(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 105190638 A
(43)申请公布日 2015.12.23

(21)申请号 201480013912.0
(22)申请日 2014.02.26
(30)优先权数据
61/784,276 2013.03.14 US
14/189,259 2014.02.25 US
(85)PCT国际申请进入国家阶段日
2015.09.11
(86)PCT国际申请的申请数据
PCT/US2014/018626 2014.02.26
(87)PCT国际申请的公布数据
WO2014/158596 EN 2014.10.02
(71)申请人 柯惠有限合伙公司
地址 美国马萨诸塞
(72)发明人 P·F·克拉默 W·G·帕特森
(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 11038
代理人 金晓
(51)Int.Cl.
G06F 21/30(2006.01)
G06K 19/07(2006.01)

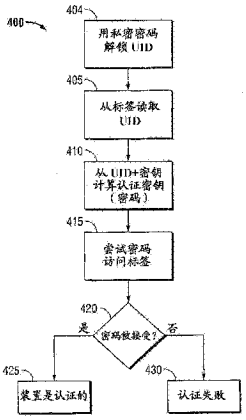
权利要求书3页 说明书9页 附图6页

(54)发明名称

RFID安全认证

(57)摘要

本公开描述了用于其中每个装置均与RFID标签相关联的多个装置的认证系统和方法。对于每个装置，密钥与公开可读的RFID标签的唯一识别码(UID)加密地结合以获得唯一的授权签名。利用唯一的授权签名作为存储器访问和/或标签操作密码制备RFID标签。所述系统和方法可以防范攻击从而单个标签的损害不会导致全部多个装置的损害，并且可以减少或消除在外科手术过程期间不适当的外科装置的使用。



CN 105190638 A

1.一种认证 RFID 标签的方法,包括 :

选择密钥 ;

制备所述 RFID 标签,其中制备所述 RFID 标签包括 :

从所述 RFID 标签读取唯一识别码 ;

从所述密钥和所述唯一识别码创建认证签名 ;和

将所述 RFID 标签的密码设置为所述认证签名 ;并且

认证所述 RFID 标签,其中认证所述 RFID 标签包括 :

从所述 RFID 标签读取所述唯一识别码 ;

从所述密钥和所述唯一识别码重建所述认证签名 ;

通过向所述 RFID 标签提供所述认证签名作为密码尝试访问所述 RFID 标签的功能 ;和

如果对所述 RFID 标签的功能的尝试访问是成功的,则判定所述 RFID 标签是认证的。

2.如权利要求 1 所述的认证 RFID 标签的方法,其中创建认证签名包括对所述密钥和唯一识别码 UID 执行散列函数以获得所述认证签名。

3.如权利要求 2 所述的认证 RFID 标签的方法,其中所述散列函数是从由 SHA-1 函数、SHA-1HMAC 函数、SHA-2 函数和 MD5 函数组成的组中选出的。

4.如权利要求 1 所述的认证 RFID 标签的方法,其中创建认证签名包括 :

连接所述唯一识别码 UID 和所述密钥以创建比特串 ;和

对所述比特串执行散列函数以获得所述认证签名。

5.如权利要求 4 所述的认证 RFID 标签的方法,其中所述散列函数从由 SHA-1 函数、SHA-1HMAC 函数、SHA-2 函数和 MD5 函数组成的组中选出的。

6.如权利要求 4 所述的认证 RFID 标签的方法,进一步包括 :

将所述认证签名分割为等长的多个比特串 ;

对所述多个比特串的第一个和所述多个比特串的第二个执行异或操作以获得中间结果或最终结果的至少一个。

7.如权利要求 6 所述的认证 RFID 标签的方法,进一步包括 :

对最新计算得到的中间结果和所述多个比特串中的随后一个执行异或操作以获得中间结果或最终结果的至少一个。

8.如权利要求 1 所述的认证 RFID 标签的方法,其中尝试访问的功能是从由读功能、写功能和读写功能组成的组中选出的。

9.一种用于制备在电外科手术中使用的外科器械的系统,包括 :

具有 RFID 标签的外科器械,其中所述 RFID 标签包括 :

唯一识别码,能够由制备单元读取 ;和

密码模块,被配置为存储密码和返回表明提供的密码是否等于所存储的密码的状态 ;和

制备单元,包括 :

RFID 通信单元 ;

处理器,可操作地耦合到所述 RFID 通信单元 ;和

存储器,可操作地耦合到所述处理器,存储密钥并具有一组指令,用于 :

读取所述外科器械的所述 RFID 标签的所述唯一标识符 ;

至少部分基于所述外科器械的所述 RFID 标签的唯一标识符和密钥产生认证签名 ;和

在所述密码模块中存储所述认证签名作为密码。

10. 如权利要求 9 所述的用于制备在电外科手术中使用的外科器械的系统，其中所述密码与所述 RFID 标签的功能相关联。

11. 如权利要求 10 所述的用于制备在电外科手术中使用的外科器械的系统，其中所述 RFID 标签进一步包括读写存储器，以及从由允许读写存储器可读、允许读写存储器可写和允许读写存储器可读写组成的组中选出所述 RFID 标签的功能。

12. 如权利要求 9 所述的用于制备在电外科手术中使用的外科器械的系统，其中所述 RFID 标签进一步包括读写存储器，并且其中所述指令组进一步包括被配置为初始化所述读写存储器内的数据结构的指令。

13. 如权利要求 12 所述的用于制备在电外科手术中使用的外科器械的系统，其中所述数据结构被配置为存储从由使用计数、生产日期、生产序列号、失效日期、校准数据、历史数据、认证数据和操作限制参数组成的组中选出的数据。

14. 如权利要求 9 所述的用于制备在电外科手术中使用的外科器械的系统，其中至少部分根据所述 RFID 标签的所述唯一识别码和所述密钥的加密散列产生所述认证签名。

15. 如权利要求 14 所述的用于制备在电外科手术中使用的外科器械的系统，其中所述加密散列从由 MD5 散列、SHA-1 散列、SHA-1HMAC 函数和 SHA-2 散列组成的组中选出。

16. 一种用于认证在电外科手术过程期间使用的外科器械的系统，包括 :

具有 RFID 标签的外科器械，其中所述 RFID 标签包括 :

唯一标识符，能够由认证单元读取 ;和

密码模块，存储密码并被配置为返回表明提供的密码是否等于所存储的密码的状态 ;和

认证单元，包括 :

RFID 通信单元 ;

处理器，可操作地耦合到所述 RFID 通信单元 ;和

存储器，可操作地耦合到所述处理器，存储密钥并具有一组指令，用于 :

读取所述外科器械的所述 RFID 标签的所述唯一标识符 ;

至少部分基于所述密钥和所述外科器械的所述 RFID 标签的所述唯一标识符产生认证签名 ;

向所述密码模块提供所述认证签名作为密码 ;和

接收表明所提供的密码是否等于所存储的密码的状态。

17. 如权利要求 16 所述的用于认证在电外科手术过程期间使用的外科器械的系统，进一步包括可操作地耦合到所述处理器的电外科产生器。

18. 如权利要求 17 所述的用于认证在电外科手术过程期间使用的外科器械的系统，其中如果所接收的状态表明所提供的密码不等于所存储的密码，则所述电外科产生器的操作被禁止。

19. 如权利要求 16 所述的用于认证在电外科手术过程期间使用的外科器械的系统，其中所述 RFID 标签进一步包括读写存储器并且其中所述指令组进一步包括配置为修改所述读写存储器内数据的指令。

20. 如权利要求 16 所述的用于认证在电外科手术过程期间使用的外科器械的系统，其中至少部分根据所述 RFID 标签的所述唯一标识符和所述密钥的加密散列产生所述认证签名。

RFID 安全认证

[0001] 背景

[0002] 1. 技术领域

[0003] 本公开一般涉及射频识别技术（也称为 RFID），并且更具体地，涉及用于不需要使用标签的读写存储器的 RFID 标签的安全认证的系统、设备和相关方法。

[0004] 2. 相关技术背景

[0005] RFID 是使用射频 (RF) 信号用于自动识别的方法。被称为 RFID 读写器的装置无线地读取并且可选地写入存储在以物理方式连接到物品（例如产品、包装或运输容器）的被称为 RFID 标签的应答器中的数据。通常地，RFID 标签包括两个主要部分：用于存储和处理数据并且用于调制和解调 RF 信号的集成电路 (IC)，和与芯片耦合以使得芯片在标签和读写器之间交换数据的天线。RFID 标签可以是只读的，其中所述 IC 包含不可变更的数据（例如由标签生产商不可消除地编码的用于唯一地识别标签的唯一识别码）。可选择地，RFID 标签可以是可读写的，其中存储的数据可以被修改或删除。然而，通常可读写 RFID 标签也会包含只读数据（例如不可消除的唯一识别码）以使得单个的标签可以被唯一地识别。可读写 RFID 标签的某些类型或型号（这里称为安全 RFID 标签）提供安全或保护特征或机制，以使得在一个或多个密码的成功通信时标签的读取和 / 或写入是可控的并且有条件的。在这些安全 RFID 标签中，密码存储在只写存储器中；也就是说，密码可以通过写操作设置或修改，但不能被任何读操作显示。为了使读写器在安全 RFID 标签中访问数据，任何读或写操作前必须有密码操作，其中标签对读写器提供的密码和标签存储的密码进行比较。所述安全 RFID 标签通常在它对密码操作的响应中表明密码比较的成功或失败。密码的成功匹配将暂时允许随后的读或写操作，直到标签由读写器故意地重置（在操作结束时）或者由当无源标签从读写器的附近移除时的断电意外地重置。

[0006] RFID 标签的特征是有源的或无源的。有源 RFID 标签包含电源（例如电池），而无源 RFID 标签由从 RF 读写器信号获得的能量供电。其结果是，无源 RFID 标签通常具有相对适中的处理和存储能力。一般但不是排他地，有源 RFID 标签被用于重工业、市政和军事应用中，而无源 RFID 标签被用于比较小的装置中（例如工具、电子装置和组件、信用卡 / 借记卡等）。有源 RFID 标签可以提供超过无源类型标签更大的范围。

[0007] RFID 标签可以用于多种目的。一个这样的目的是用于认证配件装置（例如外科手术器械）来确定所述配件或器械装置是否适合与主装置（例如电外科产生器或微波产生器）一起使用。通过产生和存储或者“编程”在连接或贴在配件装置上的标签中的信息的秘密片段进行认证的准备或供应。称为“认证签名”的该秘密意在仅由所述 RFID 标签的编程者及由生产商、供应商或要被认证的主装置和配件装置的拥有者知道或决定。在通过认证意图保护的后续的使用中，认证签名必须在用于比较的安全 RFID 标签和所述读写器之间传递。假设这些安全 RFID 标签不能执行加密或解密，并且因此在认证事件期间认证签名必须以明文形式由 RF 通信暴露。因此，对手可能试图使用随时可用的设备（例如 RFID 读写器和 RF 信号捕获或记录装置（“监听器”））以发现认证签名。

[0008] 如果认证签名是由多个装置内的配件装置的所有实体共有的简单秘密（密钥或

密码)，则对手对一个认证签名的任何发现（不管以何种方式）将会破坏用于不限制数量的配件装置的认证。

[0009] 在现有技术的系统中，所述认证签名存储在 RFID 标签的读写存储器的已知位置中。在这些系统中，寻求认证配件的主装置将从与配件相关联的 RFID 标签读取 UID，并且使用与假设地用于初始编程标签相同的密钥执行相同的计算。接着从配件的 RFID 标签中读取存储的认证签名，并且与计算的认证签名进行比较。如果确认匹配，则所述配件被判定为认证的。

[0010] 这种现有技术的系统具有一些缺点：因为它们需要读写存储器的消耗，而所述读写存储器为 RFID 标签中的稀缺资源；而且因为 RFID 读写存储器可以被拥有易获取的 RFID 读写器的任何一方访问，并且因此针对给定的 RFID 芯片的认证签名可能是容易读取的。这样可读性的另一个缺点是：可以读取一定数量的认证签名的对手可以推断或获得用于大量配件装置的多元化模式或规则，从而挫败所述认证系统。

发明内容

[0011] 本公开涉及安全 RFID 认证系统、设备或相关使用方法。在一个新的方面，通常与密码功能相关联的 RFID 标签的存储区域适用于存储认证签名，从而释放了要分配给应用使用的读写存储器。在一些实施例中，RFID 标签包括密码控制的对读取和 / 或写入功能的访问。通过存储认证签名作为读、写、读写、或其他密码，读、写或进一步操作或与 RFID 标签通信的能力能被防止，并且因此与这样的标签相关联的装置的使用也可以被更可靠和安全地控制。例如但不限于，根据本公开的 RFID 标签可以使用于控制装置的互操作性、允许认证的装置和 / 或配件的使用和禁止未授权的装置和 / 或配件的使用，并且具有比易受攻击和损害的现有技术更好的确定性和可靠性。

[0012] 这样的能力可具有益处，例如，可以减少或消除在外科手术过程期间不适当的外科手术装置的使用。不适当的外科手术装置可以包括但不限于，先前使用过的、未消毒的、通过未授权分发渠道购买的、伪造的、未测试的、不相容的、未校准的、没有批准的、不受适当的质量控制的、重生产的等外科手术装置。

[0013] 在一些实施例中，认证 RFID 标签的方法包括：选择密钥；通过读取来自所述 RFID 标签的唯一识别码 (UID) 制备 RFID 标签，通过加密地结合密钥和 UID 创建唯一认证签名，和将 RFID 标签的密码或密码组设置为所述唯一认证签名；以及通过读取来自 RFID 标签的唯一识别码 (UID) 对 RFID 标签进行认证，通过加密地结合密钥和 UID 重建所述唯一认证签名；通过向所述 RFID 标签提供唯一认证签名作为密码或密码组以尝试访问 RFID 标签的功能，并且如果 RFID 标签在密码操作中给出无错响应，或者如果访问所述 RFID 标签的密码控制的功能的尝试是成功的，则判定所述 RFID 标签是认证的。在实施例中，尝试访问的功能可以包括但不限于：读功能、写功能和 / 或私密功能。

[0014] 在一个方面，根据本公开的实施例包括如下装置：例如但不限于可以可操作地连接到器材或与器材相关联的外科手术器械；例如但不限于包括射频识别 (RFID) 读写器、或具有永久性且不可改变的 RFID 标签、唯一的识别码 (UID)、能够保持数据直到重新写入的读写存储器、能够选择性防止读写存储器的选定部分的读取或重写的保护机制以及可操作地与读写保护机制耦合并且可写不可读的密码存储中的至少一个的电外科产生器、超声产

生器和微波产生器。

[0015] 在一个方面，根据本公开的实施例的系统使用具有全局唯一识别码 (UID)、读写存储器以及只写且自保护密码的密码机制的一个或多个 RFID 标签。所述系统包括被配置为对其供电、读和写 RFID 标签的一个或多个 RFID 读写器（例如读取器或认证器）。RFID 读写器中的至少一个被配置为由授权代理使用的 RFID 编程器创建来自未制备的（例如，新出厂的或未使用的）RFID 标签的安全认证 RFID 标签。RFID 读写器中的至少一个被配置为 RFID 认证器用于查询 RFID 标签以确定其是否为有效的安全认证 RFID 标签。本公开的系统包括仅为 RFID 编程器和 RFID 认证器所知的密钥。在一些实施例中，密钥被表示为具有已知长度的比特串。

[0016] 在另一个方面，本公开描述了用于为了安全认证目的（例如为了确保、允许或同意对正确制备的 RFID 标签的出现的访问，同时禁用和 / 或拒绝对相似但不正确制备的或未制备的 RFID 标签的访问，同时阻止对认证的 RFID 标签的未授权复制、克隆或伪造）生产和识别一个或多个 RFID 标签的方法和设备。有利的是，因为所述安全认证签名存储为只写密码并且因此不占用所述 RFID 标签的读写存储器，所以通过利用安全认证信息制备的 RFID 标签的所述读写存储器容量不会减少。拥有密钥的 RFID 编程器可以通过将每个标签唯一的信息（例如 UID）与预定的密钥结合而从新出厂的 RFID 标签制备为授权的安全认证 RFID 标签。拥有相同密钥的 RFID 认证器可以验证 RFID 标签以判定这个标签是否为已经利用授权的认证密钥编程的安全认证 RFID 标签。根据本公开的实施例中，任何 RFID 编程器在没有认证密钥的知识的情况下不能可行地创建安全认证 RFID 标签。类似地，没有拥有相同密钥的 RFID 读取器不能可行地确认给定的 RFID 标签是否利用密钥制备——尽管如果 RFID 标签不是利用所述认证密钥编程、制备或是利用 RFID 认证器拥有的其他密钥（秘密或其他）编程的，它可能是可以辨认的。拥有一定数量的安全认证 RFID 标签和空白或其他编程的 RFID 标签但是不拥有认证密钥的任何一方，不能可行地确定或提取所述密钥。可以拦截具有安全认证 RFID 标签的事务（如认证）会话的认证事件的 RFID 信号而不知道密钥的一方，不能可行地确定、推导、计算或提取所述密钥。可以拦截具有安全认证 RFID 标签的编程（例如制备或生产）会话的事件的 RFID 信号但不拥有所述密钥的一方，不能可行地确定、推导、计算或提取所述密钥。具有这样制备的 RFID 标签或拦截的信号但不拥有所述密钥的一方，不能可行地克隆、复制、伪造或由未制备的（例如新出厂的或未使用的）RFID 标签可行地创建安全认证 RFID 标签。具有这样制备的 RFID 标签或拦截的信号但不拥有所述密钥的一方，不能可行地改变或禁用包括在安全认证 RFID 标签内的认证信息。

[0017] 在另一个方面，本公开描述了认证 RFID 标签的方法的实施例，包括 :选择密钥 ;制备所述 RFID 标签，其中制备 RFID 标签包括从所述 RFID 标签读取唯一识别码，由所述密钥和所述唯一识别码创建认证签名，设置所述 RFID 标签的密码为认证签名 ;以及认证所述 RFID 标签，其中认证所述标签包括从 RFID 标签读取所述唯一识别码，由所述密钥和所述唯一识别码重建所述认证签名，通过向所述 RFID 标签提供所述认证签名作为密码以尝试访问所述 RFID 标签的功能，以及如果对 RFID 标签的功能的尝试访问是成功的则确定所述 RFID 标签是认证的。在一些实施例中，尝试访问的功能是读功能、写功能、读写功能及私密功能。

[0018] 在一些实施例中，根据本公开的认证 RFID 标签的方法包括 :将所述唯一识别码

(UID) 和所述密钥连接起来以创建比特串，在比特串上执行加密地安全散列功能（例如 SHA-1 或 SHA-1HMAC) 以获得所述认证签名。

[0019] 在一些实施例中，根据本公开的认证 RFID 标签的方法包括：将所述认证签名分割为等长的多个比特串，在多个比特串之间执行异或 (XOR) 操作以获得适用于 RFID 标签中的密码比特的数目的压缩的或变短的结果。

[0020] 在另一方面，本公开描述了用于制备为了在电外科手术过程中使用的系统。所述系统包括：具有 RFID 标签的外科器械，所述 RFID 标签包括由制备单元可读的唯一识别码和被配置为存储密码及返回表明所提供的密码是否等于所存储的密码的状态的密码模块；制备单元，所述制备单元具有 RFID 通信单元，与所述 RFID 通信单元可操作地耦合的处理器，存储器，其与处理器可操作地耦合且存储密钥、有用于读取外科器械的 RFID 标签的所述唯一识别码的一组指令、至少部分基于外科器械的 RFID 标签的所述唯一识别码和所述密钥产生认证签名、并且在所述密码模块中存储所述认证签名作为密码。所述密码可以与所述 RFID 标签的功能相关联。所述功能可以是使所述读写存储器可读，使所述读写存储器可写，或使所述读写存储器可读写。

[0021] 在一些实施例中，所述 RFID 标签进一步包括读写存储器，而所述一组指令进一步包括被配置为初始化所述读写存储器内数据结构的指令。在一些实施例中，所述数据结构被配置为存储使用计数、生产日期、生产序列号、失效日期、校准数据、历史数据、认证数据或操作限制参数。

[0022] 在一些实施例中，目前描述的系统至少部分地使用所述密钥和所述 RFID 标签的所述唯一识别码 (UID) 的加密散列产生所述认证签名。

[0023] 在另一方面，本公开描述了为了在电外科手术过程期间使用的用于认证外科器械的系统。在一些实施例中，所述系统包括具有 RFID 标签的外科器械，其中所述 RFID 标签包括由认证单元可读的唯一识别码和存储密码及被配置为返回表明所提供的密码是否等于所存储的密码的状态的密码模块。所述系统进一步包括认证单元，所述认证单元具有 RFID 通信单元，具有与所述 RFID 通信单元可操作地耦合的处理器，具有与处理器可操作地耦合的存储器，其存储密钥、具有用于读取外科器械的 RFID 标签的所述唯一识别码的一组指令、至少部分基于所述密钥和外科手术器械的 RFID 标签的所述唯一识别码产生认证签名、向所述密码模块提供所述认证签名作为密码、及接收表明所提供的密码是否等于所存储的密码的状态。在一些实施例中，所述系统包括与所述处理器可操作地耦合的电外科产生器。在一些实施例中，如果接收的状态表明所提供的密码不等于所存储的密码，则电外科产生器的操作被抑制。在一些实施例中，所述 RFID 标签包括读写存储器，而所述一组指令进一步包括被配置为修改所述读写存储器内数据的指令。在一些实施例中，所述认证签名至少部分基于所述密钥和所述 RFID 标签的唯一识别码的加密散列产生。

附图说明

[0024] 当结合附图时，根据如下的详细描述，本公开的上述以及其他的方面、特征及优点将变得更加清楚，其中：

[0025] 图 1 是根据本公开的 RFID 认证系统的实施例的示意图；

[0026] 图 2 是根据本公开的在电外科器械生产期间的 RFID 标签制备过程的示意图；

[0027] 图 3 是根据本公开的实施例制备的 RFID 标签的框图；

[0028] 图 4 是根据本公开的 RFID 制备方法的实施例的流程图；

[0029] 图 5 是根据本公开的 RFID 制备方法的另一个实施例的流程图；和

[0030] 图 6 是根据本公开的 RFID 认证方法的实施例的流程图。

具体实施方式

[0031] 本公开的具体实施例将参考附图描述如下；然而，应当理解，本公开的实施例仅仅是本公开的示例且可以以多种形式实现。为了避免在不必要的细节模糊本公开，在此没有详细地描述公知的功能或结构。因此，在此公开的具体结构和功能的细节不应被解释为限制的，而其仅仅作为权利要求的基础，并作为教导一个本领域技术人员在几乎任何适当的详细结构中多样地运用本公开的代表性基础。在下面的图和描述中，术语“近端”，如传统的，应当指的是靠近用户的器械的末端，而术语“远端”指的是远离用户的末端。在本说明书以及附图中，类似的参考标号代表执行相同、相似或等同功能的元件。

[0032] 参考附图 1，显示了根据本公开的电外科系统 10 的实施例。所述系统 10 包括被配置为与电外科产生器 65 可操作地耦合的电外科器械 20。电外科器械 20 包括具有从其延伸出握把 50 的壳体 22 以及在第一位置和第二位置之间可移动的手柄 45，所述第一位置为手柄 45 以间隔关系远离握把 50 定位的位置，而第二位置是手柄 45 以间隔关系比在第一位置更靠近握把 50 定位的位置。电外科器械 20 包括可以以任何合适的方式固定到壳体 22 的 RFID 标签 80。附加地或可选择地，RFID 标签 80 可以固定到连接器 70。在一些实施例中，RFID 标签 80 可以固定到电外科器械 20 的任何机械关联的部分（例如轴 25，握把 50，电缆 60 等）。优选地，RFID 标签 80 以如下方式固定到电外科器械 20：使得从电外科器械 20 的任何试图移除 RFID 标签 80 或对 RFID 标签 80 物理解除关联将使得 RFID 标签 80 和 / 或电外科器械 20 不起作用。轴 25 从壳体 22 向远侧延伸并且包括在其远端 26 的相对的钳口部件 30、35。钳口部件 30、35 是可以在打开位置和第二位置之间移动，其中在打开位置，钳口 30 以间隔关系远离钳口 35，而在第二位置，钳口 30 以间隔关系更靠近钳口 35 以抓取在其间的组织。

[0033] 为了电控制到钳口部件 30、35 的电外科能量的输送，所述壳体 22 支持在其上的开关 55，开关 55 由用户可操作地启动和终止到钳口部件 30、35 的电外科能量的输送。所述开关 55 与电外科能量源（例如电外科产生器 65 或在壳体 22 内支持的电池（未显示））电通信。所述产生器 65 可以包括如由 Colorado，Boulder 的 Covidien Energy-Based Device 销售的 **LIGASURE®** 血管闭合产生器和 FORCE **TRIAD®** 产生器的装置。电缆 60 在壳体 22 和产生器 65 之间延伸并且在其上包括连接器 70 以使得所述器械 20 可以选择地与所述产生器 65 电耦合或解耦。在一些实施例中，电外科器械 20 可以包括血管闭合器械，例如但不限于在授予 Dycus 等人的美国专利 No. 7，255，697 中描述的电外科钳。

[0034] 器械 20 可以包括旋转控制器 40，所述旋转控制器 40 使得用户在不需要扭转壳体 22、握把 50 等的情况下能够绕着所述轴 25 的纵轴旋转轴 25 和 / 或钳口部件 30、35 到相对于外科部位的必要位置。产生器 65 包括被配置为显示操作数据并且向用户提供可听音调以及接受用户输入的用户界面 75。

[0035] 相对的钳口部件 30、35 经由延伸穿过细长轴 25 的导体（未明确示出）电耦合到

电缆 60，并由此电耦合到产生器 65，来分别提供到布置在钳口部件 30、35 的组织接触面上的一对导电的、组织接合的密封板 31、36 的电通路。钳口部件 30 的密封板 31 与钳口部件 35 的密封板 36 相对，并且在一些实施例中，密封板 31 和 36 电耦合到相对的终端，例如产生器 65 相关联的正端或有源端 (+) 和负极或与返回端 (-)。因此，双极能量可以通过密封板 31、36 提供。可选择地，密封板 31、36 可以配置为向组织传递单极能量。在单极配置中，密封板 31、36 的一个或两个从有源端（例如 +）传递电外科能量，而返回垫（未明确示出）一般被放置在病人身上并且提供到产生器 65 的相对端 (-) 的返回路径。

[0036] 产生器 65 包括与被配置为向器械 20 传递电外科能量的 RF 源 90 可操作地通信的控制器 94。控制器 94 与 RFID 读写器 95 和存储器 93 可操作地通信。存储器 93 包括密钥 97 的副本。在一些实施例中，密钥 97 可以以加密或编码形式存储在存储器 93 中以阻止攻击者反向工程和 / 或发现密钥 97。RFID 读写器 95 包括使得产生器 65 能够有效地与 RFID 标签 80 通信的天线 96。产生器 65 包括可操作地与控制器 94 通信的用户界面 75，其被配置为显示操作数据和向用户提供可听音调以及接受用户输入。

[0037] RF 源 90 被配置为响应于从控制器单元 94 接收的一个或多个控制信号选择性地传递电外科能量。控制器单元 94 被配置为接收来自开关 55 和用户界面 75 的用户输入信号，并被配置为接收来自 RFID 读写器 95 的认证信号。相似的产生器在共同拥有的美国专利 7,927,328 和 8,211,099 中描述，其中每个专利的全部通过引用并入此处。

[0038] 本公开的实施例从 RFID 标签 80 的唯一 UID81 和密钥 97 产生加密安全的认证签名。有利的是，本公开的方法使得拥有密钥 97 的第一装置能够处理标签 80 的 UID81 从而容易地确定用于与标签 80 关联并且与第一装置关联使用的第二装置（例如器械、配件或设备）的实例，同时使得攻击者复制、伪造或选择重造正确的认证签名是非常困难或昂贵的。可以预期的是密钥 97 存储在被配置为执行根据本公开的认证的每个装置中。例如，密钥 97 可以如本领域技术人员所理解的存储在产生器 65 的存储器 93 内以及 RFID 读写器 95 内。所述密钥 97 可以存储在 RFID 编程器 110（图 2）的存储器 120 中。在一些实施例中，所述 RFID 标签 80 符合 ISO 15693RFID 标签标准并且因此包括在制造标签期间不可消除地写入的绝对（全局）唯一 64 比特 UID。

[0039] 参考图 2 和 3，显示了 RFID 标签 80 的制备过程 100，其中所述标签的 UID 81 由编程器 110 读出。在一些实施例中，编程器 110 与组装线 150 可操作地相关联，并被配置为经由算法结合密钥以得出唯一认证签名而在大量生产中顺序编程多个器械 20(20a，20b，…20d)。然而，编程器 110 可以被用于在其他环境中根据需要制备 RFID 标签 80，例如但不限于测试或修理设施。

[0040] 编程器 110 包括与 RFID 单元 112 和存储单元 120 可操作地通信的处理器 140，以及便于用户对编程器 110 操作的可选择的用户界面（未明确显示）。编程器 110 包括与处理器 140 可操作地相关联的 RFID 通信单元（例如收发器），所述 RFID 通信单元被配置为向 RFID 标签 80 提供电源并与 RFID 标签 80 通信。存储单元包括密钥 97 和包括一组可编程指令用于执行如本文描述的制备 RFID 标签 80 的方法的编程单元 130。

[0041] RFID 标签 80 包括唯一识别码 (UID)81，与读写存储器 84 可操作地通信的密码模块 83，所述读写存储器 84 包括认证签名 82 的只写副本。密码模块 83 包括控制读取和写入访问读写存储器 84 的能力。

[0042] 在一些实施例中，加密算法（例如安全散列 SHA-1 或基于安全散列的消息认证编码 SHA-1HMAC）被使用来从 UID81 和密钥 97 产生认证签名。有利的是，这种办法确保如果 UID81 或密钥 97 的任何比特发生变化，则认证签名将会变化。所产生的认证签名 82 被编程入 RFID 标签 80 作为读、写、读写或密码模块 83 内的其他密码。需要注意所述读、写、或读写密码或其他密码的使用允许无限制读访问 UID81，但可用于限制访问读写存储器 84。因此，一旦被编程，不能从标签 80 读取所述密码（亦称认证签名 82），这是因为所述认证签名 82 以只写模式存储在密码模块 83 中。在使用中，标签 80 的密码单元 83 将会接受提供的密码（例如认证签名），并且作为响应，提供是否接收了正确的密码（或不正确的密码）的指示（通常是状态标志或状态码）。因此本公开的方法使用密码单元 83 作为黑盒子，从而密码被永久隐藏在其内，并且不能从 RFID 标签 80 读取也不能从 RFID 标签 80 传输。以这种方式，本公开的实施例在无需耗费 RFID 标签 80 的任何读写存储器的情况下实现高安全性的认证。

[0043] 本文中描述的系统和方法的实施例使用制备（例如生产）阶段和认证（例如场或终端用户使用）阶段。在制备阶段，利用认证密钥制备一个或多个 RFID 标签。在认证阶段，所制备的标签中的一个或多个被认证以供使用。例如，外科器械可以包括如上所述进行制备的 RFID 标签。在使用之前，例如当器械在卫生设施（例如医院）被清点或接收、引入外科环境（例如带进手术室）时和 / 或当器械被制备以供使用（例如电外科器械附接到电外科产生器）时，包括在器械中的所述 RFID 标签被认证以确保它是适合于使用的。伪造的或不合适的器械将认证失败，其事实将通知相关人员和 / 或令相关器材失效（例如产生器将拒绝操作未认证器械）。

[0044] 为了在使用期间认证 RFID 标签，RFID 读取器从标签读取 UID。所述 RFID 读取器之后根据对 RFID 读取器已知的密钥和刚从标签读出的 UID 利用与制备标签相同的算法重新产生认证密钥。所得到的认证签名被提供给 RFID 密钥作为读、写、或读写或其他密码。如果 RFID 标签返回成功状态（例如输入了正确密码），则 RFID 标签以及因此与其相关联的装置被认为是认证的并且其使用被允许。任何其他状态（例如不成功状态），表明所述标签和 / 或装置不是认证的并且将采取合适的动作（例如装置的使用被禁止或限制），“kill”代码可以发给装置以使其永久无法操作，还可以发送警报，以及传送信息到执行机构等。

[0045] 在一些实施例中，在认证后附加的数据可以写入 RFID 标签。例如但不限于，包括使用计数和使用最大量的使用数据可以保持在所述 RFID 标签的读写存储器内。因此，即使装置是认证的，如果装置的使用计数超过了可接受的数目，装置的使用也不被允许。设想了可以与本文描述的授权系统和方法结合使用的其他数据类型（例如失效日期、校准数据、历史数据、认证数据、操作限制、生产日期、生产序列号等），以确保各种系统装置的正确使用。

[0046] 参考图 4，显示了根据本公开的 RFID 安全认证方法 200 的实施例，其中通过产生 160 比特消息摘要的 SHA-1 算法产生安全散列。在本实施例中，密钥是具有“n”比特长度的比特串 206。在步骤 205 中，密钥以任何合适的方式产生，包括但不限于手动输入、噪声采样、伪随机数产生或者其任意组合。密钥 206 以被普通技术人员熟悉的安全又可靠的方式记录，并优选利用冗余记录，这是因为所述密钥的丢失或损害将使得利用所述密钥制备的所有安全标签不适合使用。

[0047] 在步骤 210 中，编程器 110 从 RFID 标签 80 读取 UID 81。在一些实施例中，UID 81 是具有 64 比特长度的比特串。在步骤 215 中，UID81 与安全密钥连接起来以创建具有 n+64 比特长度的合成比特串 216。在步骤 220 中，对合成的 n+64 比特的比特串执行 SHA-1 散列算法（例如符合 PIPS PUB 180-2IETF RFC 3174）或 SHA-1HMAC 消息认证算法（例如符合 PIPS PUB 198IETF RFC 2104），产生 160 比特散列 221（例如散列摘要）。所述散列 221 可以直接用作认证签名，或可替代地或可选择地，所述 160 比特散列摘要可以通过以下操作而被缩短：将散列摘要分割为每个都是 32 比特的五组，对前两个 32 比特的组执行第一异或操作以计算第一中间结果 227，对第一中间结果和第三组执行异或操作以计算第二中间结果，以此类推直到剩下 32 比特最终的授权签名 229。在步骤 230 中，所述授权签名（例如散列密钥 221 或 32 比特最终授权签名 229）被写入 RFID 标签 80 作为读、写、读写或其他密码，或 32 比特异或结果中的一些数目可以被写入几个 RFID 密码。

[0048] 现在参考图 5，显示了根据本公开的 RFID 安全认证方法 300 的实施例，其中通过基于散列的消息认证编码 (HMAC) 产生最终认证签名。本实施例在需要增加加密强度的应用中是合适的。HMAC 是根据 IETF RFC 2104:FIPS PUB 198 的加密标准，并且基本由 SHA-1 散列算法（见上文）的两次迭代组成。

[0049] 在步骤 305 中，512 比特密钥 306 可以由任何合适的方式产生，包括但不限于手动输入、噪声采样、伪随机数产生或它们的任意组合。密钥 306 以安全又可靠的方式被记录，并且优选地如上所述利用冗余。在一些实施例中，密钥 306 最初可以小于 512 比特，使用零或任何其他合适比特类型填充以获得 512 比特的最终大小。在步骤 310 中，读出了经历制备的标签 80 的 UID 81。在步骤 315 中，对 512 比特的密钥 306 和由十六进制类型 3636…36（又称“内填充”比特类型）组成的 512 比特的填充 316 执行异或操作，以获得第一中间结果 317。在步骤 320 中，第一中间结果 317 与 64 比特的 UID311 连接起来以获得第二中间结果 318。在步骤 325 中，对第二中间结果 318 执行 SHA-1 操作以获得包括 160 比特散列的第三中间结果 326。在步骤 330 中，第三中间结果 326 与由十六进制类型 5C5C…5C（又称“外填充”比特类型）组成的 512 比特的填充 331 连接起来以形成第四中间结果 332，并且在步骤 335 中，对第四中间结果 332 执行 SHA-1 操作以形成 160 比特的认证签名 336。在步骤 340 中，所述授权签名 336 被写入 RFID 密钥 80 作为读、写、读写或其他密码。由于所述 UID 在私密模式不能被读取，因此所述认证签名不能被使用为私密密码。

[0050] 典型的，未制备（例如新出厂的或“未使用的”）的 RFID 标签会包含默认或空密码，或者可能包含制造商提供的“传输密码”。标签可以包括辨认独立的和有区别的密码（例如只允许读取的密码（“读密码”）、只允许写入的密码（“写密码”）、允许读和写的密码（“读写密码”）或其他密码）的能力。

[0051] 所述标签的 UID 被例如 RFID 读写器读取，并且以下详细描述了所述 UID 用于计算 RFID 签名。为了改变默认的或现有的读密码为新的读密码，现有的密码利用“设置读密码”命令被写进标签以解锁所述 RFID 标签，然后新密码结合“写入读密码”命令被写入芯片。另外地或可选择地，为了改变默认或现有的写密码为新的写密码，现有的写密码结合“设置写密码”命令被写入标签中，其接下来使得新的写密码通过“写入写密码”命令被写入芯片中。

[0052] 所述认证签名被写入 RFID 存储器的安全区域，所述安全区域经常被用于存储读或写密码并且其不是读写存储器的一部分。有利的是，RFID 标签的实际密码存储区域对任

何用户是不可访问的（不可读取的）。RFID 标签揭示的唯一事实是已经提供了正确的（或不正确的）密码。因此，因为依赖 UID 和密钥的密码对个体 RFID 芯片是唯一的，暴力攻击来猜密码，在最坏的情况下，将只导致单个装置可访问。因为系统总体内的所有其他装置具有不同认证签名，单个标签的损害不会导致系统中任何其他标签的损害。

[0053] 在一些实施例中，所述 32 比特的读和写密码可以被组合以创建提供增强安全性的单个 64 比特的密码。在一些实施例中，所述 RFID 标签包括表明读和写密码的长度均为 64 比特的参数，其接下来由连接的 32 比特的读密码和 32 比特的写密码限定。

[0054] 如果需要进一步保证 RFID 标签免受攻击，可以使用私密密码，从而 RFID 标签的所有内容（包括 UID）变得不可见，除非提供了正确的私密密码。一旦处于私密模式中，在任何数据能被读出标签或写入标签之前，必须向 RFID 标签提供正确的私密密码。RFID 标签可以被设置为私密模式，从而在任何数据（包括标签的 UID）从标签读出之前，必须向标签提供正确的私密密码。在这种情况下，实现了额外的安全层，其进一步阻止对所述 RFID 标签的内容的未授权地尝试读取或修改。应当指出的是，私密密码应该在标签的整个目标群（和与其相关联的装置）内一致，因为直到提供了私密密码 UID 才可用，这排除了基于 UID 的唯一“私密授权密钥”的使用。

[0055] 一旦 RFID 标签处于私密模式，所述标签将仅响应于顺序发出的“获取随机数”命令和“设置（私密）密码”命令。所述“获取随机数”命令使得所述 RFID 标签产生 16 比特的随机数并将其传输到所述读写器。所述 16 比特的随机数重复两次以生成 32 比特的数，其之后与 32 比特的私密密码进行异或。以这种方式，实际密码不是在空中传输，并且因此，其易受拦截性大大降低。拥有用于编码密码的随机数的所述标签随后可以重建实际的私密密码。在接收“设置密码”命令后，随后所述标签从“私密”模式改为“公开”模式。一旦处于“公开”模式，随后所述 RFID 芯片可以被正常地访问，例如根据读或写密码的状态处于读或写模式。

[0056] 现在转向图 6，其显示了与如本文描述制备的 RFID 标签相关联的装置的认证方法 400 的实施例。在步骤 404 中，如果需要，私密密码被写入所述标签以解锁所述 UID。在实施例中，所述私密密码由 RFID 读取器或读写器写入。在步骤 405 中，所述 UID 从标签读出，并且在步骤 410 中，如上所述，授权签名从刚读取的 UID 和密钥来计算。在步骤 415 中，所述授权签名被传输到 RFID 标签作为读、写、读写或其他密码以尝试访问所述 RFID 标签的读写存储器和 / 或尝试验证所述器械 20 的真伪。在步骤 420 中，所述密码被 RFID 标签处理并且结果被传送到读取器 / 读写器。如果认证签名（又称密码）被所述标签接受，则在步骤 425 中，所述标签和 / 或与其一起的装置是认证的。相反地，如果所述认证签名 / 密码不被接受，则在步骤 430 中指示了授权失败。

[0057] 应当理解，可对本文公开的实施例做多种修改。上述公开的进一步变形和其他特征和功能，或其替代物，可以被期望地结合为多个其他不同的系统、器械或应用。尽管显示了利用 SHA-1 或 SHA-1HMAC 加密算法的示例实施例，应当理解，本公开的实施例可以利用任何合适的加密安全签名算法（包括但不限于 SHA-2, MD5, GOST, RIPEMD 和 / 或 SNEFRU）来实施。因此，在其中的多种目前无法预料或无法预期的替代、修改、变化或改进可随后由本领域的技术人员实现，这些替代、修改、变化或改进也意在通过下列的权利要求所涵盖。

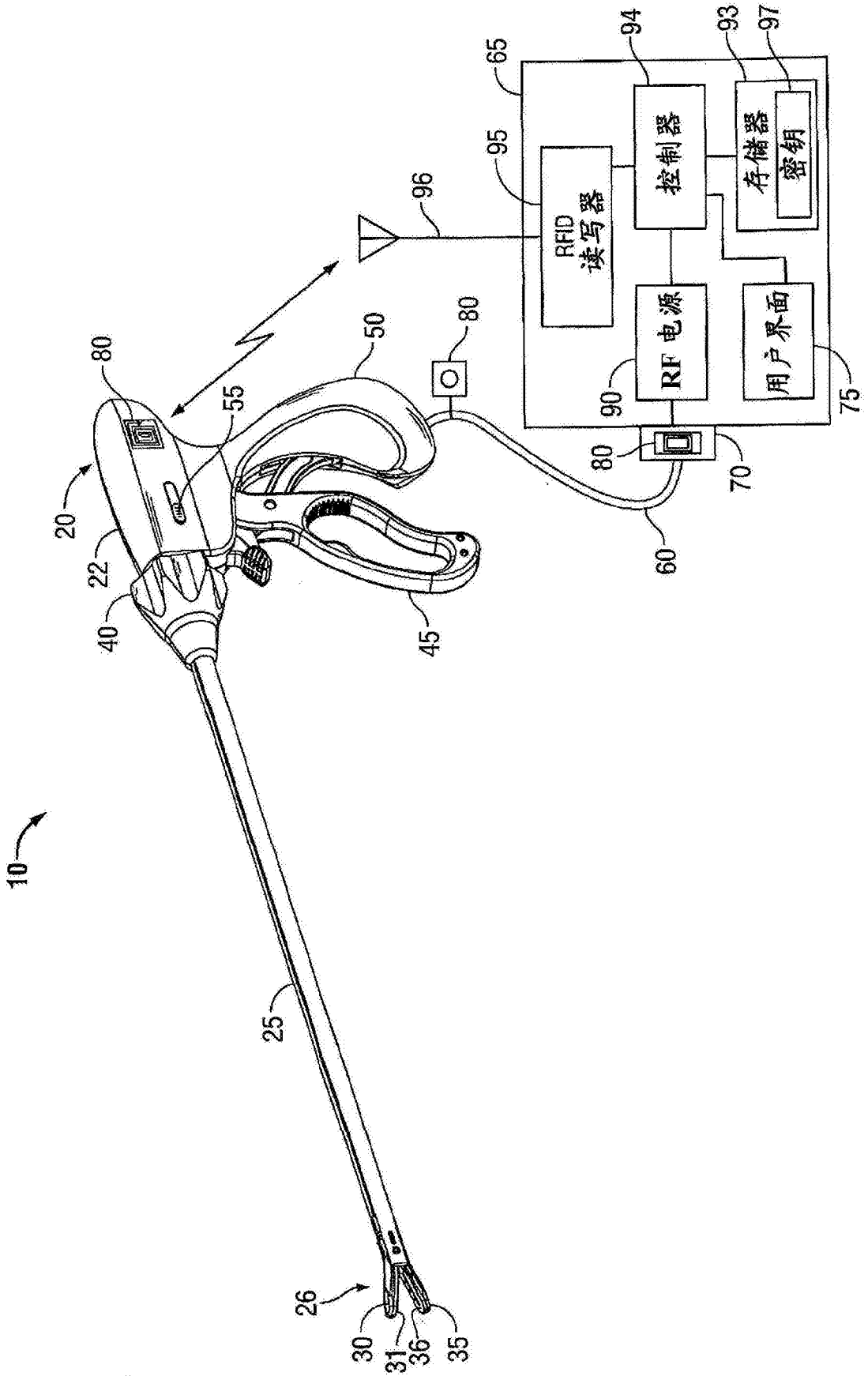

65
94
93
97
95
96
RFID
读写器
控制器
存储器
密钥
RF 电源
用户界面
90
75
80
70
60
50
80
55
80
20
22
40
45
10
25
26
30
31
36
35

图 1

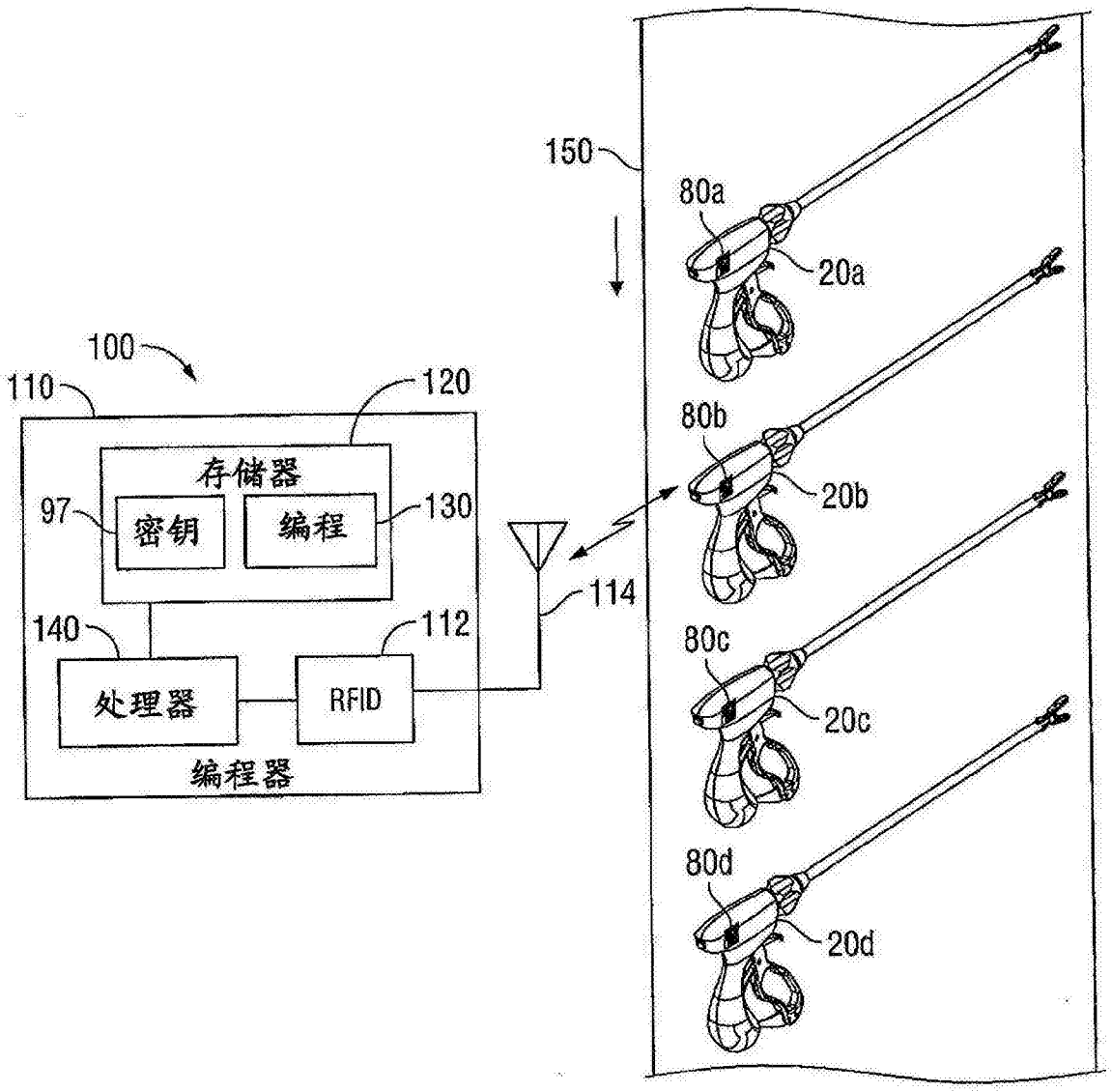

100
110
120
存储器
97
密钥
编程
130
140
处理器
RFID
112
114
编程器
150
80a
20a
80b
20b
80c
20c
80d
20d

图 2

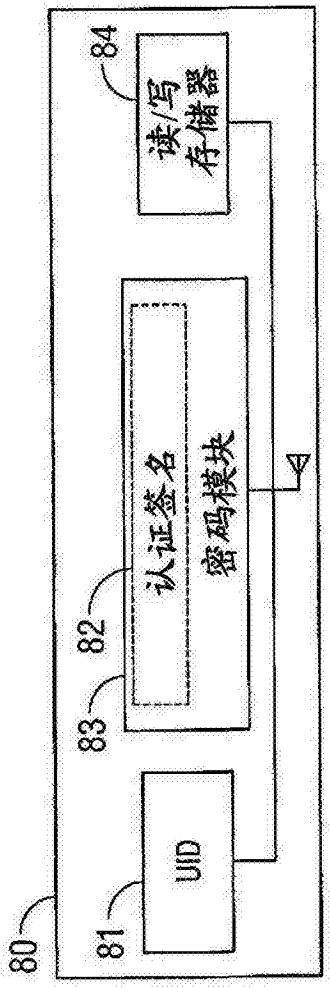


图 3

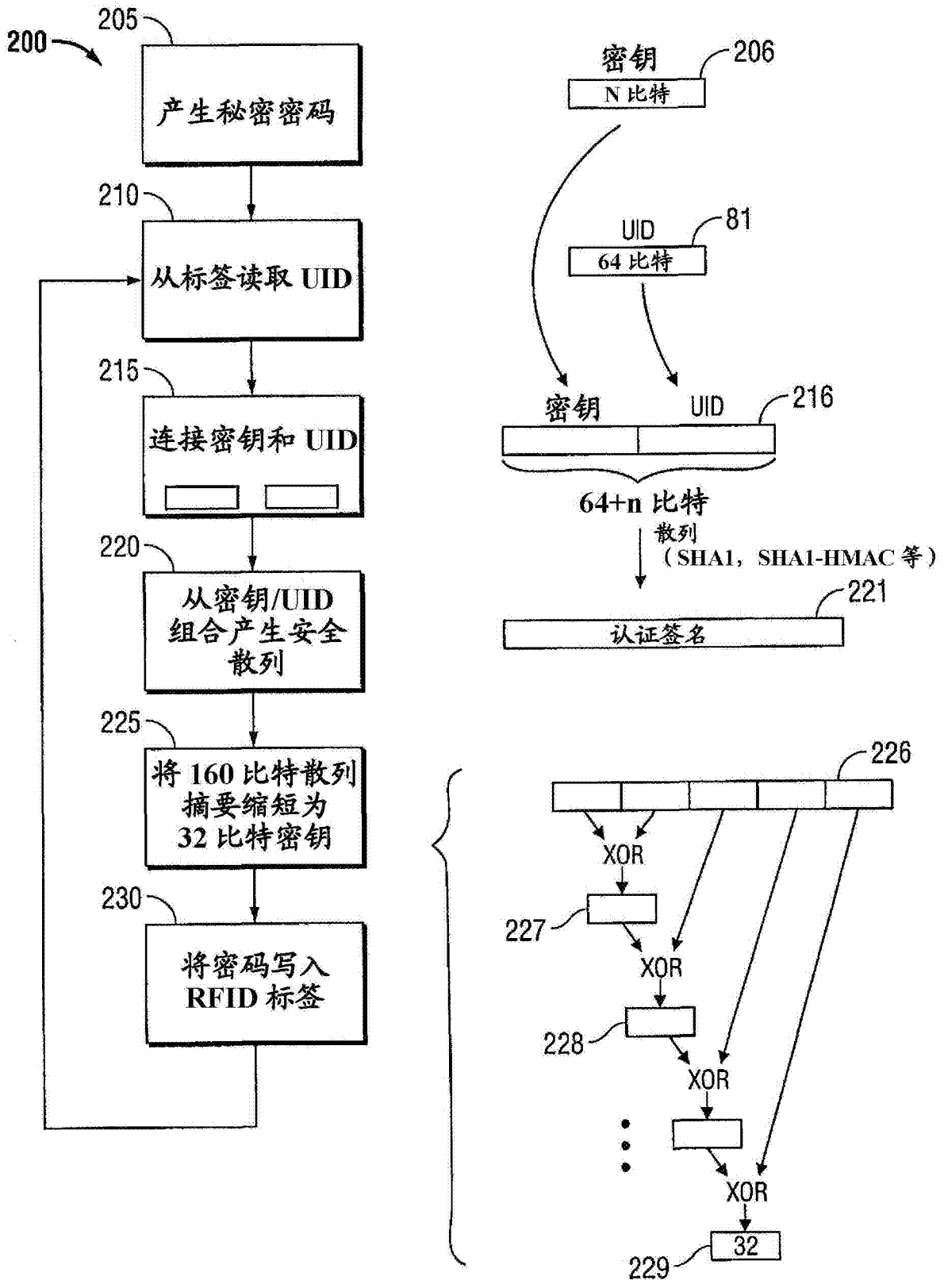

200
205
产生秘密密码
210
从标签读取 UID
215
连接密钥和 UID
220
从密钥/UID 组合产生安全散列
225
将 160 比特散列摘要缩短为 32 比特密钥
230
将密码写入 RFID 标签
密钥
206
N 比特
UID
81
64 比特
密钥
UID
216
64+n 比特
散列
（SHA1，SHA1-HMAC 等）
221
认证签名
226
XOR
227
XOR
228
XOR
XOR
32
229

图 4

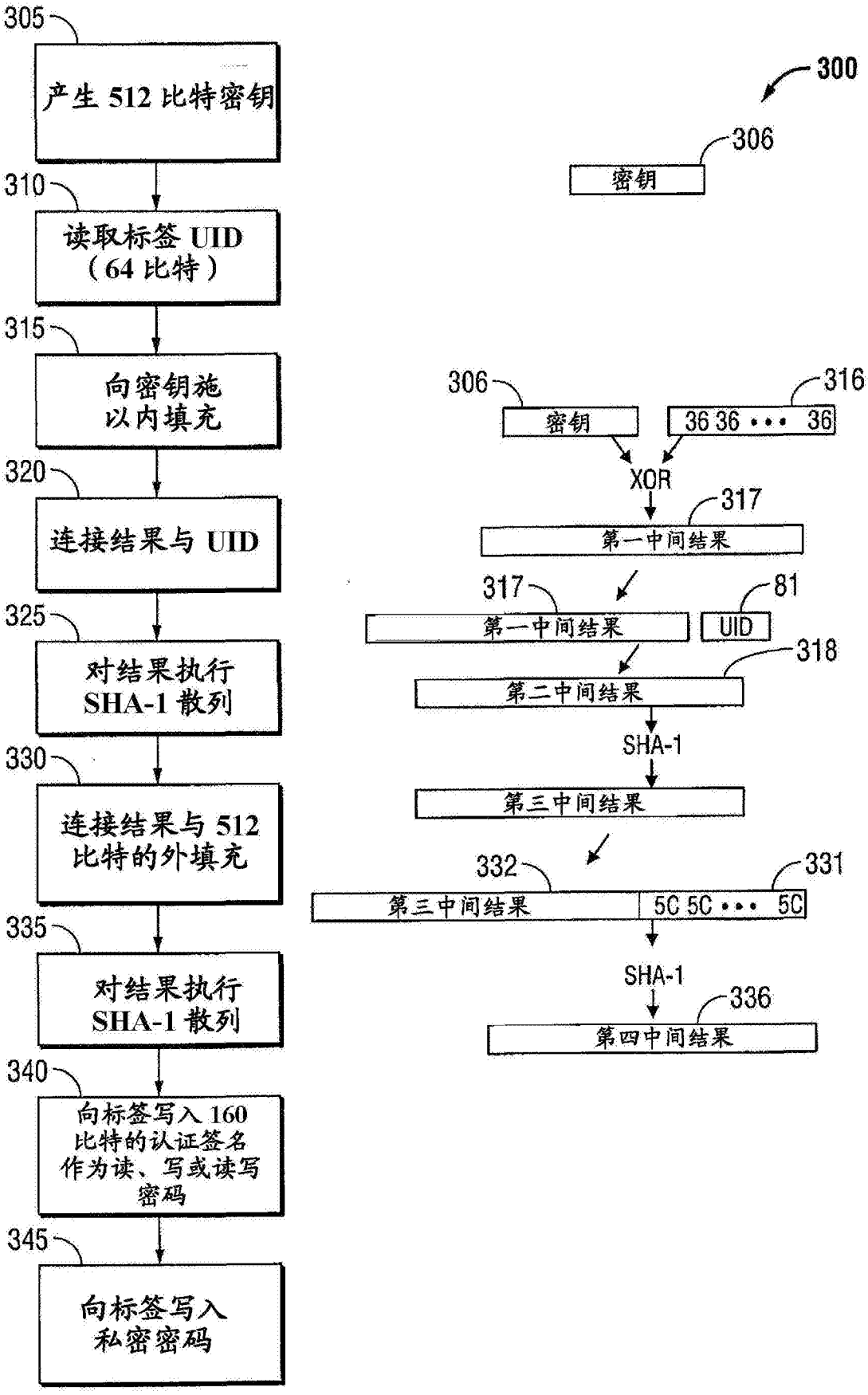

305
产生 512 比特密钥
310
读取标签 UID
（64 比特）
315
向密钥施
以内填充
320
连接结果与 UID
325
对结果执行
SHA-1 散列
330
连接结果与 512
比特的外填充
335
对结果执行
SHA-1 散列
340
向标签写入 160
比特的认证签名
作为读、写或读写
密码
345
向标签写入
私密密码
300
306
密钥
306
密钥
316
36 36 ••• 36
XOR
317
第一中间结果
317
第一中间结果
81
UID
318
第二中间结果
SHA-1
第三中间结果
332
第三中间结果
331
5C 5C ••• 5C
SHA-1
336
第四中间结果

图 5

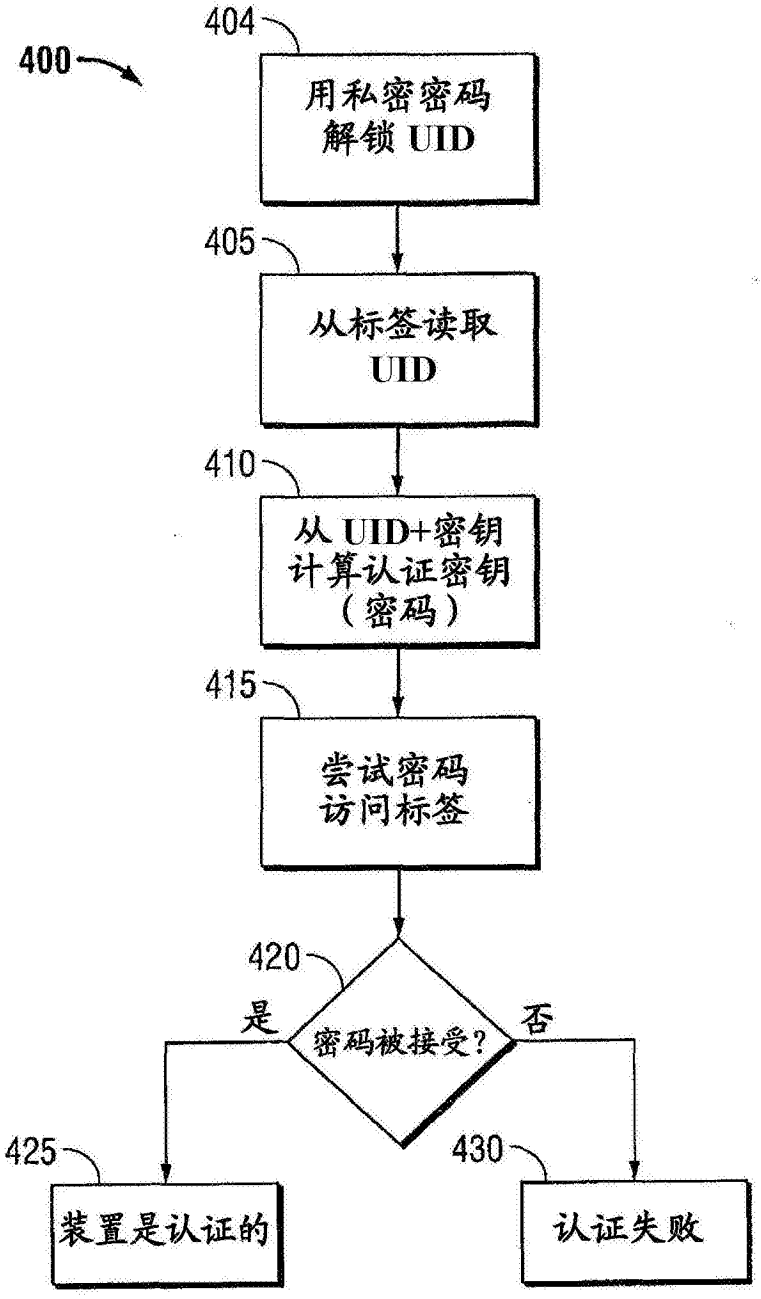

400
404
用私密密码
解锁 UID
405
从标签读取
UID
410
从 UID+密钥
计算认证密钥
（密码）
415
尝试密码
访问标签
420
密码被接受?
是
否
425
装置是认证的
430
认证失败

图 6