 存储在只读存储器的一部分内的标签中。

所述 ID 不必是绝对唯一的。通常来讲，如果在使用标签的实际系统（例如，在使用标签的场合中）范围内所述标签是唯一的，这就足够了。可以使用其他测量手段，以便确保标签只能用于一个系统中（例如，在标签上使用可视标识）。在优选实施例中，密码技术用来确保即使在一个系统内标签是唯一的，询问通常也是唯一的。例如，ID 在对于系统来说是唯一的密钥的控制下被加密。接着，询问基于被加密的 ID。可以使用任意合适的加密系统。可以随机选择密钥或者利用合适的伪随机发生器。

通过组合两个（或多个）字段，还可以生成绝对唯一的 ID。第一字段能够用于识别系统/应用，并能够在制造期间进行设置，生成一批相同的标签。第二字段可用于存储在系统/应用范围内是唯一的标识符。可以在之后的阶段写入所述字段。因此，这种字段必须是一次写入型（或者看起来在存取电路的介入过程中是一次写入型的）。

从标签内的存储器中获得 ID 是比较方便的，因为这就使得读出站实现了全自动并快速验证。如果需要，可以以其他方式获得与标签相关联的唯一 ID 。例如，可以将 ID 以可视可读取方式印刷在标签上（例如，使用数字或条形码）。ID 还可以是标签持有者的标识符，例如护照或驾驶证上的标识代码。

读出站为电子标签获得相关联的唯一的标识（例如，通过从存储单

元 404 中读取）。接着，读出站为该标识确定相应询问。在密码询问－应答系统中，一方（验证者，即读出站）想要确认其他人的标识，就将消息发送给另一方（持证人，即，电子标签）。所述消息叫做“询问”。对于所述询问来说，只有一个正确应答。当收到正确应答时，验证者就相信了另一方的标识。对于该系统的有效运行来说，每次执行协议时（还需要不同的应答），发布的询问必须不同，否则攻击者会很容易冒充持证人。可以使用公共密钥技术和对称秘密密钥技术来实施询问－应答系统。在第一种情况中，验证者需要事先知道持证人的公共密钥（例如，通过公共密钥证书得知）。在第二种情况中，验证者和持证人必须共享秘密密钥。所述验证是根据下述事实进行的，即持证人能够“解密”验证人的询问并根据私有/秘密密钥生成正确的应答。询问－应答系统的一个公知的例子，是 Guillon-Quisquater 标识协议（Philips 的美国专利 5,140,634）。可以使用这种算法，还可以使用其他合适的算法。一旦选定了询问－应答协议，系统的操作者就会知道询问需要的正确位数或者可由其选择。系统 100 能够生成足够数量的唯一询问，每个询问用于系统可能要用的每个标签。由此能够生成标签的 ID 与相关联的询问相匹配的表格。通过获得 ID，就能够由此从表格中读取相应的询问。在这种装置中，优选对这种表格进行保密存储（例如，在模块 340 中）。通过增加与询问相关联的应答，可以进一步对所述表格进行扩充。通过选择的询问－应答协议，应答可以被关联，但是还可以有其他的关联，诸如关联两个随机数。在图 5 中示出了这种表格。在表格中一个标签使用一行。第一个字段给出了与标签相关联的 ID。读出站一旦获得所述标签的 ID，就会使用该 ID 搜索整个第一列并查找相关的行。然后发送询问给标签。在该实施例中，能够从所确定行的第二列获得询问。如果标签认为所述询问是可接受的，读出站就能够从标签收到应答。接着读出站通过对收到的应答和根据所选密码询问－应答协议与所述询问相对应的应答进行比较，验证标签的真实性。利用图 5 中的表格能够仅仅从行的第三字段取出想要的（可接受的）应答。

图 4 也示出了优选实施例，其中存储器 220 包括第四存储单元 404，用于存储询问。第四存储单元 404 可从标签外部写入（实际上由读出站）。配置存取电路 210，用来响应于从标签外部对第二存储单元 224

的读取访问，对存储于第四存储单元 404 的询问和存储于第一存储单元 222 的预先计算的询问进行比较，并只在比较认定匹配的情况下，提供存储于第二存储单元 224 的应答。通过这种方式，读出站将电子标签只看作普通的存储器。本领域技术人员能够很容易地设计出这种存取电路。

图 6 示出了上述实施例的读出站（左边）和标签（右边）中的操作和数据的交换的示意性流程图。在该实施例中，通过从标签中读出标识符，读出站在步骤 610 中获得唯一的标识符。将存有 ID 的存储单元的地址（ID addr）发送给标签。在步骤 612，标签取出所存的标识符（ID），并将 ID 传回。例如，整个操作可以是常规的存储器读取操作。在步骤 615，读出站获得与 ID 相关联的询问。如图 5 中所示，通过从表格中读出来实现该步骤。或者，可以利用对标签 ID 进行的加密功能以及存于读出站内部的保密密码密钥 k，由读出器即时地（on-the-fly）计算出所述询问。在这种实施例中，读出站不必存储询问和相应的应答的长长的列表，而只需保持密钥 k 的保密状态。可以使用诸如标准分组密码算法 Triple DES 或者 AES 等任意合适的密码算法 。在步骤 620，读出站向标签提供询问，在该实施例中以存储器写操作的形式：提供用来存储所提供的询问的存储单元地址（cha1 addr）并提供实际的询问值（cha1）。在步骤 622，标签存储该值。在步骤 630，读出站设法从标签中取出应答，在该实施例中以从标签中读出的方式。将持有应答的存储单元地址（Resp addr）发送给标签 。所述标签由对应答地址的读取操作触发。如上所述，仅仅有条件地提供应答。由存取电路 210 进行该测试。在该实施例中，测试 632 所示出的是，检查所提供的地址是否为持有应答的存储单元的地址。如果是，在步骤 634，检查在步骤 622 收到的询问是否与在单元 222 中存储的预先存储的询问相匹配。若匹配，标签就从单元 224 中取出预先存储的应答，并在步骤 636 传回应答。在步骤 640，读出站检查收到的应答是否与预期应答匹配（根据预定的询问－应答协议）。如图 5 所示所述预期应答可以是预先计算的或者利用所述协议即时生成的。如果收到的应答与预期应答相匹配，就认为标签是真的，并针对该标签进行诸如同意访问某活动等的下一步骤 650。如不匹配，在步骤 660 拒绝该标签。

图 7 示出了根据本发明的系统的又一实施例的方框图。在该实施例

中，唯一的标识符已经与标签相关联（例如，在制造过程中就已经存于标签中）。在该实施例中，系统包括激活器 710。激活器 710 还对标签“编程”。每个活动/应用都可以使用专用激活器 710。激活器 710 获得与唯一的标识相关联的电子标签，例如通过从存储单元 402 将其读出。为此，激活器 710 还需要硬件/软件，以便与标签通信，并且只要可用就可向标签供电。然后，激活器 710 为标识确定相应的询问。所述询问必须适合所选择的询问－应答协议（如果完全使用的话）并可以随机选择。接着，激活器在电子标签 200 的第一存储单元 222 中存储询问。所述存储单元优选是一次写入型。可以使用任意合适的一次写入型实施方式。如果需要，存取电路 210 中的状态机可以用来记录单元 222 已经被写入以及锁住对该单元的任何进一步的读和写访问。激活器 710 还确定与询问相关联的应答（例如，根据预定询问－应答算法）。激活器 710 在标签的第二存储单元 224 中存储计算的应答。优选地，该存储单元 224 也是一次写入型。激活器 710 为系统的每个标签向读出站 110 提供下列信息：ID 和询问。如果读出站本身不计算应答，激活器 710 优选还向读出站 110 提供应答。

优选地，配置存取电路，用于只提供一次从标签外部对第二存储单元 224 中所存储的应答的访问，确保最大的保密性。存取电路利用状态机来实现上述功能，其中所述状态机记录是否已经同意了对单元 224 中的应答的成功的访问。如果是，就一直拒绝再次访问。对于降低了保密需要的系统来说，可以同意更多数目的访问，例如三次。允许访问的最大次数可以存储在不能从外部写入的存储单元中（或者一次性设置数量）。计数器可以用来记录成功访问的次数并且达到允许的最大数量后状态机可以拒绝再次访问。

图 8 是出了根据本发明的系统的又一实施例的方框图，其中电子标签的存储器 220 包括多对存储单元。示出的是几对 810、820 和 830。每对的第一存储单元 812、822、832 用于存储预定的询问，而每对的第二单元 814、824 和 834 用于存储预定的应答。所述应答与所述询问相关联（例如，根据预定密码询问－应答算法）。类似于参照图 1 所描述的，第一存储单元 812、822、832 中的每一个都不能从标签外部读出。配置存取电路 210，用来只响应于收到的与存储在一对中的第一存储单元中的询问相匹配的询问，提供存储在同一对中的第二存储单

元中的应答。因此现在能够对每对执行和图 2 中所描述的一样的操作。所述对能够被看作是完全独立的，例如读出站将自由访问其选择的任意一个。这在下述应用中尤为有用，即所述对具有其自身特有的功能（例如，每一对提供对主要活动的不同区域的访问）并且没有规定顺序。

在优选实施例中，存储单元对按顺序地设置，因此按顺序地使用他们 。存取电路从同意提供对存储器对中的第一对的应答进行访问开始。每次响应于收到的正确询问提供应答时，存取电路都为随后的存取操作按顺序自动选择接下来的一对。

应该理解，询问和应答必须是合适的位数，以避免强制性的攻击。根据应用，技术人员能够选择合适的位数。影响它的因素是：在真正被使用之前标签对于攻击者的有效持续时间（例如，在活动前一个月发布标签）、标签的通信和处理速度，以及黑客能够并行分析的标签数。技术人员能够很容易地算出给出可接受的保密级别的位数。技术人员还将意识到预防定时攻击。在这种攻击中，攻击者向标签发送随机询问。标签处理该询问，包括比较该询问与所存储的预先计算的询问。如果应答时间取决于标签的处理（例如，匹配的位数），这就向攻击者提供了信息。提高应答时间可能意味着更多位是正确的。因此需要应答时间是固定的。密码电路领域的技术人员将会明白这些并知道如何设计出合适的电路。

应该理解，本发明还可以扩展成计算机程序，尤其是载体上或内的计算机程序，适于用来实施本发明。所述程序可以是下述形式，即源代码、目标代码，以及诸如部分编译形式的中间源和目标代码，还可以是适于在本发明方法的实施中使用的其他形式。所述载体可以是任何能够承载程序的实体或装置。例如，所述载体可以包括存储介质，诸如 ROM，例如 CDROM 或半导体 ROM，或者磁性记录介质，例如软盘或硬盘。此外，所述载体可以是能够由无线或其他装置通过电缆或光缆传送的诸如电或光信号的可传输载体。当所述程序以这种信号实现时，载体可以由这种电缆或其他装置或手段构成。或者，所述载体可以是嵌入了程序的集成电路，所述集成电路用于执行相关方法或者在相关方法的执行中使用。

应该注意到，上述实施例是对本发明的说明而不是限制，在不脱离

所附权利要求的范围内，本领域的技术人员能够设计出很多可替换的实施例。在权利要求中，放入括号中的所有附图标记不应被解释为对权利要求的限制。动词“包括”及该动词的变化形式的使用并没有排除权利要求所陈述的元件和步骤之外的元件和步骤。元件前面的冠词“一”并没有排除多个这种元件的存在。本发明可以利用由几个不同元件构成的硬件实施，还可以利用合适的程序控制计算机来实施。在列举了几个元件的装置/系统权利要求中，这些元件中的几个可以被做成同一个硬件。在不同的从属权利要求中相互引用某些方法，并不是指这些方法的组合不利于使用。

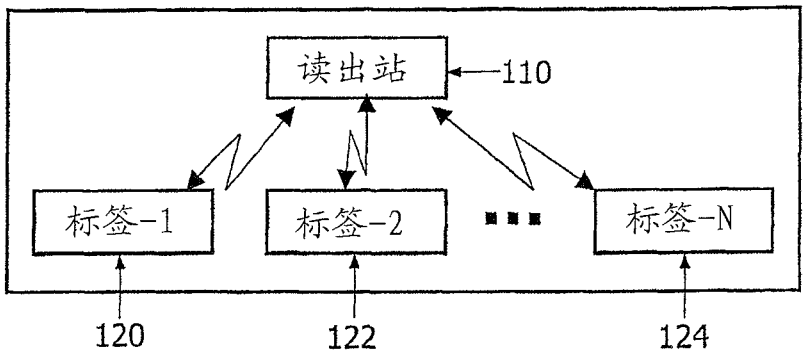

读出站
110
标签-1
标签-2
标签-N
120
122
124

图 1

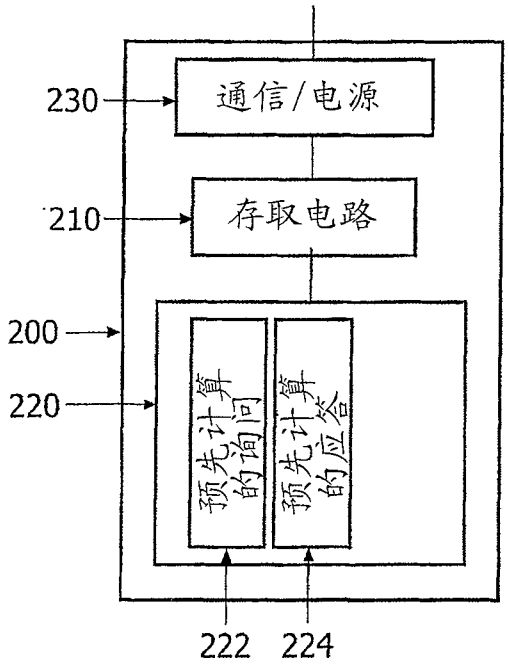

230
通信/电源
210
存取电路
200
220
预先计算的询问
预先计算的应答
222
224

图 2

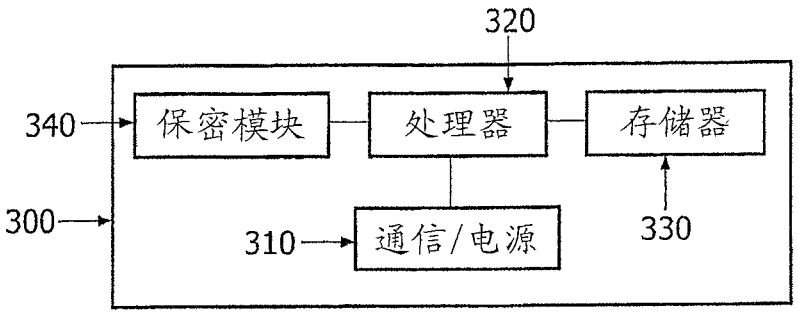

320
340
保密模块
处理器
存储器
300
310
通信/电源
330

图 3

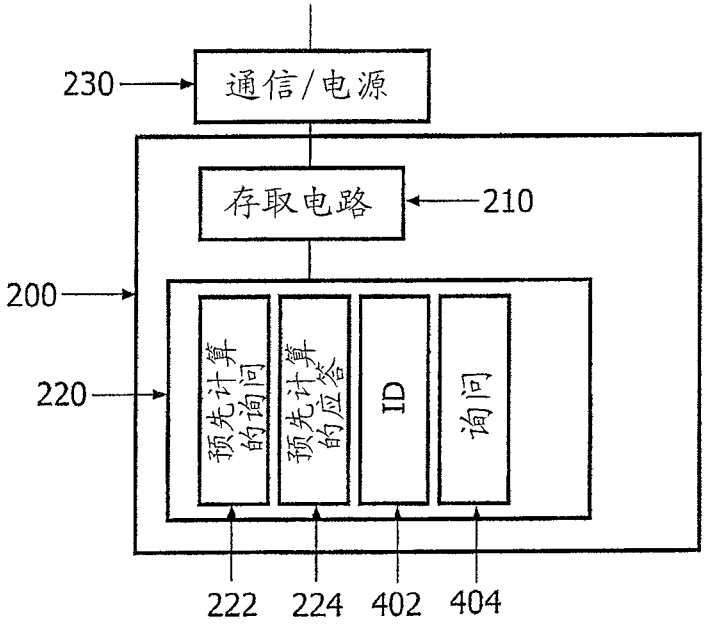

230
通信/电源
存取电路
210
200
220
预先计算的询问
预先计算的应答
ID
询问
222
224
402
404

图 4

ID-1	询问-1	应答-1
ID-2	询问-2	应答-2
ID-3	询问-3	应答-3
…	…	…
ID-n	询问-n	应答-n

图 5

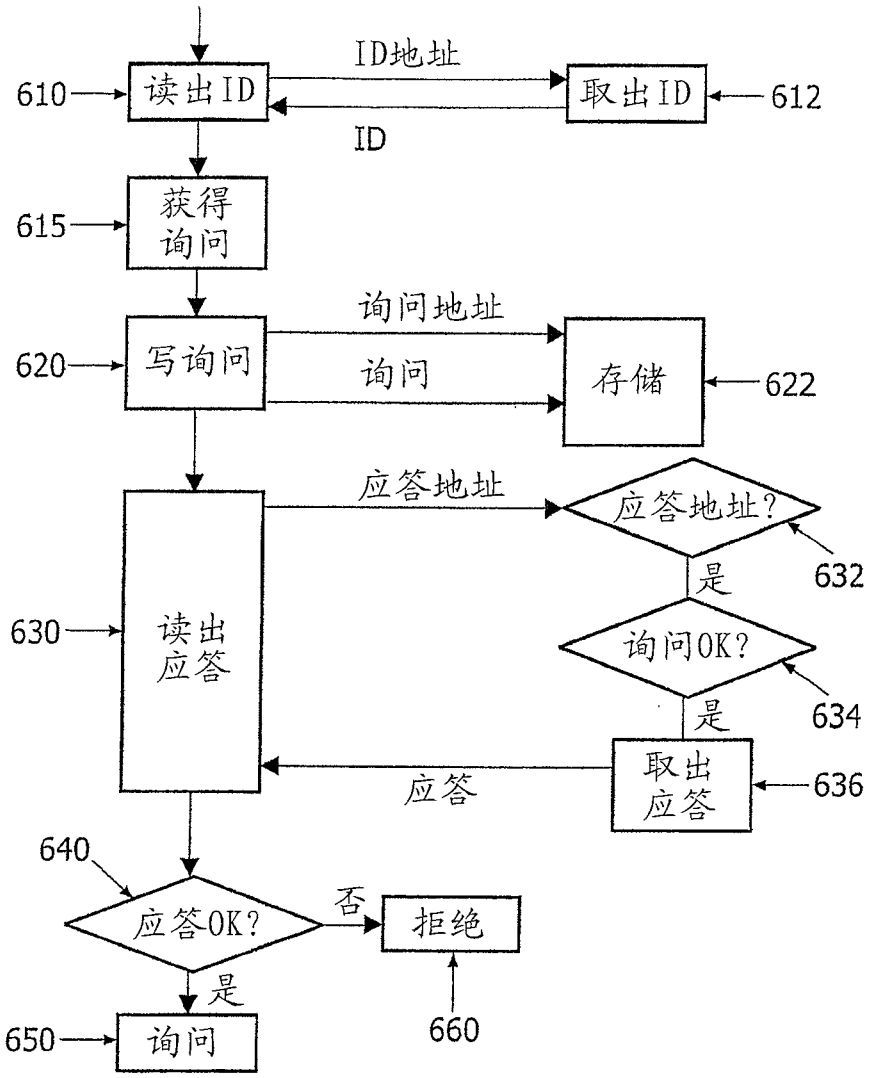

610
读出ID
ID地址
取出ID
612
ID
615
获得
询问
620
写询问
询问地址
询问
存储
622
应答地址
应答地址?
632
是
630
读出
应答
询问OK?
634
是
取出
应答
636
应答
640
应答OK?
否
拒绝
是
650
询问
660

图 6

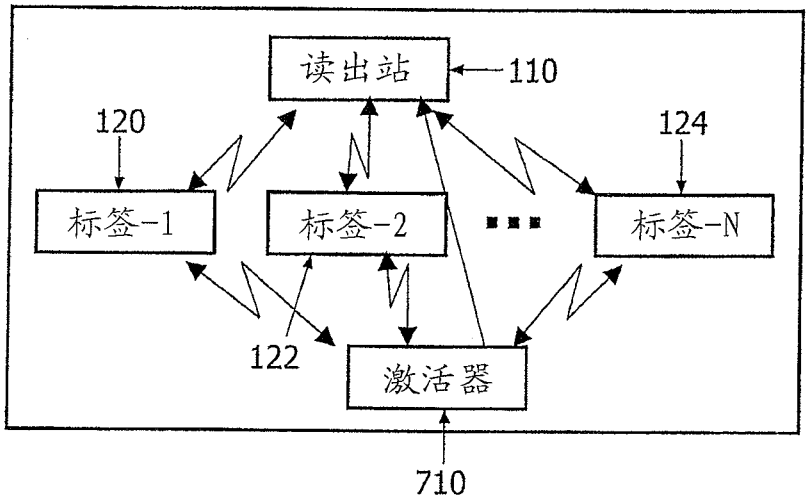


图 7

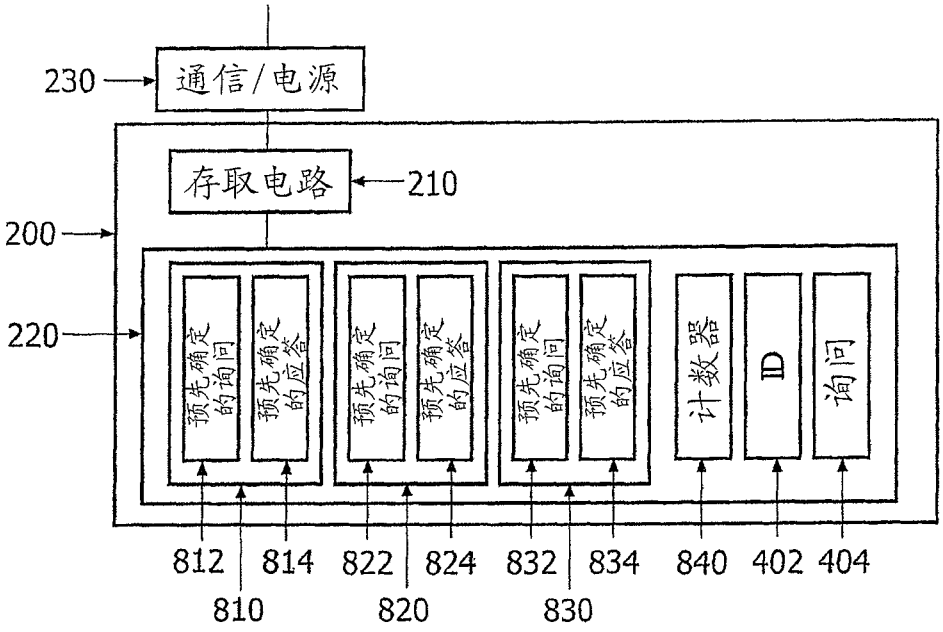

230
通信/电源
存取电路
210
200
220
预先确定的询问
预先确定的应答
预先确定的询问
预先确定的应答
预先确定的询问
预先确定的应答
计数器
ID
询问
812
814
822
824
832
834
840
402
404
810
820
830

图 8