

(12) 发明专利申请

(10) 申请公布号 CN 102640448 A

(43) 申请公布日 2012. 08. 15

(21) 申请号 201080028329. 9

(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

(22) 申请日 2010. 05. 13

代理人 叶勇

(30) 优先权数据

61/213, 166 2009. 05. 13 US

(51) Int. Cl.

H04L 9/28 (2006. 01)

(85) PCT申请进入国家阶段日

2011. 12. 26

(86) PCT申请的申请数据

PCT/US2010/034777 2010. 05. 13

(87) PCT申请的公布数据

W02010/132695 EN 2010. 11. 18

(71) 申请人 敬畏技术有限责任公司

地址 美国得克萨斯

(72) 发明人 丹尼尔·韦恩·恩格斯

埃里克·迈伦·史密斯

特洛伊·A·舒尔茨

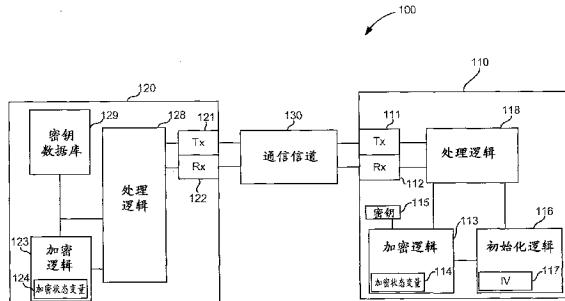
权利要求书 3 页 说明书 9 页 附图 7 页

(54) 发明名称

用于在对称加密系统内安全地识别和认证设备的系统和方法

(57) 摘要

本发明描述了用于在对称加密系统内对设备进行安全识别和认证的系统和方法。RFID标签可使用加密状态变量和对称密钥来产生指示符。在从所述标签接收加密状态变量之后，RFID读取器可通过在密钥数据库中执行密钥的穷举检索来识别所述标签。通过使用所述密钥和加密状态变量来测试数据库中的各密钥，以执行类似于所述标签所执行的加密操作。接着，将结果与接收的标签指示符进行比较，以确定是否识别了所述标签。基于转轮的加密方案提供低成本的密钥检索，同时有效地抵御了克隆、跟踪、篡改和重放攻击。



1. 一种用于在对称加密系统中对设备进行安全识别和对第一设备和第二设备之间的通信进行安全认证的方法,各设备具有加密状态变量,所述方法包括:

在该第二设备处接收来自该第一设备的加密状态变量;

对该第二设备的密钥数据库中的各个加密密钥,使用接收的加密状态变量来产生指示符;和

通过所使用的加密密钥,将所产生的指示符与自该第一设备接收的指示符进行比较,以识别该第一设备。

2. 如权利要求1所述的方法,进一步包括:

在该第二设备处确定接收的加密状态变量是否与该第二设备的密钥数据库中的加密密钥相关。

3. 如权利要求2所述的方法,进一步包括:

响应于查询,在第一设备处产生初始化向量;

使用该初始化向量对该第一设备的加密状态变量进行初始化;和

使用该第一设备的加密状态变量来产生指示符。

4. 如权利要求3所述的方法,其中,从LFSR、计数器或随机数发生器中的任何一个产生所述初始化向量。

5. 如权利要求3所述的方法,其中,查询包括用于产生所述初始化向量的标识符。

6. 如权利要求3所述的方法,其中,查询包括用于产生所述指示符的标识符。

7. 如权利要求3所述的方法,进一步包括:

在该第二设备处产生询问命令;

使用加密状态变量对该询问命令进行加密;

通过使用该第二设备的加密状态变量,在该第二设备处产生第二指示符;和

向该第一设备传送该询问命令和该第二指示符。

8. 如权利要求7所述的方法,进一步包括:

在该第一设备处接收该询问命令和该第二指示符;

在该第一设备处对该询问命令进行加密;和

如果接收的第二指示符与在该第一设备处使用该第一设备的加密状态变量所产生的指示符相匹配,则证实该第二设备。

9. 如权利要求8所述的方法,进一步包括:

在该第一设备处,使用该第一设备的加密状态变量来产生第三指示符;

对该第一设备的初始化向量进行加密;和

向该第二设备传送该第三指示符和初始化向量。

10. 如权利要求9所述的方法,进一步包括:

使用该第二设备的加密状态变量,在该第二设备处产生第三组指示符值;和

如果接收的第三指示符与在该第二设备处使用该第二设备的加密状态变量所产生的指示符相匹配,则证实该第一设备。

11. 如权利要求10所述的方法,进一步包括:将接收的初始化向量存储在该第二设备的密钥数据库中。

12. 如权利要求10所述的方法,其中,该加密状态变量与加密的数据相关。

13. 如权利要求 12 所述的方法,其中,该加密状态变量是基于转轮的加密方案的转轮设置。

14. 如权利要求 10 所述的方法,其中,该第一设备为 RFID 标签,而该第二设备为 RFID 读取器。

15. 一种用于在对称加密系统中对通信进行安全认证的系统,所述系统包括:

具有加密状态变量的第一设备,该第一设备包括:

用于传送加密状态变量和指示符的传送器;

具有加密状态变量的第二设备,该第二设备包括:

用于从该第一设备接收加密状态变量的接收器;

用于存储加密密钥的密钥数据库;

用于使用从该密钥数据库接收的加密状态变量和加密密钥来产生指示符的加密逻辑;和

用于通过所使用的加密密钥,将产生的指示符值与接收的指示符值进行比较,以识别该第一设备的处理逻辑。

16. 如权利要求 15 所述的系统,其中,该处理逻辑确定接收的加密状态变量是否在该密钥数据库内。

17. 如权利要求 15 所述的系统,其中,该第一设备进一步包括:

用于响应于查询产生初始化向量并初始化加密状态变量的初始化逻辑;和

用于使用该加密状态变量来产生指示符值的加密逻辑。

18. 如权利要求 17 所述的系统,其中,所述初始化逻辑由 LFSR、计数器或随机数发生器中的任何一个组成。

19. 如权利要求 17 所述的方法,其中,所述查询包括用于产生所述初始化向量的标识符。

20. 如权利要求 17 所述的方法,其中,所述查询包括用于产生所述指示符的标识符。

21. 如权利要求 17 所述的系统,其中,该第二设备进一步包括:

用于传送由该处理逻辑产生的随机询问命令和由该加密逻辑通过对该第二设备的加密状态变量进行加密而产生的第二指示符的传送器。

22. 如权利要求 21 所述的系统,其中,该第一设备进一步包括:

接收器,用于接收该询问命令、查询和第二指示符;

处理逻辑,用于如果接收的第二指示符与使用该加密状态变量所产生的指示符相匹配,则证实该第二设备。

23. 如权利要求 22 所述的系统,其中,该第一设备的传送器传送第三指示符,所述第三指示符由该加密逻辑使用该加密状态变量而产生;而且,该传送器传送由该加密逻辑加密的初始化向量。

24. 如权利要求 23 所述的系统,其中,如果接收的第三指示符与使用该加密状态变量而产生的指示符相匹配,则该第二设备的处理逻辑证实该第一设备。

25. 权利要求 24 所述的系统,其中,该第二设备的密钥数据库存储接收的与该第一设备相关的初始化向量。

26. 如权利要求 24 所述的系统,其中,该加密状态变量与加密的数据相关。

27. 如权利要求 26 所述的系统,其中,该加密状态变量是基于转轮的加密方案的转轮设置。

28. 如权利要求 24 所述的系统,其中,该第一设备为 RFID 标签,而该第二设备为 RFID 读取器。

29. 一种用于在对称加密系统中对第一设备和第二设备之间的通信进行安全识别和认证的方法,所述方法包括 :

首先提供从该第一设备到该第二设备的安全识别 ;和
接着提供该第一设备和第二设备之间的安全认证。

30. 如权利要求 29 所述的方法,其中,提供安全识别的步骤包括 :

使用该第一设备的加密状态变量来产生指示符 ;

向该第二设备传送该加密状态变量和该指示符 ;

在第二设备处,对密钥数据库中的每一个加密密钥,将使用该加密密钥和接收的加密状态变量而产生的指示符与接收自该第一设备的指示符进行比较。

31. 如权利要求 30 所述的方法,其中,该第一设备和第二设备是 RFID 设备。

32. 如权利要求 31 所述的方法,其中,提供安全识别和安全认证的步骤被集成到 RFID 标准中。

33. 如权利要求 32 所述的方法,其中,RFID 标准是 EPCglobalGen 2 标准。

34. 如权利要求 33 所述的方法,其中,提供安全识别的步骤可提供为 EPCglobal Gen 2 标准的识别步骤。

用于在对称加密系统内安全地识别和认证设备的系统和方法

技术领域

[0001] 所描述的实施例总体上涉及用于在对称加密系统内对设备进行安全识别和认证的系统和方法，并且，更特别地，提供安全识别的方法，其使用低成本的、有效的密钥检索。

背景技术

[0002] 通信信道上的安全认证是系统安全的一个重要方面。当通信信道没有安全保护时，对手也许能拦截通信并模仿成另一方。必须发展能够经得起来自对手的重放、克隆及其他攻击的鲁棒认证协议 (Robust authentication protocol)，这些对手可能会拦截、修改或插入通信。

[0003] 由于低资源设备，特别是对无源 RFID 标签上施加的极限功率、存储器以及大小的限制，它们间的安全通信的问题尤其严重。这些约束意味着所述设备必须使用轻量加密技术，该加密技术要足够安全以经得起攻击，同时也要足够有效，以适应所述设备的限制和约束，特别是对具有极限约束的设备，例如，无源 UHF RFID 标签。对大多数受限的设备来说，大多数安全建议要么被证明是可轻易开发但不切实际的，要么要求过大的尺寸、过多的时间或过强的计算能力。此外，如果不对已制定的 RFID 标准（例如，EPCglobal Gen 2 标准）进行修改的话，这些建议通常不能集成到其中。

[0004] 典型地，安全通信要求在通信过程开始时执行两个基本功能：识别一个或更多的通信方，并认证这些通信方正是它们所声称的。传统上，低资源无线设备中的识别要么是手动执行，使得处理中涉及人，要么是在识别通信中没有安全性地执行。在这种情况下，典型地，在识别步骤之后，通过使用询问 - 应答协议来执行认证。

[0005] 执行没有安全保护的识别会带来安全和隐私风险。举例来说，如果个体携带的 RFID 标签广播它的识别信息，则可跟踪该个体的位置。如果该识别信息没有安全性，那么也比较容易克隆设备或执行重放攻击。

[0006] 典型地，为了识别通信方，那些还没有执行识别步骤的询问 - 应答认证协议要求大的密钥检索，在最坏的情况下，所述检索与数据库中的密钥的数目成线性比例。用二叉树检索协议处理密钥检索问题，因为检索代价与密钥的数目在对数上成比例。然而，二叉树检索方法要求标签存储 $O(\log N)$ 个密钥，还要求 $O(\log N)$ 次通信。此外，几个标签中密钥的泄密可能会破坏整个系统的安全性。

[0007] 同步方式避免大范围密钥检索的代价，这是因为，识别标签所需要的全部常常就是简单表查找。缺点是，如果由于秘密装置或硬件、通信或者其它故障，标签和读取器应变得不同步，则系统必须退回到穷举的密钥检索。

[0008] 大多数的加密方案使用块密码，其对多个字进行操作并且是大计算量的。使用块密码，接收器必须在算法可以开始之前等待整个块被接收，这就给加密和认证处理增加了额外的延迟。

发明内容

[0009] 在第一方面，一些实施例提供系统和方法，用于对在对称加密系统中的第一设备和第二设备之间的通信进行安全识别和认证，各设备具有加密状态变量。该第二设备从该第一设备接收加密状态变量。对该第二设备的密钥数据库中的各密钥来说，该第二设备使用加密状态变量和加密密钥来产生指示符，然后，将产生的指示符与从该第一设备接收的指示符进行比较，通过用来产生该指示符的加密密钥来识别该第一设备。在另一个方面，一些实施例确定接收的加密状态变量是否与该第二设备的密钥数据库中的加密密钥相关，以帮助识别该第一设备。

[0010] 在另一个方面，系统和方法的一些实施例可向该第一设备提供询问命令，以证实(validate)该第一设备的应答。该第二设备将产生询问命令，然后使用加密状态变量对此命令进行加密。通过对加密状态变量的当前状态进行加密，可产生第二指示符。然后，该询问命令和该第二指示符被传送到所述第一设备。在一些实施例中，该第一设备将接收询问命令并将对该询问命令进行加密。如果接收的第二指示符与在第一设备处使用加密状态变量所产生的指示符相匹配，则该第一设备将证实(validate)该第二设备。现在该第一设备可产生第三指示符，该第二设备可使用该第三指示符来证实该第一设备，前提是由于该第二设备所产生的指示符与该第一设备所传送的该第三指示符相匹配。

[0011] 在另一个方面，一些实施例提供一种用于在对称加密系统中对通信进行安全认证的系统。具有加密状态变量的第一设备包括传送器，用于传送加密状态变量和指示符。具有加密状态变量的第二设备包括用于接收加密状态变量的接收器；用于存储加密密钥的密钥数据库；用于使用从该密钥数据库接收的加密状态变量和加密密钥来产生指示符的加密逻辑；和，用于将产生的指示符值与接收的指示符值进行比较以通过所使用的加密密钥来识别该第一设备的处理逻辑。在另一个方面，在系统的一些实施例中，该第二设备的处理逻辑可确定接收的加密状态变量是否与密钥数据库中的加密密钥相关。在另一个方面，该第一设备还可包括用于响应于查询产生初始化向量并初始化加密状态变量的初始化逻辑；和，用于使用该加密状态变量来产生指示符值的加密逻辑。

[0012] 在另一个方面，一些实施例提供一种系统和方法，其通过首先提供从该第一设备到该第二设备的安全识别和其次提供该第一设备与该第二设备之间的安全认证，对在对称加密系统中的第一设备和第二设备之间的通信进行安全识别和认证。可通过如下方式提供该安全识别：使用该第一设备的加密状态变量来产生指示符；向该第二设备传送该加密状态变量和该指示符；和，在该第二设备处，对密钥数据库中的每一个加密密钥来说，将使用该加密密钥和所接收的加密状态变量而产生的指示符与从该第一设备接收的指示符进行比较。在另一个方面，通过提供安全识别信息，该系统和方法可被集成到 RFID 标准内，例如，EPCglobal Gen 2 标准，作为已知的 RFID 标准的一部分。

附图说明

[0013] 为了更好地理解这里所述的各实施例并且更加清楚地示出它们是如何实现的，下面仅以实例的方式参考附图，其示出至少一个示例性实施例，附图中：

[0014] 图 1 示出用于提供第一设备和第二设备之间的安全通信和认证的系统的实施例；

[0015] 图 2 示出同步的实施例的协议图；

- [0016] 图 3 示出同步的实施例的处理流程；
- [0017] 图 4 所示为异步的实施例的协议图；
- [0018] 图 5 示出异步的实施例的处理流程；
- [0019] 图 6 示出不安全的识别协议的实现；和
- [0020] 图 7 示出集成在普通 RFID 协议内部的实施例。

具体实施方式

[0021] 首先，参考图 1，其示出用于提供在通信信道 130 上进行通信的第一设备 110 和第二设备 120 之间的安全通信和认证的系统 100。第一设备 110 和第二设备 120 具有传送器 111、121 和接收器 112、122，用于在通信信道 130 上进行通信。在一些实施例中，该第一设备可为 RFID 标签，而该第二设备可为 RFID 标签读取器。

[0022] 通信信道可以是有线的或无线的，并可包括其它网络上的通信信道，例如，因特网或移动电话网络上的通信信道。设备可以是能够在该通信信道上进行通信的任何种类的设备。虽然 RFID 标签和读取器的例子被用于整个说明，但这里所描述的思想可应用于任何数量的通讯设备和网络，例如，移动电话、因特网装置、Bluetooth™ 设备或 WiFi 设备。

[0023] 第一设备 110 包括加密逻辑 113，其使用加密状态变量 114 实现加密算法。第一设备 110 还具有加密密钥 115，其用于通过加密逻辑 113 而实现的对称加密算法中。当对纯文本进行加密时，该加密逻辑将使用对称加密密钥 115 和加密状态变量 114。为了与第一设备 110 进行通信，另一设备必须知道加密密钥 115 和加密状态变量 114 的状态。加密逻辑 113 可被实现为由微处理器执行的软件模块，或被实现为 FPGA 或 ASIC 中的逻辑电路。

[0024] 在一些实施例中，该加密算法可以是基于转轮的加密算法 (rotor-based encryption algorithm)，而加密状态变量 114 可以是与任何影响转轮的状态或运动的其它变量在一起的转轮设置。由加密逻辑实现的加密算法可具有数据相关性和 / 或差错传播的性质。可使用任何使用对称密钥和加密状态变量的加密算法。术语加密状态变量用于表示加密逻辑的状态，但并不一定意味着值保存在存储器或其它寄存器中。块密码或任何变换都可用作转轮的替代。

[0025] 可在只有较少逻辑门的硬件上实现基于转轮的加密方案，并且，在计算上它要快于全尺寸的块密码。基于转轮的加密方案也可利用按比例缩小的块密码。虽然这些特征使得基于转轮的加密在高受限设备（例如，RFID 标签）中更为可取，但这里所描述的安全识别和认证的系统和方法并不限于基于转轮的加密算法的使用。

[0026] 第一设备 110 也可包括初始化逻辑 116，其被用于当第一设备 110 被查询时产生唯一的应答。该唯一的应答提供针对跟踪攻击或重放攻击的防御措施。初始化逻辑 116 可使用线性反馈移位寄存器 (LFSR)、计数器、随机数发生器或其它固定值、变化值或随机值产生器来产生初始化向量 117。在一些实施例中，初始化向量 117 可用在初始化程序中，其被用于使加密状态变量随机化。举例来说，在基于转轮的加密方案中，该初始化向量可用作初始的转轮设置，或者，如果该初始化向量的字长过短以至于不能填满初始的转轮设置时，可用零填充该初始化向量或复制该初始化向量以获得初始的转轮设置的正确字长。通过对初始的转轮设置或其组合进行加密，该初始化程序可循环转轮，以使转轮设置随机化。这个初始化程序应该能被第二设备 120 复制。

[0027] 初始化逻辑 116 也可使用标识符,例如,从查询设备接收的会话 ID,来产生初始化向量。在 RFID 标签实施例中,初始化逻辑可被实现为 LFSR,当标签被加电以响应来自读取器的命令或在正常标签作业程序下时,其被计时。使用无源 RFID 标签,被计时的 LFSR 状态可然后被保存在 RFID 标签上的非易失性存储器中,并且,一旦接收到另一查询,其被重新加载到 LFSR 中。

[0028] 第一设备 110 也可包括处理逻辑 118,其用于控制该设备的运行。这可包括控制初始化逻辑、控制加密逻辑、控制通信和控制用于实现认证系统的其它功能,下面将参照所述方法进行描述。处理逻辑 118 可被实现为由微处理器执行的软件模块,或被实现为 FPGA 或 ASIC 中的逻辑电路。

[0029] 第二设备 120 包括加密逻辑 123,其使用与该第一设备相同的加密算法。第二设备 120 从第一设备 110 接收该加密状态变量 114,并将其作为加密状态变量 124 存储在第二设备 120 内。在一些实施例中,使用加密密钥 115 或在这两个设备间共享的另一个秘密密钥,第一设备 110 也可对加密状态变量 114 进行加密。举例来说,通过执行该密钥和加密状态变量 114 的模 (modular) 2 或模 2^n 加法,该加密密钥或秘密密钥可用于使加密状态变量 114 模糊 (obfuscate)。

[0030] 第二设备 120 可安全访问密钥数据库 129,其存储所有已知设备的全部对称密钥。举例来说,在 RFID 实施例中,RFID 标签读取器可访问安全密钥数据库,其保存有系统内部所有已知的 RFID 标签所使用的加密密钥。密钥数据库 129 可位于第二设备 120 的内部,或安全连接至第二设备 120,这样,密钥数据库 129 内部的数据就不会泄露给攻击者。

[0031] 密钥数据库 129 将包括所有已知设备的对称密钥,而且,也可包括与各设备的加密状态变量相关的值。如果使用秘密密钥来对加密状态变量 114 进行加密,那么这个密钥也可存储在密钥数据库 129 中。在第二设备 120 恢复该加密状态变量之后,可使用恢复的加密状态变量来检索密钥数据库 129,并且,如果所述两个设备同步,则将发现匹配。密钥数据库 129 可以按加密状态变量来分类,或者,使用加密状态变量的散列,以允许较快的检索。

[0032] 第二设备 120 也可包括处理逻辑 128,其用于控制该设备的运行。这可包括控制加密逻辑、控制通信和控制用于实现识别和认证系统的其它功能,下面将参照所述方法进行描述。处理逻辑 128 可被实现为由微处理器执行的软件模块,或被实现为 FPGA 或 ASIC 中的逻辑电路。

[0033] 现在参照图 2,其示出用于同步交互认证和识别的方法的协议图 200。图 2 中所示的实施例说明使用 RFID 标签 202 和 RFID 读取器 204 的认证方法。RFID 标签读取器 204 通过向 RFID 标签 202 传送查询 206 来启动该方法。查询 206 还可伴有唯一标识符,例如,会话标识符,其可被用在 RFID 标签 202 的初始化程序中。

[0034] 一旦接收到查询 206,RFID 标签 202 就开始初始化步骤 208。通过产生来自线性反馈移位寄存器 (LESR) 或计数器的初始化向量 (IV),初始化步骤 208 创建各查询的唯一应答。这个步骤使得 RFID 标签 202 很可能将具有查询 206 的唯一应答。在 RFID 实施例中,这可包括当 RFID 标签加电时向计数器或 LFSR 加载来自非易失性存储器的值以及对 LFSR 或计数器计时,以产生所述初始化向量。接着,这个计时的值被存储在非易失性存储器,在下次查询 RFID 标签时将使用之。

[0035] 初始化步骤 208 也为加密算法所使用的任意加密状态变量设置初始值。在图 2 中所示的实施例中, 使用基于转轮的加密算法, 其中, 根据初始化向量 (IV) 来配置该算法所使用初始的转轮设置 (IRS)。如上关于初始化逻辑 116 所述, 为了达到唯一且不可预知的状态, IV 可经历另一个初始化程序, 这是为了使 IRS 进一步随机化。

[0036] 一旦完成该加密状态变量的初始化, 就可接着使用该加密算法来产生一组将识别设备的指示符值。在图 2 中所示的实施例中, 这些指示符值被表示为密文 CT_0 、 CT_1 和 CT_2 , 所述密文 CT_0 、 CT_1 和 CT_2 是通过对 $RS1+RS3$ 的和进行加密而产生的, 其中, $RS1$ 和 $RS3$ 是加密算法的转轮设置 1 和 3。类似地, 在块密码方法中, 可以以某种方式使用该状态变量, 将其作为加密算法的输入, 以产生所述密文。

[0037] 索引 $j+X$ 用于表明加密算法在初始化之后的第 X 次迭代, 并反映各迭代的转轮设置的变化。如果使用相同的加密状态变量和对称加密密钥, 那么, 通过使用内部变量, 例如, 加密状态变量或转轮设置, 接收器将能复制加密处理以产生指示符值。在会话标识符被传送到标签的实施例中, 该标识符也可用于产生指示符值。举例来说, 在图 2 中, 使用转轮设置和会话 ID (SSID) 来产生 CT_0 。

[0038] 如步骤 210 所示, 在产生指示符值之后, RFID 标签 202 向 RFID 读取器 204 传送该加密状态变量和该指示符值。可以使用秘密密钥 K 来使图 2 中所示的实施例中的加密状态变量或初始的转轮设置模糊, 其中, 秘密密钥 K 是标签和读取器所共享的。密钥 K 可以是来自驱动该加密算法的加密密钥的单独密钥。

[0039] 在接收到加密状态变量之后并在接收标签指示符之前, RFID 读取器 204 可立即开始该认证方法。如果该读取器和标签是同步的, 那么与该加密状态变量相关的值将在密钥数据库内。与该加密状态变量相关的值可以是步骤 212 中所示的初始的转轮设置, 或者, 其它实施例可使用下列之一或其任意组合: 初始化向量; 用于产生指示符值的初始的转轮设置的子集; 加密的初始的转轮设置; 和, 指示符值自身。在步骤 212 中, 读取器确定 IRS 是否是密钥数据库的一部分。如果已经识别了 RFID 标签, 则该加密算法将被配置为: 为所识别的 RFID 标签 202 使用加密状态变量和对称加密密钥。

[0040] 虽然已经识别了标签, 但出于额外的安全性, 类似于标签所执行的步骤, 读取器可产生标签指示符, 以检验读取器接收到的标签指示符都是相同的。为了对标签和读取器之间的加密状态变量进行同步, 执行这个步骤也可能是必需的。替代地, 该同步的加密状态变量可存储在数据库中。

[0041] 如果标签和读取器没有同步, 那么, 该加密状态变量就不会出现在密钥数据库内, 而读取器必须对数据库中的所有密钥执行穷举检索。对数据库内的各密钥来说, 读取器将恢复接收的加密状态变量, 并接着使用该加密状态变量来产生指示符值, 其方式与步骤 208 中使用的标签相同。如果产生的指示符值与读取器接收到的指示符值相匹配, 那么就已经识别了该密钥。参照图 3 中所示的处理流程更详细地描述所述密钥检索过程。

[0042] 在识别标签之后, 应当对标签进行询问, 确保标签对查询的应答并不单是之前广播的重放。在步骤 212 中, 读取器 204 将产生随机询问命令, 并接着对该命令进行加密。如果加密算法具有数据相关的性质, 那么, 通过对该加密状态变量进行加密可产生该询问命令的派生。结果可能被认作该询问命令的散列。在图 2 中所示的实施例中, 由 CMD_0 和 CMD_1 组成的询问命令被加密, 这促成转轮设置。这些转轮设置与之前的转轮设置和询问命令是

相关的。接着,对该转轮设置的和进行加密,以产生指示符值 CT_5' 和 CT_6' 。

[0043] 在步骤 214 中,该询问命令和该指示符值被传送到标签 202。一旦接收到该询问命令和指示符值,标签 202 就在该询问命令上执行操作,所述操作与读取器 204 在步骤 212 中执行的操作相同。在图 2 中所示的实施例中,在步骤 216 中进行这些步骤。如果该加密的加密状态变量与接收自标签 202 的指示符值相等,则标签 202 将对读取器 204 进行认证。如果接受读取器 204,那么,该读取器可进一步产生指示符值,显示为 CT_7 和 CT_8 ,并加密该初始化向量,显示为 CT_9 。接着,在步骤 218 中,该指示符值和该加密的初始化向量被传送到读取器 204。

[0044] 在步骤 220 中,读取器 204 执行操作以产生指示符值,所述操作与标签 202 在步骤 216 中的类似。在预期来自标签 202 的应答的步骤 212 之后,读取器可立即执行步骤 220。如果接收的指示符值与读取器 204 产生的指示符值相匹配,那么可认证该标签。为了同步标签 202 和读取器 204,读取器 204 可对接收的初始化向量进行解密,并将该值存储在密钥数据库中。如图 2 所示,所接收的 LFSR 值被传递给“UPDATE DATABASE”函数,作为其参数。在一些实施例中,该 UPDATE DATABASE 函数可使用接收的初始化向量,以产生加密变量,在下次查询标签时将由该标签使用之。此外,该函数可对加密变量进行加密,其方式与标签被查询后的相同,而且,该函数可将该加密的加密变量存储到密钥数据库中,以允许更快查找。如上所述,有许多可能的值与该加密状态变量相关,其可被存储在数据库中,仅作为例子提供的是初始化向量和 LFSR。

[0045] 一旦完成步骤 220,标签 202 应该准备接受询问命令外的任何命令。为了避免攻击者插入不期望的命令,标签 202 将对其接收的任何命令进行认证。这可以通过对读取器发送给标签 202 的各命令进行加密而完成。在图 2 中所示的 RFID 实施例中,标签 202 可受限于功率和尺寸的限制,导致它只具有加密功能。在这个实施例中,读取器可实现解密功能,以使来自攻击者的命令模糊,其可接着由标签 202 使用逆操作(即,加密功能)而得以恢复。在其它实施例中,会话标识符可与该命令一起传送,用于接收标签的补充认证。该会话标识符可类似地解密,这样标签就可通过该加密操作来恢复该会话标识符。用于命令认证的另一个选择包括用附加的二进制位来填充命令用于补充的认证,这样,当标签接收该命令时,它就可以确认所填充的二进制位与所接受的填充格式相匹配。

[0046] 步骤 222 示出被传送到标签 202 的解密命令和会话标识符。在步骤 224 中,为了恢复该命令和会话标识符,标签 202 接着执行该命令和会话标识符上的加密操作。如果该命令有效,则可接着由标签 202 执行之。

[0047] 现在参照图 3,其示出同步的实施例的处理流程 300。在步骤 302 中,RFID 读取器可向 RFID 标签传送查询和会话标识符。在步骤 304 中,该标签可接着产生来自 LFSR 或计数器的初始化向量(IV)。接着,在步骤 306 中,LFSR 或计数器的状态可被存储在非易失性存储器中,例如,EEPROM 中。接着,该初始化向量将经历初始化程序,以将该加密状态变量随机化。举例来说,在步骤 308 中,通过将初始化向量(IV)传递给 INIT 函数,来配置初始的转轮设置(IRS)。

[0048] 接着,在步骤 310 中,产生标签指示符,其中,读取器可使用所述标签指示符来识别标签。使用该加密算法和加密变量来产生该标签指示符。在图 3 中所示的实施例中,转轮设置 1(RS1) 和转轮设置 3(RS3) 是初始的转轮设置的子集,并与会话标识符一起被加密,

以产生被用作标签指示符的密文 CT_0 、 CT_1 和 CT_2 。

[0049] 在步骤 312 中,为了使在通信链路上传送的加密状态变量模糊,标签可使用秘密密钥 K,所述秘密密钥 K 可以是来自驱动该加密算法的加密密钥的单独密钥。该操作可以是使用该密钥对该加密状态变量执行模 2 或模 2^n 加法。举例来说,图 3 示出与密钥 K XOR 的 IRS。

[0050] 一旦该读取器从该标签接收了该加密状态变量,它就可以开始检索密钥数据库,以确定是否有匹配。如果发现匹配,则将该读取器和标签同步,并将该读取器加密算法配置为:使用从该密钥数据库接收的加密状态变量和对称加密密钥。如果该标签和读取器没有同步,那么该读取器必须对该数据库中的所有密钥执行穷举检索,以识别标签。在步骤 340 中,处理从将迭代变量 i 设置为 0 开始。只要 i 小于 N,处理步骤 342 就一直检索该密钥数据库,其中, N 是该密钥数据库中的密钥的总数。

[0051] 密钥检索处理的第一步是恢复该加密状态变量。在图 3 中所示的实施例中,在步骤 344 处,接收的 IRS 与密钥 K_i XOR,其中, K_i 代表该密钥数据库中的第 i 个标签条目的秘密密钥。恢复的 IRS 和 K_i 可接着被用于该加密算法。

[0052] 在步骤 346 处,为确定是否已经从数据库选择了正确的密钥条目,读取器在标签所使用的相同变量上执行相同的加密算法。如果该读取器所产生的标签指示符与该读取器所接收的标签指示符相等,在图 3 中显示为 $CT_0' = CT_0$,那么,就可能选择了正确的密钥。如果继续步骤 348 和步骤 350,分别比较 $CT_1' = CT_1$ 和 $CT_2' = CT_2$,那么该处理就可能选择了正确的密钥。各个连续的比较可除去候选密钥。一旦发现了正确的密钥,就可使用与数据库中的正确密钥相关的数据来识别该标签。可在各标签指示符上按照它接收的顺序相继执行这些步骤,根据所述执行可允许与该标签指示符的接收并行进行密钥检索。

[0053] 一些实施例可被配置为使用基于转轮的加密。通常,与典型的操作 128 位的块或更大的块的块密码相反,基于转轮的加密只操作较小的块,例如,16 位块。使用基于转轮的加密算法允许读取器比典型的块密码更有效和更快地除去可能的密钥匹配。

[0054] 如果任何比较步骤失败,那么,在步骤 343 处可增加迭代变量,并可测试数据库中的下一密钥。在比较测试中,数据库中的大多数候选密钥都会失败。因此,除去数据库的候选密钥的代价通常只是在小的块执行的单个加密操作。

[0055] 在步骤 352 中,读取器产生随机的询问命令,接着该询问命令被加密。接着,该读取器使用从属于识别的标签的密钥数据库接收的转轮设置和加密密钥,来产生指示符 CT_5' 和 CT_6' 。在步骤 354 中,该未加密的询问命令和该指示符接着被传送到所述标签。在产生询问命令并对其加密后,该读取器立即开始产生指示符 CT_7' 和 CT_8' ,如步骤 356 中所示。

[0056] 当标签接收询问命令时,它可以开始对该命令进行加密,并接着产生标签指示符,如步骤 358 中所示的 CT_5 和 CT_6 。在处理步骤 360 处,把在步骤 358 中所产生的标签指示符与接收自读取器的标签指示符进行比较。如果 $CT_5 = CT_5'$ 而 $CT_6 = CT_6'$,那么该标签证实该读取器,否则,该标签终止它与该读取器的通信。

[0057] 接着,该标签响应询问命令,其带有与该加密状态变量和初始化向量的状态相关的标签指示符。举例来说,在步骤 362 中,通过对 RS1 和 RS3 进行加密来产生标签指示符 CT_7 和 CT_8 ,而通过对 LFSR 进行加密来产生 CT_9 。在步骤 364 中,该标签指示符和该初始化向量

接着被传送到所述读取器。

[0058] 当接收该标签指示符时,读取器比较先前从步骤 356 产生的标签指示符是否与接收的标签指示符相匹配。如果标签指示符匹配,那么该读取器就会接受该标签为可信的。在步骤 368 中,可接着对接收的初始化向量进行解密,并用于更新数据库,以同步该读取器和标签,如步骤 370 中所示。

[0059] 现在,标签和读取器都已经被认证了,因此该标签准备接受不同于询问命令的命令。为了避免对手插入任何不期望的命令,该标签可对其接收的任何命令进行认证。在图 3 中所示的实施例中,标签只具有加密功能,因此读取器可在命令 (CMD) 上执行解密功能,而且,在一些实施例中,为了更高的保密性也可对会话标识符 (SSID) 进行解密,如步骤 372 中所示。对攻击者来说,这将具有对命令进行编码或加密的效果。在步骤 374 中,解密命令和会话标识符可接着被传送到标签。

[0060] 接着,标签可在接收的标签指示符上执行加密操作,以恢复命令和会话标识符,如步骤 376 中所示。接下来,在步骤 378 处,该标签确定该命令是否有效以及是否使用了正确的会话标识符,如果是,则在步骤 380 处执行该命令。

[0061] 现在参照图 4,其示出用于异步的交互认证和识别的方法的协议图 400。在这个实施例中,标签 402 可能没有可用的非易失性存储器来存储初始化向量的状态。既然该标签不能保存之前会话的状态,读取器就不能与该标签同步,而读取器将为各会话执行密钥数据库的密钥的穷举检索。图 4 的部件保持着图 2 的编号方案,其中,异步协议类似于同步协议。

[0062] 为了避免跟踪攻击,标签 402 应产生查询 406 的唯一应答。标签 402 可使用任何数量的方法来产生随机应答,举例来说,在图 4 中,从板载伪随机数发生器输出 64 位随机数 (RN64)。该随机数可接着被用作初始化向量。在步骤 409 中,与图 2 中所示的实施例中的步骤 208 相似,可接着进行加密算法和指示符值的产生的初始化。

[0063] 在步骤 411 中,标签 402 可接着向读取器传送加密状态变量和标签指示符。该加密状态变量可以是转轮设置自身或是初始化向量,其中,通过遵循类似于该标签所使用的初始化程序,从该初始化向量可得出加密状态变量。

[0064] 当接收该加密状态变量和标签指示符时,读取器必须执行密钥的穷举检索,以识别该标签。在步骤 413 中,当该标签和读取器没有同步时,类似于图 2 的实施例的步骤 212,读取器使用接收的数据对该加密状态变量进行初始化,并开始测试各密钥。协议的其他部分类似于图 2 中所示的实施例,除了步骤 417、419 和 421。这些步骤不再要求传送和在密钥数据库中存储初始化向量或加密状态变量,这是因为该标签产生随机应答且与该读取器不同步。

[0065] 现在参照图 5,其示出异步的实施例的处理流程 500。处理流程 500 类似于图 3 中所示的同步方法的处理流程,除了处理密钥数据库和初始化向量的步骤。图 5 的部件保持着图 3 的编号方案,其中,异步协议类似于同步协议。在异步方法的处理流程 500 中,在步骤 505 中,从伪随机数发生器产生初始化向量。当接收该初始化向量和标签指示符时,在步骤 540 到 550 中,该读取器必须执行密钥数据库的穷举检索。

[0066] 现在参考图 6,其示出不安全的识别协议的实现。协议 600 与 RFID 标签的 ECP Global Gen 2 标准中所使用的相类似。协议 600 的开始是在步骤 610 中由读取器 604 向

标签 602 发送查询。如步骤 612 中所示, 标签 602 可接着以由标签 602 产生的 16 位随机数作为应答, 其中, RN16 是该 16 位随机数。接下来, 在步骤 614 中, 读取器 604 通过发布具有与标签相同的 16 位随机数的确认命令, 来确认该标签。标签 602 可接着以产品电子代码 (EPC) 或其它识别标签 602 的信息作为应答, 如步骤 616 所示。在 EPC Global Gen 2 标准中, 在明文中 (in the clear) 传送这个识别信息。攻击者可拦截这个识别信息, 并使用它来追踪特定标签的位置, 或使用该信息来克隆该标签。在步骤 618 中, 标签处于开放状态, 并可响应许多命令。

[0067] 现在参考图 7, 其示出集成在普通 RFID 协议内部的实施例。如上参照图 1-4 所述的交互认证和识别的方法可被集成到 EPCglobalGen 2 标准中, 如协议 700 中所示。以上所述方法可能具有插入了 Gen2 标准的其它通信, 并且, 也可使用该标准的命令, 以执行部分协议。

[0068] 在图 7 中所示的协议中, 读取器 704 通过向标签 702 发送步骤 711 中所示的查询命令来启动协议。该查询命令也可包括数据, 例如, 读取器识别信息或会话识别信息。与图 6 中 Gen 2 标准的步骤 612 和 614 类似, 标签 702 以 16 位随机数作为应答, 而读取器 704 通过返回该 16 位随机数来进行确认。为产生 16 位随机数, 该标签可使用用于产生初始化向量的相同的 LFSR 或 PRNG。

[0069] 在发送该 16 位随机数之后, 标签 702 可接着对加密状态变量进行初始化并产生标签指示符, 如上所述。标签指示符的产生可使用读取器所传送的信息, 所述信息带有查询命令, 例如会话标识符或读取器标识符。响应于该查询命令而产生的该 16 位随机数也可用于标签指示符的产生。

[0070] 代替在明文中 (in the clear) 发送识别信息, 标签 702 现在可以把转轮设置或转轮设置可从其导出的值 (例如步骤 717 中的 IRS) 与所产生的标签指示符一起传送。EPCglobal Gen 2 标准规定协议控制和可被用于这个目的的扩展的协议字。于是, 根据以上所述方法, 读取器 704 将使用这个信息来执行密钥查找, 以识别标签 702。执行标签识别的方式是: 不允许攻击者知道该标签的身份或追踪该标签。

[0071] 在步骤 719 中, 根据以上所述方法, 读取器和标签现在可执行交互认证。

[0072] 这里, 仅仅通过实例描述了本发明。对这些示例性实施例可以做出各种修改和变化而不脱离仅由所附权利要求书所限定的本发明的精神和范围。

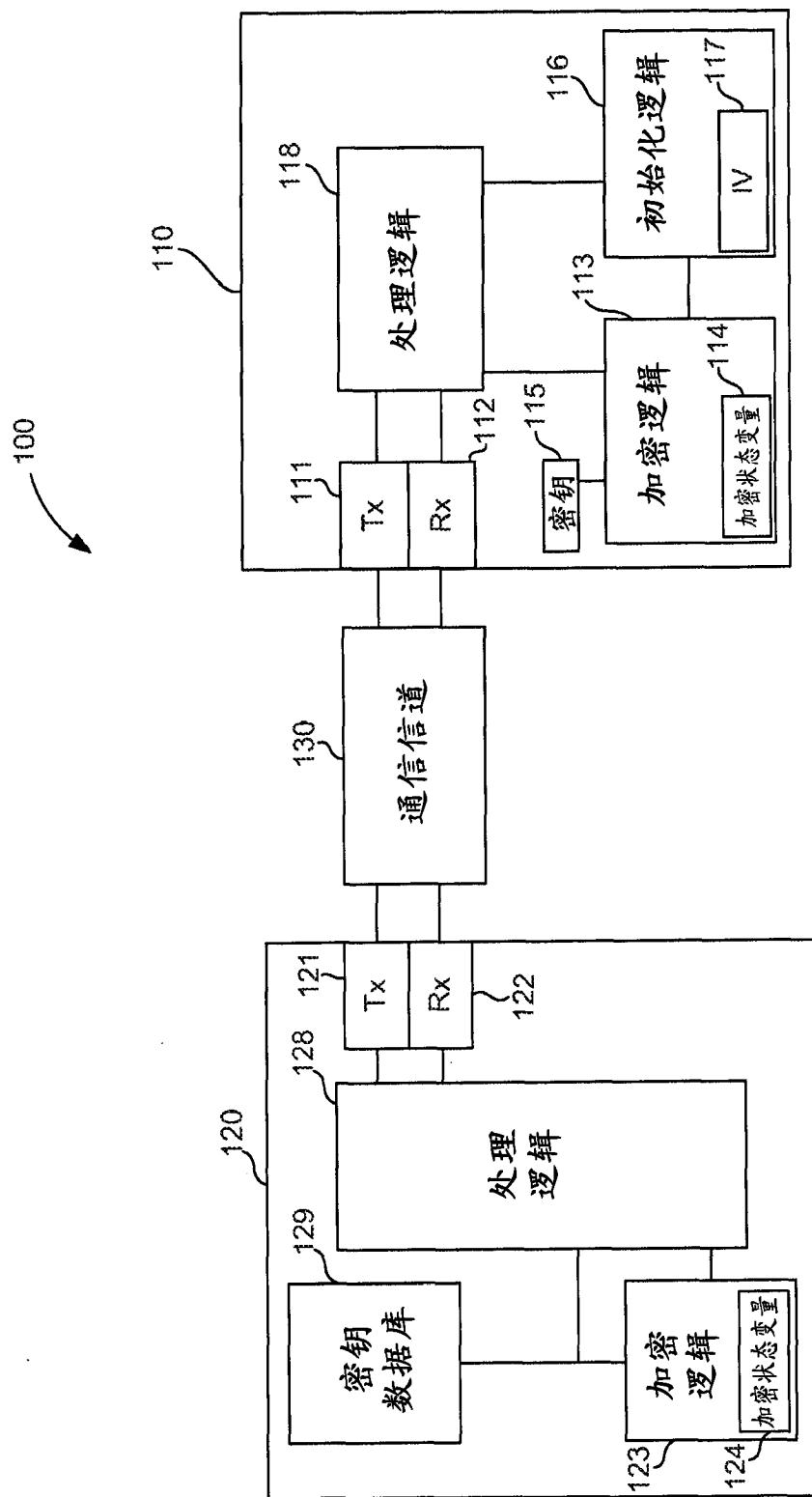


图 1

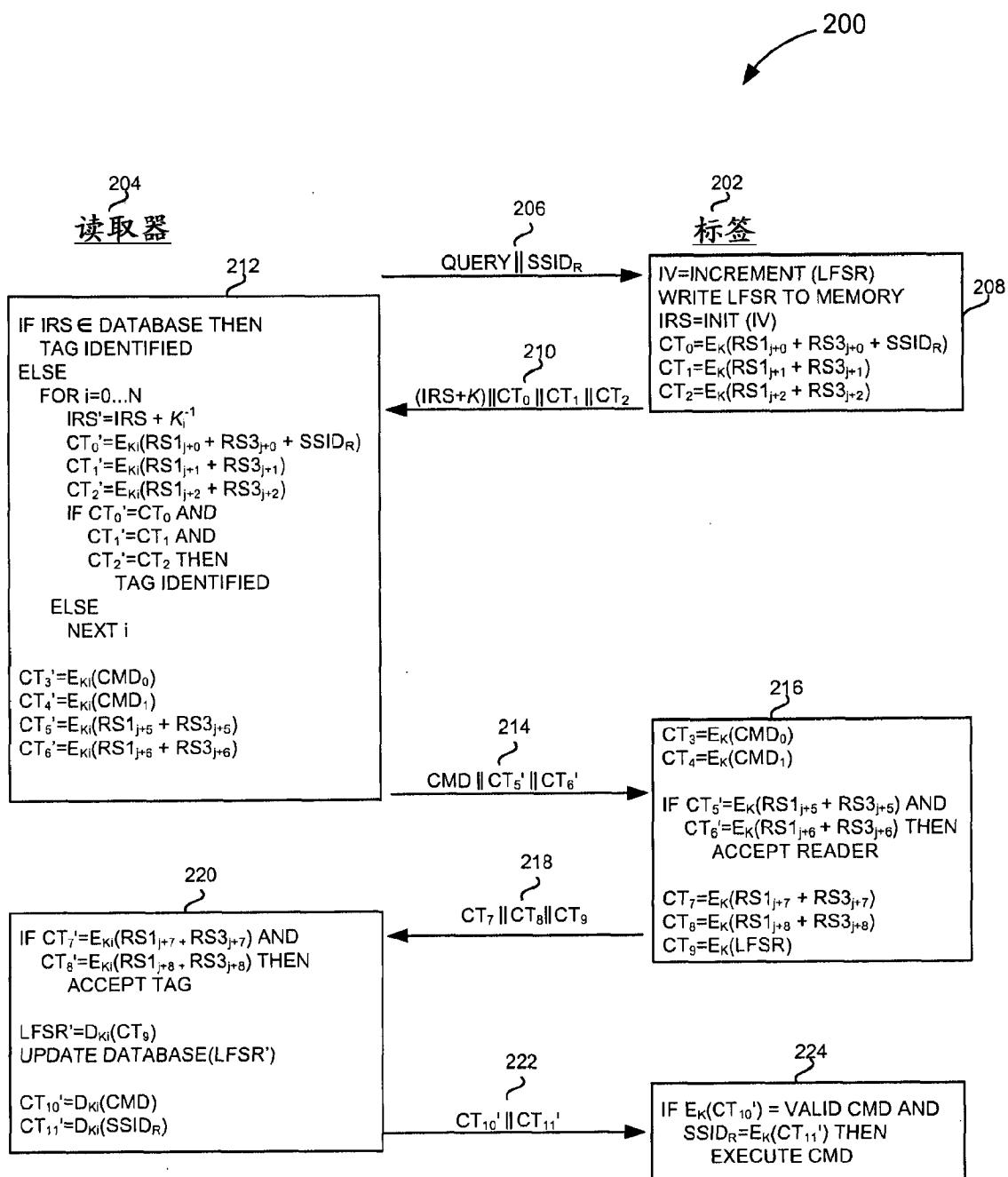


图 2

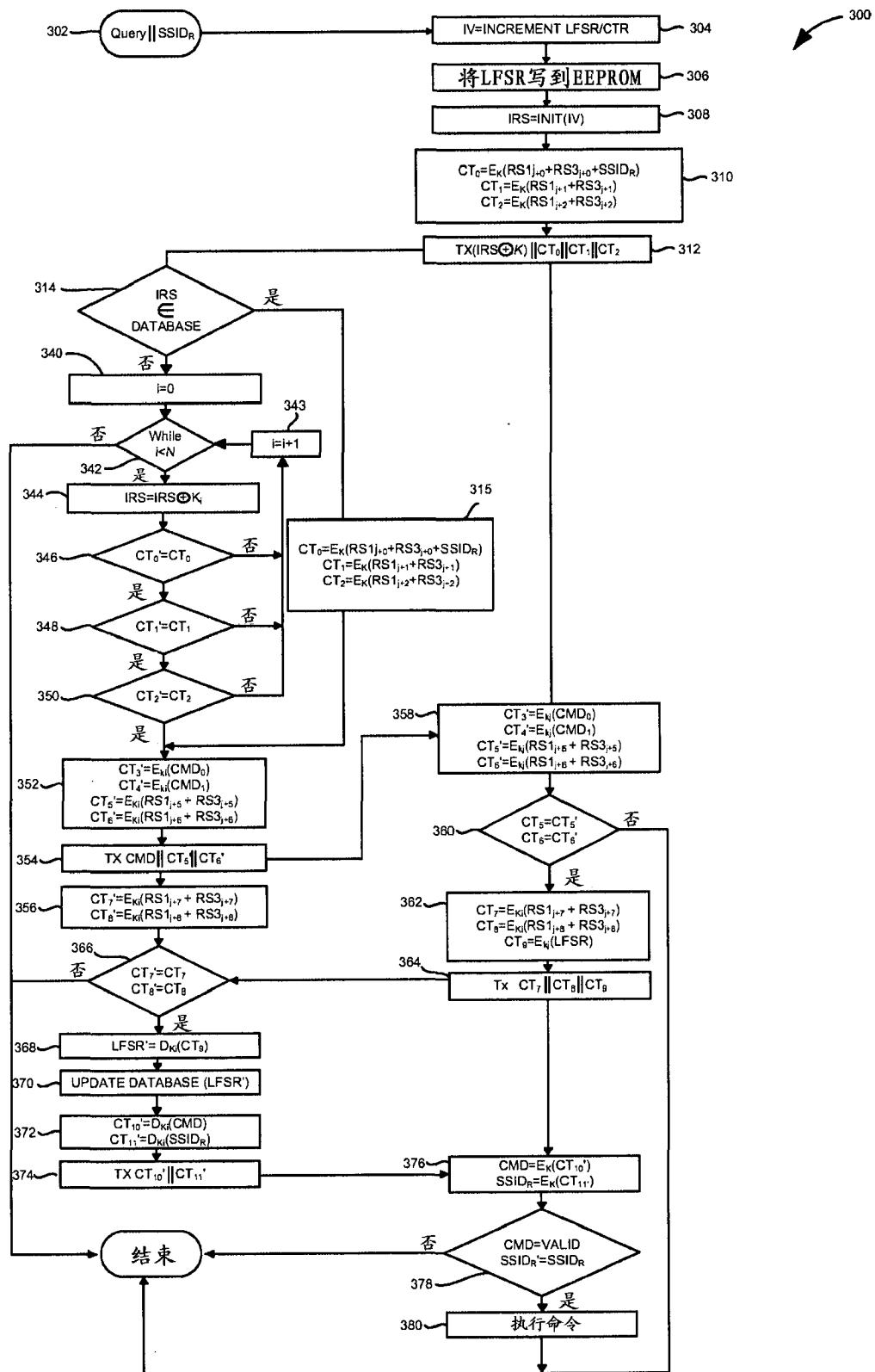


图 3

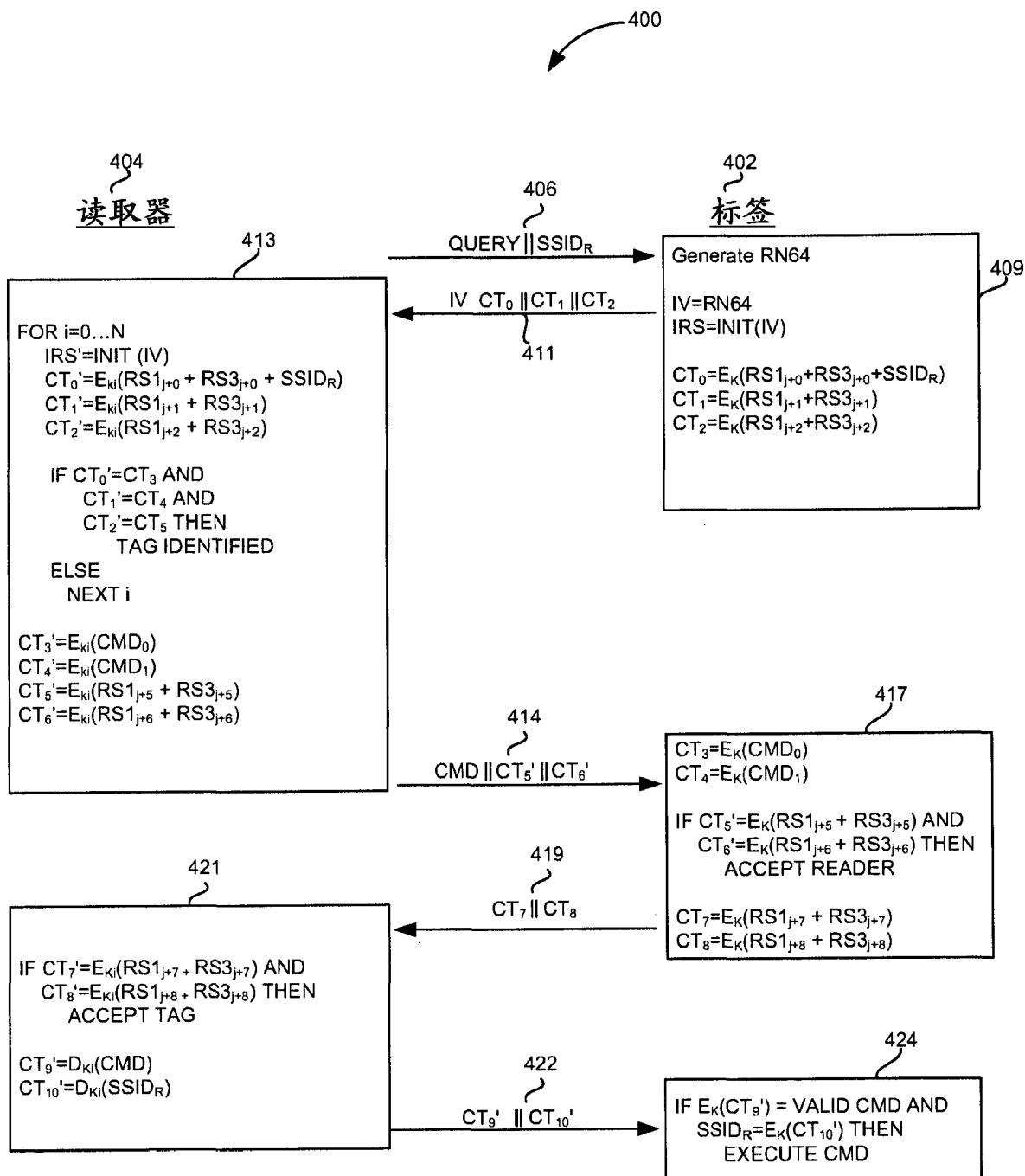


图 4

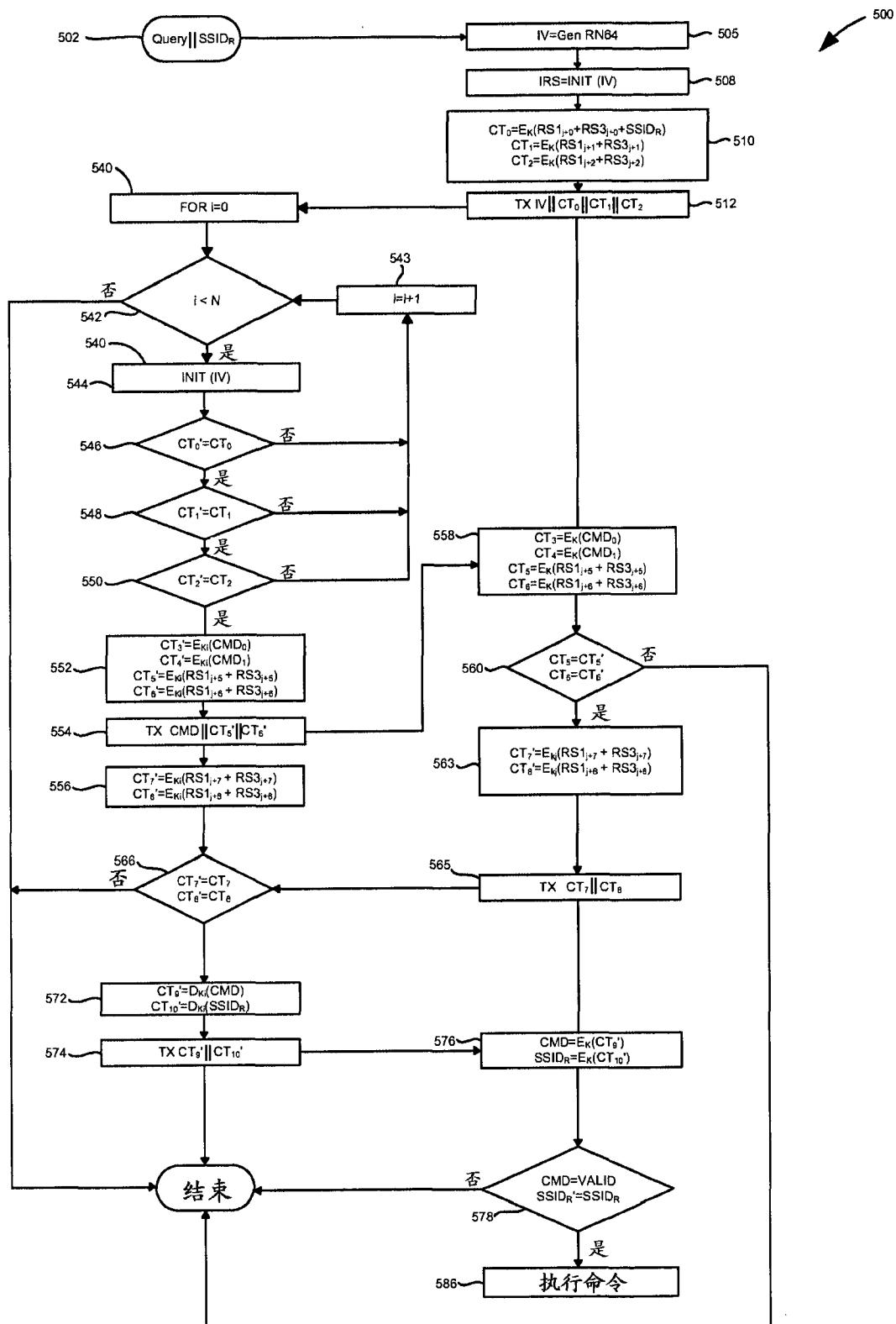


图 5

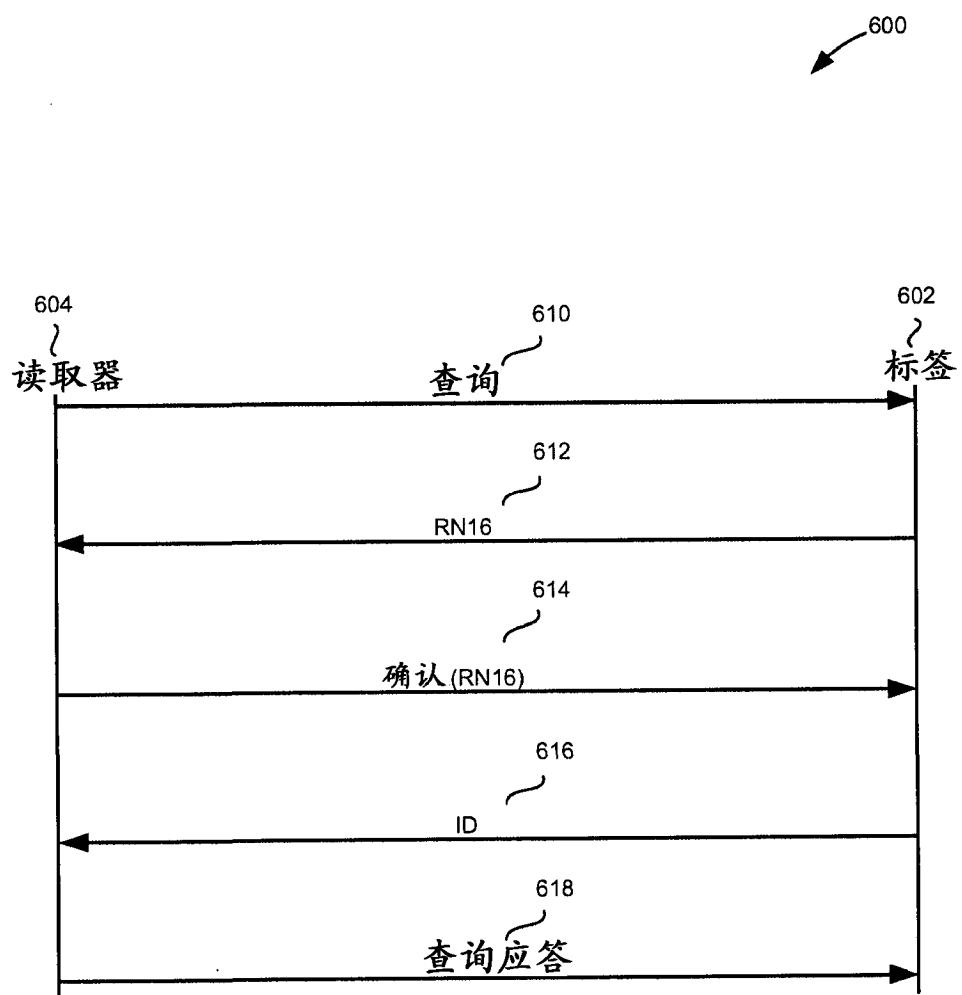


图 6

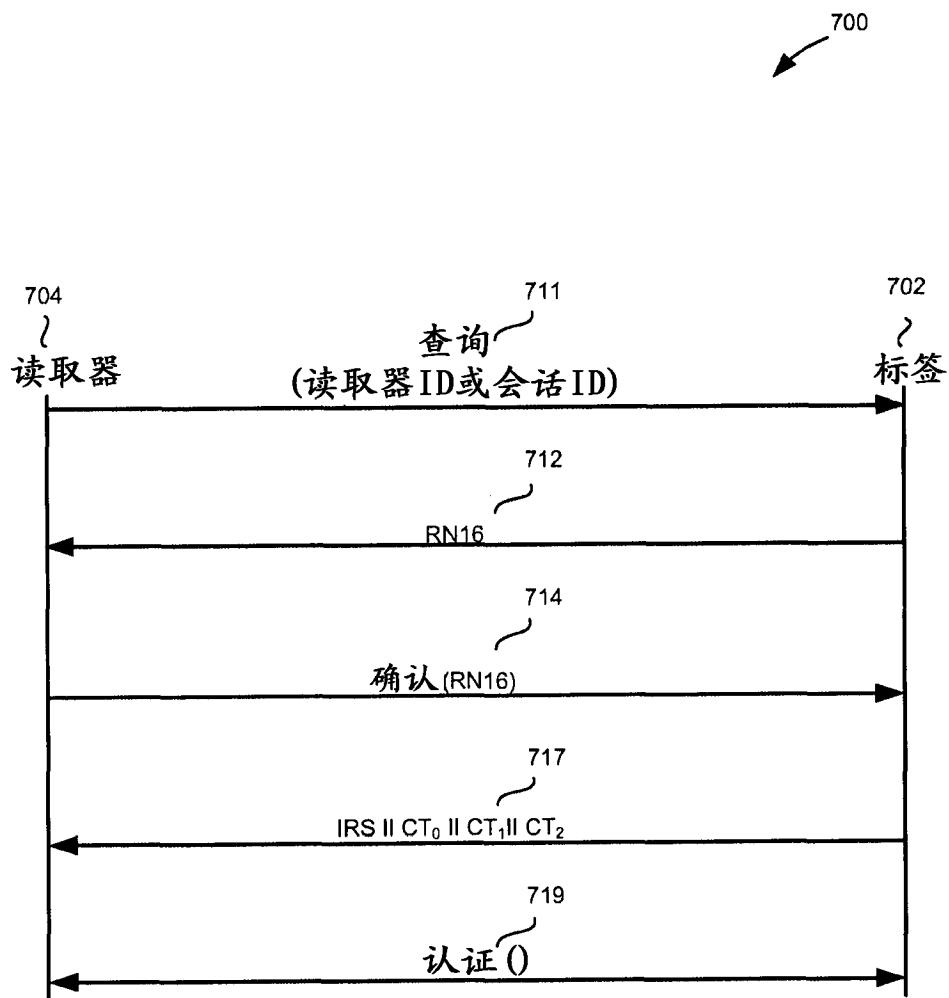


图 7