



## (12) 发明专利

(10) 授权公告号 CN 1736055 B

(45) 授权公告日 2010.10.13

(21) 申请号 200380108159.5

(51) Int. Cl.

(22) 申请日 2003.12.30

H04L 9/00(2006.01)

## (30) 优先权数据

H04K 1/00(2006.01)

60/438,617 2003.01.07 US

## (56) 对比文件

(85) PCT申请进入国家阶段日

CN 1285102 A, 2001.02.21, 全文.

2005.07.01

US 5761306 A, 1998.06.02, 权利要求 1 和说  
明书第 2 栏第 2 段到第 12 栏第 45 行.

(86) PCT申请的申请数据

WO 01/08347 A1, 2001.02.01, 说明书第 3 页  
第 18 行到第 8 页第 16 行.

PCT/US2003/041538 2003.12.30

US 5675649 A, 1997.10.07, 全文.

(87) PCT申请的公布数据

US 5201000 A, 1993.04.06, 全文.

W02004/064312 EN 2004.07.29

(73) 专利权人 高通股份有限公司

审查员 熊金安

地址 美国加利福尼亚州

(72) 发明人 G·G·罗丝 A·甘特曼

J·W·内伦贝格

(74) 专利代理机构 永新专利商标代理有限公司

72002

代理人 王英

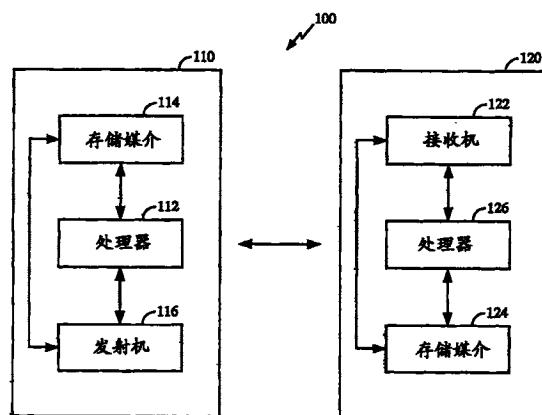
权利要求书 4 页 说明书 9 页 附图 5 页

## (54) 发明名称

替换密钥的系统、设备和方法

## (57) 摘要

实施例描述了一种方法和 / 或系统 (200), 由此可以替换加密系统中的密钥而不泄漏该密钥。一个实施例包括创建第一私钥 (210) 和相应的第一公钥。还创建了与所述第一私钥相关联的第二私钥和对应于该第二私钥的第二公钥 (220)。输出一次所述第二私钥 (230) 以使该第二私钥可以被重新创建，并且当输出所述第一公钥时输出所述第二公钥 (240)。所述第一私钥用于验证 (260)。所述方法还包括重新创建所述第二私钥；并使用该第二私钥进行验证。另一个实施例包括通过关联的系统参数来创建私钥和相应的公钥 (410)；当输出所述公钥时输出系统参数 (430)；并使用所述私钥进行验证 (460)。所述方法还可以包括使用先前的密钥和系统参数来创建新的私钥 (470)。



1. 一种用于在公共加密系统中进行验证的方法,其包括下列步骤 :

创建第一私钥和相应的第一公钥 ;

创建与所述第一私钥关联的第二私钥并创建对应于该第二私钥的第二公钥 ;

输出一次所述第二私钥,以使该第二私钥可以被重新创建 ;

当输出所述第一公钥时输出所述第二公钥 ;

使用所述第一私钥进行验证 ;

重新创建所述第二私钥 ;以及

使用该第二私钥进行验证。

2. 根据权利要求 1 的方法,其中,输出所述第二私钥包括 :

创建所述第二私钥的至少两个共享 ;以及

将每个共享输出一次给不同的实体。

3. 根据权利要求 1 的方法,还包括 :

当使用所述第二私钥进行验证时,使所述第一私钥失效。

4. 根据权利要求 1 的方法,还包括 :

创建与所述第二私钥相关联的第三私钥,并创建对应于该第三私钥的第三公钥 ;以及  
输出所述第三公钥。

5. 根据权利要求 4 的方法,还包括 :

输出一次所述第三私钥,以使该第三私钥可以被重新创建 ;以及

重新创建所述第三私钥并使用该第三私钥进行验证。

6. 根据权利要求 4 的方法,还包括 :

使用于验证的所述第二私钥的使用失效 ;

使用所述第三私钥进行验证 ;以及

重新创建所述第二私钥并使用该第二私钥进行验证。

7. 根据权利要求 1 的方法,还包括下列步骤 :

创建与所述第二私钥相关联的第三私钥,并创建对应于该第三私钥的第三公钥 ;

创建与所述第三私钥相关联的第四私钥,并创建对应于该第四私钥的第四公钥 ;

将所述第四私钥输出一次,以使该第四私钥可以被重新创建 ;以及

输出所述第三和第四公钥。

8. 根据权利要求 7 的方法,还包括 :

使用于验证的所述第二私钥的使用失效 ;以及

使用所述第三私钥进行验证。

9. 根据权利要求 8 的方法,还包括 :

重新创建所述第四私钥 ;以及

使用该第四私钥进行验证。

10. 一种用于在公共加密系统中进行检验的方法,其包括下列步骤 :

接收第一公钥 ;

接收与所述第一公钥相关联的第二公钥 ;

使用所述第一公钥进行验证 ;以及

如果所述第一公钥失败,则使用所述第二公钥进行验证。

11. 根据权利要求 10 的方法,还包括:

如果所述第一公钥失败并且所述第二公钥导致了成功的验证,则接收与该第二公钥相关联的第三公钥。

12. 根据权利要求 10 的方法,还包括:

如果所述第一公钥失败并且所述第二公钥导致了成功的验证,则接收第三公钥和第四公钥,其中所述第三公钥和第四公钥与所述第二公钥相关联。

13. 一种用于在公共加密系统中进行验证的设备,其包括:

用于创建第一私钥和相应的第一公钥的装置;

用于创建与所述第一私钥相关联的第二私钥并创建对应于该第二私钥的第二公钥的装置;

用于将所述第二私钥输出一次以使该第二私钥可以被重新创建的装置;

用于当输出所述第一公钥时输出所述第二公钥的装置;以及

用于使用所述第一私钥进行验证的装置;

用于重新创建所述第二私钥的装置;以及

用于使用所述第二私钥进行验证的装置。

14. 根据权利要求 13 的设备,其中,用于输出所述第二私钥的装置包括:

用于创建所述第二私钥的至少两个共享的装置;以及

用于将每个共享输出一次给不同的实体的装置。

15. 根据权利要求 13 的设备,还包括:

用于创建与所述第二私钥相关联的第三私钥并创建对应于该第三私钥的第三公钥的装置;以及

用于输出所述第三公钥的装置。

16. 根据权利要求 13 的设备,还包括:

用于创建与所述第二私钥相关联的第三私钥并创建对应于该第三私钥的第三公钥的装置;

用于创建与所述第三私钥相关联的第四私钥并创建对应于该第四私钥的第四公钥的装置;

用于将所述第四私钥输出一次以使该第四私钥可以被重新创建的装置;以及

用于输出所述第三和第四公钥的装置。

17. 一种用于在公共加密系统中进行检验的设备,其包括:

用于接收第一公钥的装置;

用于接收与所述第一公钥相关联的第二公钥的装置;

用于使用所述第一公钥进行验证的装置;以及

用于在所述第一公钥失败的情况下使用所述第二公钥进行验证的装置。

18. 根据权利要求 17 的设备,还包括:

用于在所述第一公钥失败并且所述第二公钥导致了成功的验证的情况下接收与该第二公钥相关联的第三公钥的装置。

19. 根据权利要求 17 的设备,还包括:

用于在所述第一公钥失败并且所述第二公钥导致了成功的验证的情况下接收第三公

钥和第四公钥的装置，其中所述第三公钥和第四公钥与所述第二公钥相关联。

20. 一种用于在公共加密系统中进行验证的方法，其包括下列步骤：

创建私钥、对应于该私钥的公钥和关联的系统参数；

当输出所述公钥时，输出所述系统参数；以及

使用所述私钥进行验证；

使用先前的私钥和系统参数来创建新的私钥；以及

使用该新的私钥进行验证。

21. 根据权利要求 20 的方法，还包括：

创建指出公钥和私钥的产生的计数器值；以及

当输出所述公钥时，输出该计数器值。

22. 根据权利要求 21 的方法，还包括：

基于所述计数器值，使用先前的私钥和系统参数来创建新的私钥。

23. 一种用于在公共加密系统中进行检验的方法，其包括下列步骤：

接收公钥；

接收与所述公钥相关联的系统参数；

使用所述公钥进行验证；以及

如果先前的公钥失败，则产生新的公钥并使用该新的公钥进行验证，所述新的公钥是从先前的公钥和系统参数导出的。

24. 根据权利要求 23 的方法，其中，产生所述新的公钥包括：

使用先前的公钥的若干次方进行验证；以及

接受作为新的公钥工作的一个公钥。

25. 根据权利要求 23 或 24 的方法，还包括：

接收指出私钥和公钥的产生的计数器值；以及

基于该计数器值，使用先前的公钥和系统参数来产生所述新的公钥。

26. 一种用于在公共加密系统中进行验证的设备，其包括：

用于创建私钥、对应于该私钥的公钥以及关联的系统参数的装置；

用于在输出所述公钥时输出所述系统参数的装置；以及

用于使用所述私钥进行验证的装置；

用于使用先前的私钥和系统参数来创建新的私钥的装置；

用于使用所述新的私钥进行验证的装置。

27. 根据权利要求 26 的设备，还包括：

用于创建指出公钥和私钥的产生的计数器值的装置；以及

用于当输出所述公钥时输出该计数器值的装置。

28. 根据权利要求 27 的设备，还包括：

用于基于所述计数器值，使用先前的私钥和系统参数来创建新的私钥的装置。

29. 一种用于在公共加密系统中进行检验的设备，其包括：

用于接收公钥的装置；

用于接收与所述公钥相关联的系统参数的装置；

用于使用所述公钥进行验证的装置；以及

用于在先前的公钥失败的情况下产生新的公钥并使用该新的公钥进行验证的装置,所述新的公钥是从先前的公钥和系统参数导出的。

30. 根据权利要求 29 的方法,其中,产生所述新的公钥包括:

用于使用先前的公钥的若干次方进行验证的装置;以及

用于接受作为新的公钥工作的一个公钥的装置。

31. 根据权利要求 29 或 30 的设备,还包括:

用于接收指出私钥和公钥的产生的计数器值的装置;以及

用于基于该计数器值,使用先前的公钥和系统参数来产生所述新的公钥的装置。

## 替换密钥的系统、设备和方法

### 技术领域

[0001] 本发明通常涉及加密系统，并且更具体地涉及用于加密系统的密钥的产生和替换。

### 背景技术

[0002] 可以利用公钥加密来产生加密签名。在公钥加密系统中，用户具有私钥 (private key) 和公钥 (public key) 来对文档进行验证。共享公钥而保密私钥。用户通过将通信连同数字签名一起发送给目标实体或一方，以用户私钥来对通信签名，所述目标实体或一方然后通过用户公钥来检验所述通信和数字签名。

[0003] 在一个应用中，公钥加密系统可以被实现在便携式设备中（下文中为令牌）。针对令牌产生私钥和公钥。所述私钥被保留在令牌中，而发送所述公钥给一个或多个目标实体。所述令牌因而可以由所有者使用以建立与目标实体的各种关系，从而能够进入门 (door)，访问银行帐目、计算机网络等。

[0004] 然而，令牌（并且因此私钥被存储在其中）可能被偷窃、或可选地被损坏、丢失或破坏。如果令牌被偷窃，则当盗贼拥有该令牌时限制他们所进行的破坏是很重要的。如果不管出于何种原因其所有者不能再使用所述令牌，则问题在于当重新建立令牌所使能的各种关系时，对于所有者而言存在不止一个的主要不便利因素。

[0005] 因此，需要一种在令牌中替换密钥的更方便、有效和 / 或机密的方法。

### 发明内容

[0006] 实施例描述了一种方法和 / 或系统，由此可以替换密钥而不泄漏该密钥。更具体地，例如，令牌的所有者可以为了其将来的替换预作安排而此时不用泄漏密钥。例如，当使用替换令牌时，可以对其进行暗中检验，并且验证器将利用使用新令牌的动作而使旧的令牌失效。这对至少两个原因而言是重要的。第一，如果初始令牌被偷窃，则小偷将不再能够通过所述验证器使用该被偷的令牌。第二，如果不知何故地滥用针对将来使用的安排，并且在不知道令牌所有者的情况下而产生新的令牌，则当利用现有令牌的验证被拒绝时，所有者将很快知道这个情况。因此，所有者可以采取其它校正动作。

[0007] 在一个实施例中，用于在公共加密系统中进行验证的方法包括创建第一私钥和相应的第一公钥。也创建与所述第一私钥相关联的第二私钥以及对应于所述第二私钥的第二公钥。将所述第二私钥输出一次以使该第二私钥可以被重新创建，并且当输出所述第一公钥时输出所述第二公钥。使用所述第一私钥进行验证。所述方法还包括重新创建所述第二私钥；以及使用所述第二私钥进行验证。

[0008] 当使用所述第二私钥进行验证时，所述第一私钥可能失效。此外，可以创建与所述第二私钥相关联的第三私钥，以及对应于第三私钥的第三公钥。可以将所述第三公钥输出一次以使该第三公钥可以被重新创建。所述第三私钥因而可以被重新创建并被用于验证。可选地，可以使用于验证的所述第二私钥的使用失效并且所述第三私钥可以被用于验证。

所述第二私钥因而可以被重新创建并被用于验证。

[0009] 所述方法还可以包括创建与第二密钥相关联的第三私钥，并创建对应于所述第三私钥的第三公钥；创建与所述第三私钥相关联的第四私钥，并创建对应于所述第四私钥的第四公钥；将所述第四私钥输出一次以使该第四私钥可以被重新创建；并且输出所述第三和第四公钥。可以使用于验证的所述第二私钥的使用失效并且所述第三私钥被用于验证。所述第四私钥可以被重新创建并被用于验证。此外，输出所述第二公钥可能包括创建该第二公钥的至少两个共享，并且将每个共享输出一次给不同的实体。

[0010] 在另一个实施例中，用于加密检验的方法包括接收第一公钥；接收与该第一公钥相关联的第二公钥；利用所述第一公钥进行验证；并且如果所述第一公钥失败则使用所述第二公钥进行验证。所述方法还包括如果所述第一公钥失败并且所述第二公钥导致了成功的验证，则接收与该第二公钥相关联的第三公钥。可选地，所述方法包括如果第一公钥失败并且所述第二公钥导致了成功的验证，则接收与该第二公钥相关联的第三公钥和第四公钥。

[0011] 在另一个实施例中，用于验证的方法包括通过关联的系统参数来创建私钥和相应的公钥；当输出所述公钥时输出所述系统参数；并且使用所述私钥进行验证。所述方法还包括使用先前的私钥和系统参数来创建新的私钥。可以创建指出所述公钥和私钥的产生的计数器值，并且当输出所述公钥时输出该计数器值。然后基于所述计数器值，利用先前的私钥和系统参数，创建新的私钥。

[0012] 此外，在另一个实施例中，用于检验的方法包括接收公钥；接收与该公钥相关联的系统参数；使用该公钥进行验证；以及产生新的公钥并使用该新的公钥进行验证，其中，所述新的公钥是从先前的公钥和系统参数导出的。所述方法还包括利用先前公钥的若干次方进行验证；以及接受作为新的公钥工作的一个公钥。可选地，所述方法还包括接收指出所述私钥和公钥的产生的计数器值；以及基于该计数器值，利用先前的公钥和系统参数来产生新的公钥。

[0013] 在另一个实施例中，用于在公共加密系统中进行验证的设备可能包括用于创建第一私钥和相应的第一公钥的装置；用于创建与该第一私钥相关联的第二私钥并创建对应于该第二私钥的第二公钥的装置；用于输出一次所述第二私钥以使该第二私钥可以被重新创建的装置；用于当输出所述第一公钥时输出所述第二公钥的装置；以及用于使用所述第一私钥进行验证的装置。可选地，用于在公共加密系统中进行验证的设备可能包括，用于通过关联的系统参数来创建私钥和相应的公钥的装置；用于当输出所述公钥时输出所述系统参数的装置；以及使用所述私钥进行验证的装置。

[0014] 在另一个实施例中，用于在公共加密系统中进行检验的设备包括用于接收第一公钥的装置；用于接收与所述第一公钥相关联的第二公钥的装置；使用所述第一公钥进行验证的装置；以及如果所述第一公钥失败则使用所述第二公钥进行验证的装置。可选地，用于在公共加密系统中进行检验的设备可能包括用于接收公钥的装置；用于接收与所述公钥相关联的系统参数的装置；使用所述公钥进行验证的装置；以及如果先前的公钥失败，用于产生新的公钥并使用该新的公钥来进行验证的装置，所述新的公钥是从先前的公钥和系统参数导出的。

[0015] 在另一个实施例中，公共加密系统中的机器可读媒介可能包括用于创建第一私钥

和相应的第一公钥的一组代码段；用于创建与所述第一私钥相关联的第二私钥并创建对应于该第二私钥的第二公钥的一组代码段；用于输出一次所述第二私钥以使该第二私钥可以被重新创建的一组代码段；用于当输出所述第一公钥时输出所述第二公钥的一组代码段；以及使用所述第一私钥进行验证的一组代码段。在公共加密系统中进行验证的机器可读媒介包括，用于通过关联的系统参来创建私钥和相应的公钥的一组代码段；用于当输出所述公钥时输出所述系统参数的一组代码段；以及使用私钥进行验证的一组代码段。

[0016] 在另一个实施例中，公共加密系统中的机器可读媒介可能包括，用于接收第一公钥的一组代码段；用于接收与该第一公钥相关联的第二公钥的一组代码段；使用所述第一公钥进行验证的一组代码段；以及如果所述第一公钥失败则使用所述第二公钥进行验证的一组代码段。公共加密系统中的机器可读媒介可能包括，用于接收公钥的一组代码段；用于接收与该公钥相关联的系统参数的一组代码段；使用所述公钥进行验证的一组代码段；以及如果先前的公钥失败，用于产生新的公钥并使用该新的公钥进行验证的一组代码段，所述新的公钥是从先前的公钥和系统参数导出的。

## 附图说明

[0017] 将参考下面的附图详细描述各种实施例，附图中同样的参考号码代表同样的元件，其中：

- [0018] 图 1 示出了加密系统的一个实施例；
- [0019] 图 2 示出了用于从用户设备进行验证的方法；
- [0020] 图 3 示出了用于从检验器设备进行检验的方法；
- [0021] 图 4 示出了用于从用户设备进行验证的另一个方法；以及
- [0022] 图 5 示出了用于从检验器设备进行检验的另一个方法。

## 具体实施方式

[0023] 通常，所描述的实施例允许用于将来替换密钥的提供而不泄漏该密钥。在下面的描述中给出了特定的细节以提供本发明的全面理解。然而，一个本领域的普通技术人员应当理解，可以在没有所述特定细节的情况下实施本发明。例如，为了不以不必要的细节而使本发明变得难以理解，可以以框图的形式来示出电路。在其它情况下，为了不使本发明变得难以理解，可以详细示出众所周知的电路、结构和技术。

[0024] 应当指出，本发明可以被描述为过程，该过程被描述为流程图、作业图、结构图或框图。尽管流程图可以将所述操作描述为连续过程，但是可以平行或同时执行许多操作。此外，可以重新安排操作的顺序。过程终止于其操作完成时。过程可以对应于方法、函数、过程、子例程、子程序等等。当过程对应于函数时，其终止对应于该函数到调用函数或主函数的返回。

[0025] 图 1 示出了包括用户设备 110 和验证设备 120 的加密系统 100 的一个实施例。可以在令牌、便携式电话、个人数据助理、(桌面或膝上) 个人计算机或其它电子设备中实现用户设备 110。可以通过例如银行、代理人或例如 Verisign 公司的托管第三方的实体来实现检验器设备 120。尽管图 1 示出了一个检验器设备 120，然而本领域的技术人员应当知道可能存在一个或多个检验器设备。

[0026] 用户设备 110 包括产生和处理密钥的处理器 112、存储所产生的密钥的存储媒介 114 和发送通信的发射机 116。在公钥加密系统中，所述私钥是保留在用户设备 110 中的密钥，而使用发射机 116 将所述公钥发送给检验器设备 120。然后以所述私钥来对通信签名，并将该通信发送给检验器设备 120 以进行验证。

[0027] 检验器设备 120 包括接收来自用户设备 110 的通信的接收机 122、存储所接收的通信的存储媒介 124 和验证通信的处理器 126。存储媒介 124 也可以实现验证数据库以存储发送自用户设备 110 的公钥。更具体地，接收机 122 接收所述公钥并创建存储在所述存储媒介 124 中的验证数据库。当检验器设备 120 接收签名的通信以进行验证时，从所述验证数据库获得相应的公钥并使用该公钥来检验所述通信。应该指出，可以在与存储媒介 124 和 / 或检验器设备 120 不同位置和 / 或在其外部的位置来实现所述验证数据库。

[0028] 图 2 示出了产生用于公钥加密系统的密钥的方法 200。处理器 114 创建 (210) 第一组密钥，即第一私钥和相应的第一公钥。处理器 114 还创建 (220) 第二组密钥，即第二私钥和相应的第二公钥。所述第二组密钥与所述第一组密钥相关联。然而，与第一组无关地创建第二组。可以使用现有技术中已知的各种算法来产生所述密钥。

[0029] 例如，可以基于众所周知的数字签名标准 (DSS) 来产生密钥。这里，处理器 114 使用随机的内部源来创建将被用于 DSS 的私钥或密钥  $x$ 。然后如下计算相应的公钥  $X$ ，其中  $P$  是较大的质数，例如 1024 比特，其定义了进行数学操作的数学域， $Q$  是另一个质数，典型地是 160 比特或更大，以使  $Q \mid (P-1)$ ，并且  $g$  是所述域的元素以及  $F^*(P)$  的  $Q$  阶子群的产生器。

[0030] 
$$X = g^x \pmod{P}$$

[0031] 可以将密钥初始存储在存储媒介 114 中。所述第一私钥保存在用户设备 110 中，并输出所述第二私钥以使即使用户设备 110 被偷窃、丢失或损坏也可以重新创建该第二私钥。这里，所述第二私钥可能保存在用户设备 110 中，并且输出所述第一私钥以使该第一私钥可以被重新创建。然而，为了解释的目的，假设输出所述第二私钥。保存在用户设备 110 的密钥是用于验证的主要密钥并且变为现用。所输出的私钥是将来替换的密钥并且变为待用。

[0032] 在用户设备 110 的所有者的请求下，输出一次所述第二私钥 (230)。此后，用户设备 110 不再响应所述请求。当输出所述第一公钥时也输出所述第二公钥 (240)。这里，可以使用发射机 116 来输出所述第二私钥和公钥。

[0033] 在一个实施例中，可以使用秘密共享方案，由此在用户设备 110 内创建秘密信息的  $n$  个共享，并将其独立地发送给值得信赖的股东以使稍后  $k$  个 ( $k < n$ ) 股东可以重新创建所述秘密信息。值得信赖的股东可能是 (但不限于) 用户设备 110 的所有者；该所有者的值得信赖的朋友；例如银行、会计师或其它金融机构的已经具有该所有者的秘密信息的一方；或例如 Verisign 的“托管第三方”。

[0034] 例如，用户设备 110 的处理器 114 可以创建所述私钥的三个共享。可以在用户的请求下利用发射机 116 一次一个地输出所述共享。每个共享被输出一次给指定的三方之一。在输出所有共享之后，用户设备 110 将不再响应所述请求。然而，所述用户可以通过所述三方中任何两个的合作来重新创建所述密钥，而三方中的任一个都不能独自重新创建所述私钥，一方应当是不可信赖的。此外，如果所述方之一失去其共享，则其它两个仍可以提供创建替换所需的信息。如果实现了秘密共享方案，所述第一私钥保留在用户设备 110 中，并且

输出所述第二私钥作为共享以使该第二私钥可以被重新创建。应当理解，可以创建所述私钥的多于或少于三个的共享，并将其输出给对应数目的一方或多方。

[0035] 再次参考图 2，如果所述第一私钥是现用的，则当验证时使用该第一私钥 (250 和 260)。即，用户设备 110 以所述第一私钥来签名通信并发送具有关联的签名的通信给目标方，所述目标方然后通过所述第一公钥来检验所述通信。如果所述第一私钥不是现用的，则使用所述替换私钥，即所述第二私钥，来进行验证 (270)。

[0036] 由于各种原因，第一私钥可能不是现用的。例如，由于用户设备 110 和 / 或第一私钥被偷窃、损坏、丢失和或破坏，用户设备 110 的所有者可能已经替换了所述第一私钥。更具体地，用户设备 110 的所有者可能没有激活所述第一私钥和 / 或使其失效。在所述情况下，所述第二私钥被重新创建并被用于验证。可选地，在某些加密系统中私钥可能过期。如果所述第一私钥过期，则所述第二私钥由用户设备 110 重新创建并被用于验证。在某些实施例中，用户设备 110 可以被配置以使所述替换私钥的使用使得现有主要私钥失效，在所述情况下该主要私钥是所述第一私钥。这里，如果用户设备 110 被偷窃、损坏、丢失和 / 或破坏，则重新创建私钥可能意味着替换所述设备，例如从旧令牌到新令牌。否则，如果仅是所述密钥被偷窃、丢失和 / 或过期，则重新创建私钥可能意味着在用户设备 110 内改变私钥。

[0037] 当重新创建和使用所述第二私钥进行验证时，所述第二私钥替换所述第一私钥并变为现用。因此，处理器 112 创建 (280) 和输出 (290) 与该第二私钥相关联的一组新的替换密钥。即，第三组密钥被创建并被输出作为将来的替换密钥。与所述第一和第二组密钥一样，当所述第三组密钥关联于所述第二组密钥时，与该第二组无关地创建该第三组。同样，所述第二私钥被保存在用户设备 110 中，而输出所述第三私钥以使其可以被重新创建。这里，例如使用现有技术中众所周知的沙米尔 (Shamir) 共享方案，可以将所述第三私钥输出一次给一个或多个相同或不同的实体。当输出所述第二公钥时，可以使用例如发射机 116 输出所述第三公钥。

[0038] 如果第二密钥变为待用，则第三私钥可以被重新创建以替换所述第二私钥并被用于验证。在所述情况下，另一组新的替换密钥，例如第四组密钥，被重新创建并作为将来的替换密钥被输出。更具体地，当替换私钥被重新创建，并且变为新的主要密钥以替换先前的主要私钥时，一组替换密钥被创建并作为将来的替换密钥被输出。如果所述第三私钥变为待用，则第四私钥可以被重新创建并被用于验证，而第五组密钥被创建并作为将来的替换密钥被输出。所述密钥的创建、输出和重新创建可以在需要时如上所述地重复发生以替换先前的密钥。在某些实施例中，可以替换密钥的次数可能受限。同样，处理器 114 可能重新创建替换私钥并使用该重新创建的密钥进行验证。通过针对每个新的主要私钥预先创建一组替换密钥，私钥可以被替换而不被泄漏。

[0039] 图 3 示出了对应于方法 200 的用于验证通信的方法 300。检验器设备 120 接收 (310) 来自用户设备 110 的第一公钥和第二公钥，其中所述第一公钥对应于第一私钥并且而所述第二公钥对应于第二私钥。所述第二私钥与第一私钥相关联，并且因此所述第二公钥与所述第一公钥相关联。存储所述公钥在存储媒介 124 的验证数据库中。这里，将一个公钥作为现用的主要公钥进行存储，而将另一个公钥作为待用的替换公钥进行存储。在所述例子中，所述第一公钥是主要密钥而所述第二公钥是替换密钥。同样，可以使用接收机 122 接收所述第一公钥和第二公钥。

[0040] 当从用户设备 110 接收了用于验证的签名通信时，处理器 126 通过所述主要公钥尝试验证（320 和 330），该主要公钥即是本例中的第一公钥。即，所述第一公钥从所述验证数据库被检索并被用于检验所述通信。如果不能使用所述第一公钥检验所述通信，则处理器 126 使用（340 和 350）所述替换公钥以尝试所述签名通信的验证，该替换公钥即是本例中的与所述第一公钥相关联的第二公钥。如果成功，则检验器设备 120 可以假定所述第一私钥已经被替换。

[0041] 检验器设备 120 还接收（360）来自用户设备 110 的新的替换公钥，即第三公钥，并更新（370）所述验证数据库。检验器设备 120 可以接收具有签名检验的第三公钥。然而，验证设备 120 可以在使用所述第二公钥成功验证之后接受所述第三公钥。这防止了先前公钥的不正当所有者来创建似是而非的替换密钥。可选地，检验器设备 120 可以在使用所述第二公钥成功验证之后请求替换密钥。

[0042] 同样，虽然检验器设备 120 可以接收和 / 或接受所述第三公钥，而所述验证数据库可能没有指出所述第二公钥已经被替换。这是因为检验器设备 120 可以周期地或基于一定的间隔来更新所述验证数据库。结果，如果所述第二私钥变为待用并且在更新所述验证数据库之前从用户设备 110 接收了利用所述第三私钥的通信，则检验器设备 120 不能识别并且因而不能检验所述通信。因此，与主要密钥相关联的不止一组的替换密钥可以被预先创建并作为将来的替换密钥被输出。

[0043] 在图 3 中，假设利用所述第二公钥的验证是成功的。然而，由于各种原因，所述第二公钥可能导致不成功的验证。一个原因可能是不正当的所有者试图替换所述主要密钥。另一个原因可能是所述第二私钥已经被所述第三私钥所替换，在所述情况下，检验器设备 120 可能已经接收了第三公钥。因此，如果所述第二公钥导致了不成功的验证，则检验器设备 120 可以使用新的替换密钥在其可用的情况下尝试验证，该新的替换密钥即所述第三公钥。否则，所述验证失败。应当理解，如果所述第三私钥由第四私钥所替换，则检验器设备 120 可以使用第四公钥尝试验证，如果该第四私钥由第五私钥所替换，则检验器设备 120 可以使用第五公钥尝试验证，等等。在某些实施例中，基于给定的允许替换的数目和给定的时间周期，可以替换公钥的次数可能受限。

[0044] 如上所述，第三组密钥被创建并作为待用的替换密钥被输出，而第二组密钥变为现用并被用于后续的验证。也可以使用第三组密钥进行后续的验证。例如，用户设备 110 创建第三组密钥并重新创建第二私钥。所述第二私钥初始被用于通信的验证。这是由于检验器设备 120 可能还不知道第三组密钥已经被创建。可以通过签名的通信输出第三公钥。当成功地检验了所述通信时，检验器设备 120 可以更新所述验证数据库以使该第三组被用于后续的验证。

[0045] 如果周期地或基于一定间隔来更新所述验证数据库，则即使已经输出了所述第三公钥，所述第二私钥也可以暂时保持现用并被用于验证。基于检验器设备 120 的更新计划表，所述第三私钥因而可以在所选间隔后变为现用。可选地，当更新所述验证数据库时，检验器设备 120 可以发送控制信号给用户设备 110，该控制信号指出所述验证数据库已经被更新。用户设备 110 因而将使用所述第三私钥，并且检验器设备 120 将使用所述第三公钥进行验证。仍然可选地，检验器设备 120 可以在某时请求替换密钥以使所述验证数据库可以被更新来存储该替换密钥。这里，用户设备 110 将不输出所述第三公钥直到接收到来自

检验器设备 120 的请求。

[0046] 当用户设备 110 开始使用所述第三私钥进行验证时,可以丢弃所述第二私钥,以使如果用户设备 110 被丢失或偷窃则该第二私钥不能被重新创建。此外,应该指出,由于已经输出了所述第二私钥,因此用户设备 110 不输出所述第二或第三私钥。然而,可以配置用户设备 110 来允许用户设备的所有者在所述第二私钥被重新创建时再次将其输出。因而可以将所述第二私钥输出一次给使用例如共享方案的一个或多个相同或不同的实体。

[0047] 因此,所述第二私钥可以作为验证用户设备 110 的所有者的临时私钥,并允许以新的私钥替换所述第一私钥,该新的私钥即第三私钥。所述第三私钥因而被用于验证直到其变为待用,此时所述第二私钥被再次重新创建,并被用于验证用户设备 110 的所有者以允许以新的私钥替换所述第三私钥。这里,将创建第四组替换密钥以替换该第三私钥。

[0048] 在另一个实施例中,第三和第四组密钥可以被创建为第一和第二组密钥的替换密钥。一组私钥被用于后续的验证,而另一组私钥在用户设备 110 的所有者的请求下被输出一次以使其可以被重新创建。例如,所述第三私钥可以被用于后续的验证,而所述第四私钥被输出以使其可以被重新创建。这里,所述第二私钥可以仍作为验证用户设备 110 的所有者的临时私钥,并允许以新的密钥即第三私钥来替换所述第一私钥。在替换所述第一私钥之后可以丢弃所述第二私钥。所述第三私钥因而被用于验证直到其变为待用,此时所述第四私钥被重新创建,并被用于验证用户设备 110 的所有者以允许以新的替换密钥组来替换所述第三私钥。这样,第五和第六组密钥被创建为新的替换密钥组。

[0049] 如上所述可以独立产生多组密钥,其中一组作为用于验证的主要密钥,而另一组作为替换密钥由此在主要密钥变为待用时作为备份密钥。在另一个实施例中,可以从先前的密钥组中导出一组替换密钥。

[0050] 图 4 示出了用于针对公钥加密系统产生密钥的另一个方法 400。处理器 112 通过关联的系统参数来创建 (410) 私钥和相应的公钥。所述密钥和系统参数可以被初始存储在存储媒介 114 中。所述私钥被保存在用户设备 110 中,而使用发射机 116 输出 (430) 所述公钥和系统参数。

[0051] 当验证时,如果所述私钥是现用的 (440、450 和 460) 则使用该私钥。即,用户设备 110 以私钥来签名通信,并将所述通信和关联的签名发送给目标方或设备,所述目标方或设备然后通过相应的公钥来检验所述通信。如果所述私钥不是现用的,则利用系统参数和旧的或先前的私钥来创建 (470) 新的或替换的私钥。这里,由于各种原因,先前的私钥可以不是现用的。例如,由于用户设备 110 被偷窃、损坏、丢失或破坏,因此用户设备 110 的所有者可以具有待用的私钥。可选地,私钥可能在某些加密系统中过期了。如果所述新的私钥是现用的则其可被用于验证 (450 和 460)。新的私钥的使用使先前的私钥失效。

[0052] 图 5 示出了对应于方法 400 的用于验证通信的方法 500。检验器设备 120 接收 (510) 对应于来自用户设备 110 的私钥的公钥。检验器设备 120 也接收 (520) 与来自用户设备 110 的私钥和公钥相关联的系统参数。所述公钥和系统参数被存储在存储媒介 124 的验证数据库中。

[0053] 当从用户设备 110 接收签名的通信进行验证时,处理器 126 通过相应的公钥进行验证 (530 和 540)。即,所述相应的公钥从所述验证数据库被检索并被用于检验所述通信和关联的签名。如果不能使用公钥来检验所述通信,则处理器 126 使用先前的公钥和系统参

数导出 (560) 新的公钥。检验器设备 120 因而利用所述新的公钥来尝试验证 (540)。这种利用新的或替换的公钥所进行的导出和尝试可以在需要时如上所述重复地发生, 直到成功的验证发生。在某些实施例中, 基于给定的允许替换的数目或给定的时间周期, 所述密钥可以被替换的次数可能受限。

[0054] 在方法 400 和 500 中, 所述系统参数取决于所实现的加密系统。例如, 如果所述加密系统是基于 DSS 的, 则系统参数将是随机数。

[0055] 更具体地, 在创建密钥  $x$  时, 所述用户设备创建随机数  $r$  和可选的计数器值  $c$ , 所述随机数还是模  $Q$  子群 ( $\text{mod } Q$  subgroup) 的成员, 所述计数器值被关联于公钥和密钥。当所述公钥被输出并被存储在检验器设备 120 中时, 也输出  $r$  和  $c$ 。假设初始用户设备 110 具有  $c = 0$ , 用户设备 110 如下创建替换密钥  $y$  的共享:

$$[0056] \quad y = x * r \pmod{P}$$

[0057] 相应的公钥  $Y$  如下:

$$[0058] \quad Y = g^y = g^{(x * r)} = (g^x)^r = X^r \quad (\text{所有模 } P \text{ (all mod } P))$$

[0059] 可以从旧的公钥和  $r$  的信息中导出新的公钥。被提供以新的密钥  $y$  的最近创建的用户设备 110, 例如令牌, 将增加  $c$  并保持相同的  $r$ 。任何用户设备 110 所产生的签名可能包括  $c$ , 这使得检验器设备 120 容易地确定使用哪个公钥进行检验。此外, 即使自最后一次验证所有者以后发生了若干替换, 检验器设备 120 也可以接受并检验签名。如果  $c$  包含于所述签名中, 则基于  $c$  以合适的次数对旧的公钥取幂。如果  $c$  不被包含, 则所述检验器设备 120 可以简单尝试  $X$  的若干次幂。这里, 可以设置对尝试次数的限制。如果所导出的公钥之一用于检验所述签名, 则该公钥作为新的公钥被接受。

[0060] 因此, 所述用户设备的所有者可以为其将来的替换预先安排, 而不会此时泄漏所述密钥。同样, 当替换用户设备和 / 或密钥被使用时, 其将被暗中地检验。即, 可以通过所述检验器来使用利用新的用户设备和 / 或密钥的动作, 以使旧的用户设备和 / 或密钥失效。

[0061] 应当指出, 虽然在 DSS 方面描述了所述实施例, 而范围不限于 DSS。尽管通常通过现有技术中已知的不同的数学和处理, 然而所述实施例可以应用于其它公钥系统。同样, 在沙米尔秘密共享方法方面描述了某些实施例, 但是其它已知方法同样是可应用的。此外, 尽管用户设备 110 示出了一个处理器 112, 然而可以实现不止一个的处理器以产生和 / 或使用所产生的密钥进行验证, 所述处理器被配置以产生每个私钥、公钥和替换密钥并使用所产生的密钥进行验证。同样地, 尽管检验器设备 120 示出了一个处理器 124, 然而可以实现不止一个的处理器以产生和 / 或使用所产生的密钥进行验证, 所述处理器被配置以产生每个可应用的公钥并使用所产生的密钥进行验证。此外, 本技术的领域人员将理解到, 用户设备 110 的元件可以按照所期望的重新安排, 而不影响用户设备 110 的操作和功能。类似地, 检验器设备 120 的元件可以按照所期望的重新安排, 而不影响检验器设备 120 的操作和功能。

[0062] 另外, 可以通过硬件、软件、固件、中间件、微码或其任何组合来实现实施例。当在软件、固件、中间件或微码中实现实施例时, 执行必要任务的程序代码或代码段可以被存储在机器可读媒介中或未示出的分离存储媒介中, 所述机器可读媒介分别例如存储媒介 114 和 / 或存储媒介 124。处理器 112 和 / 或 126 可以执行所期望的任务。代码段可以表示过程、函数、子程序、程序、例程、子例程、模块、软件包、类, 或指令、数据结构或程序语句的任何组合。通过传递和 / 或接收信息、数据、变元、参数或存储器内容, 代码段可以被耦合到另

一个代码段或硬件电路。可以利用包括存储器共享、消息传递、令牌传递、网络传输等的任何合适的装置，来传递、转发或发送信息、变元、参数、数据等。

[0063] 因此，前述实施例仅是例子并且不作为本发明的限制。本说明书仅用于说明而不限制权利要求的范围。同样地，本说明可以容易地应用于设备的其它类型，并且许多选择、修改和变化对于本技术领域的技术人员而言将是明显的。

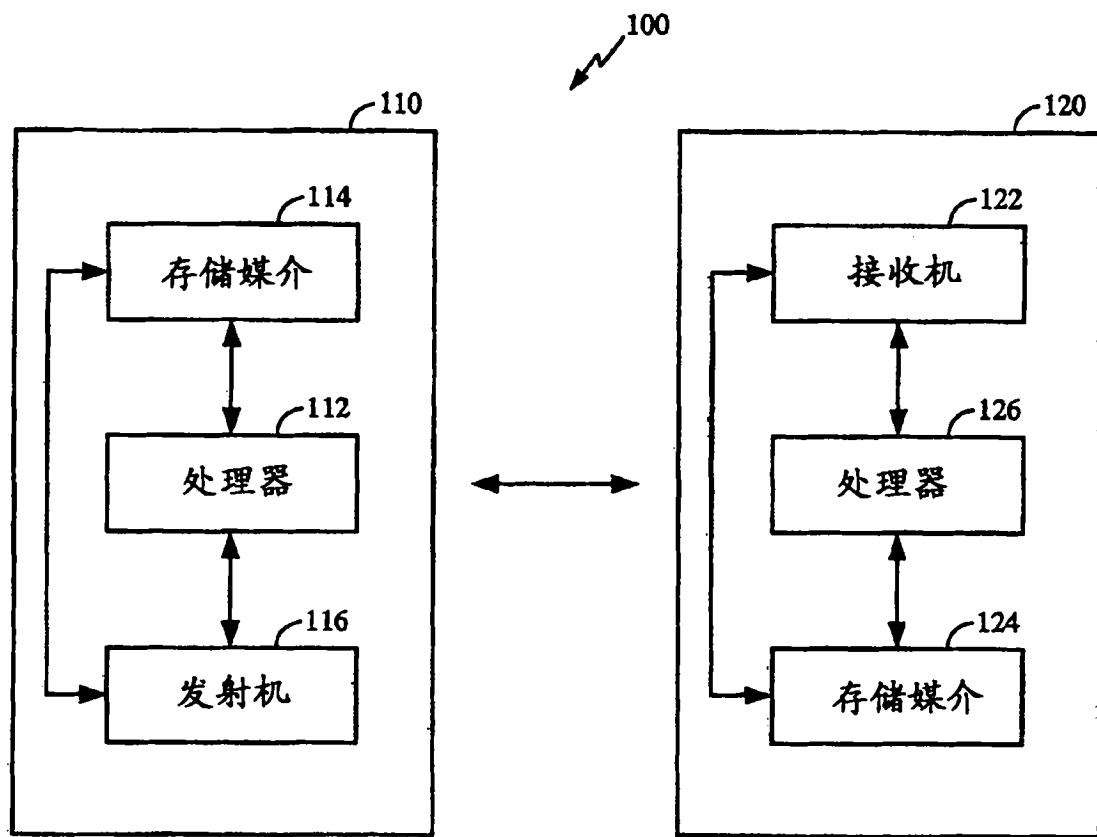


图 1

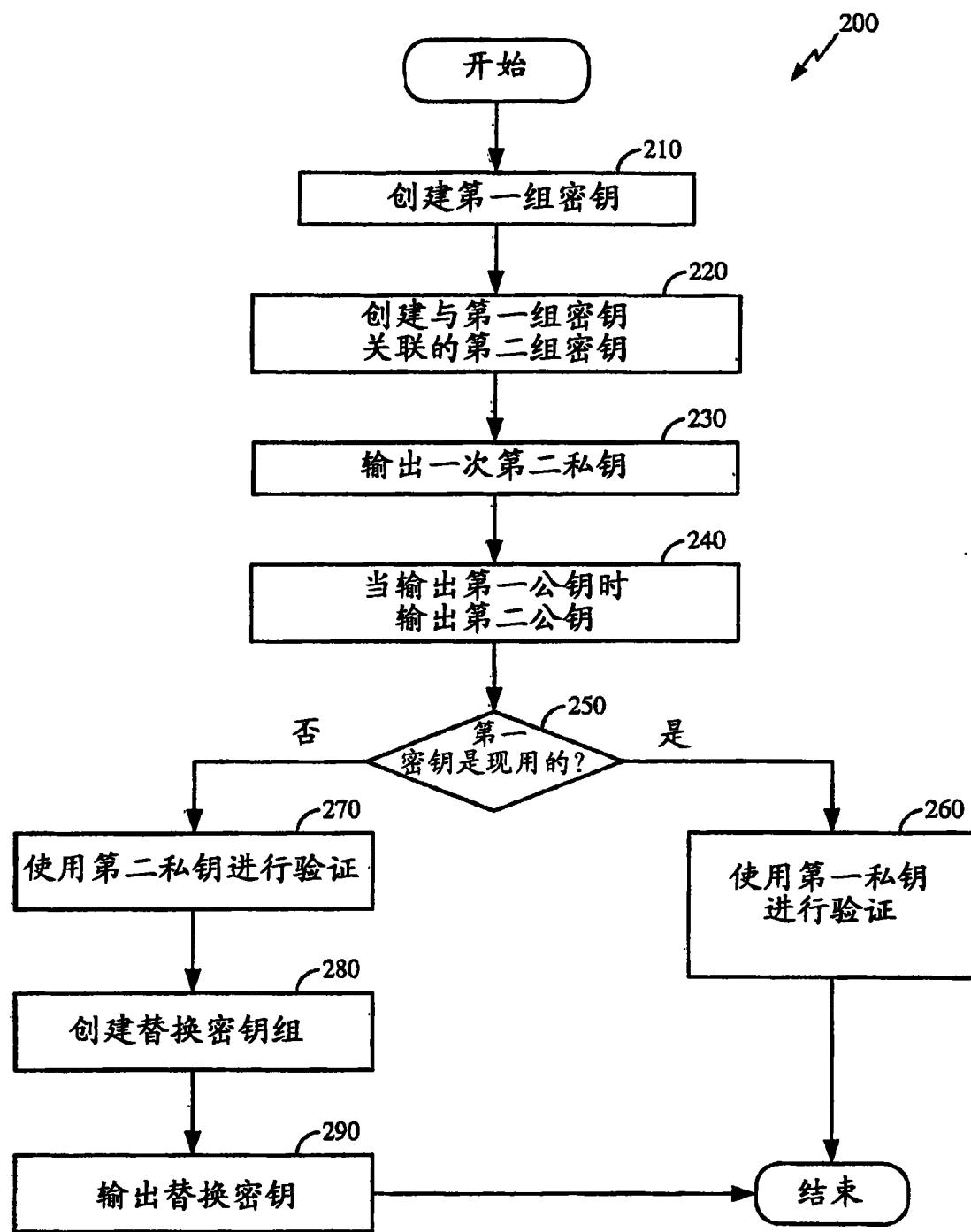


图 2

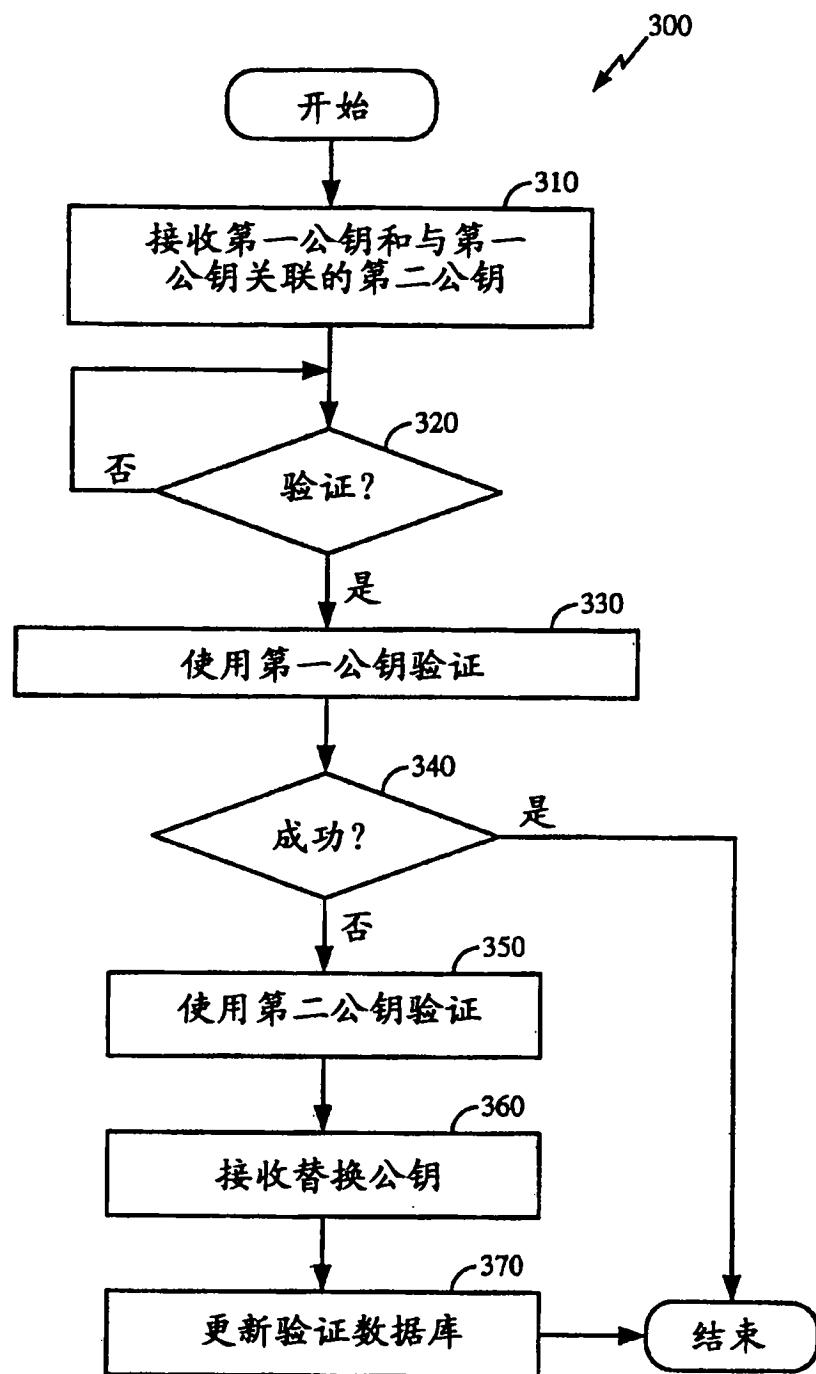


图 3

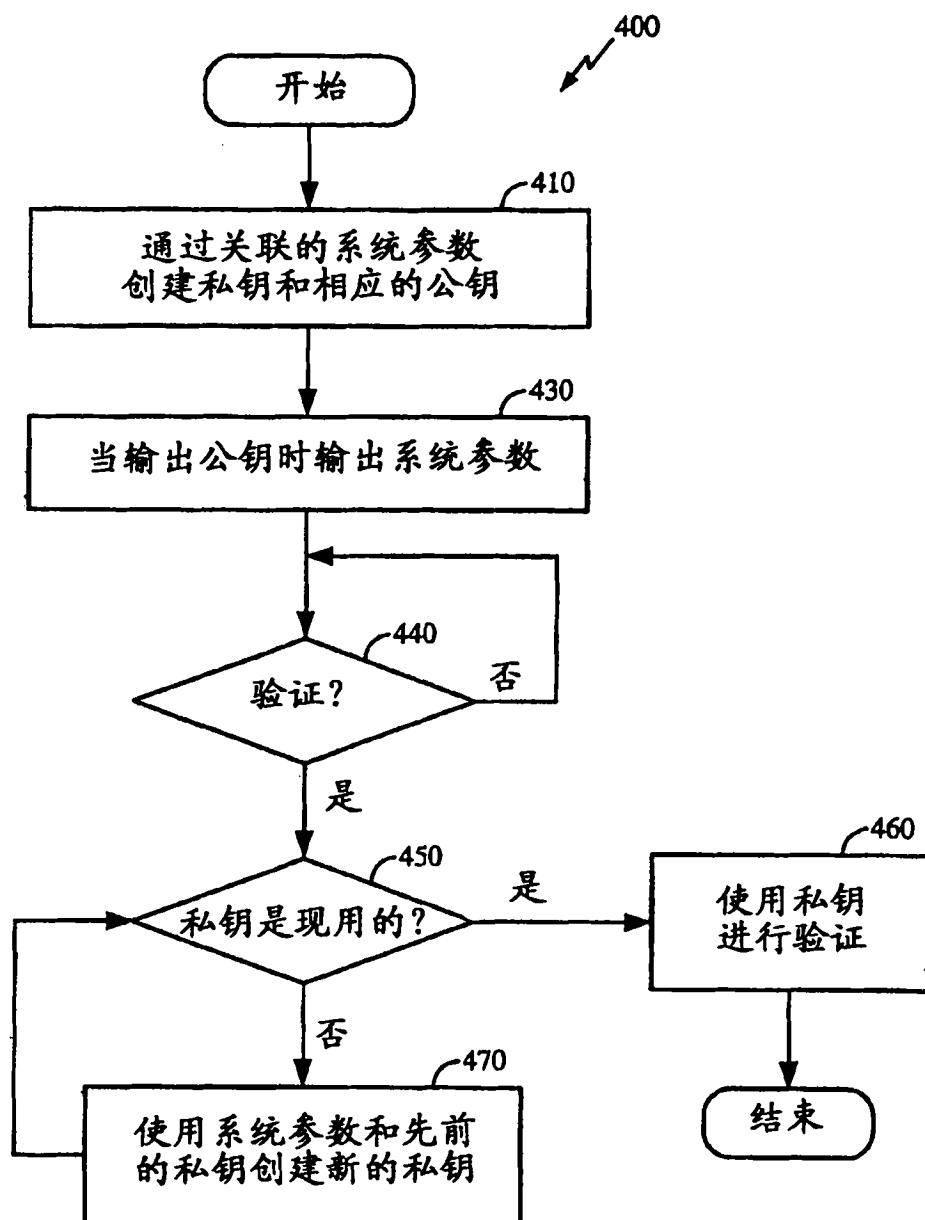


图 4

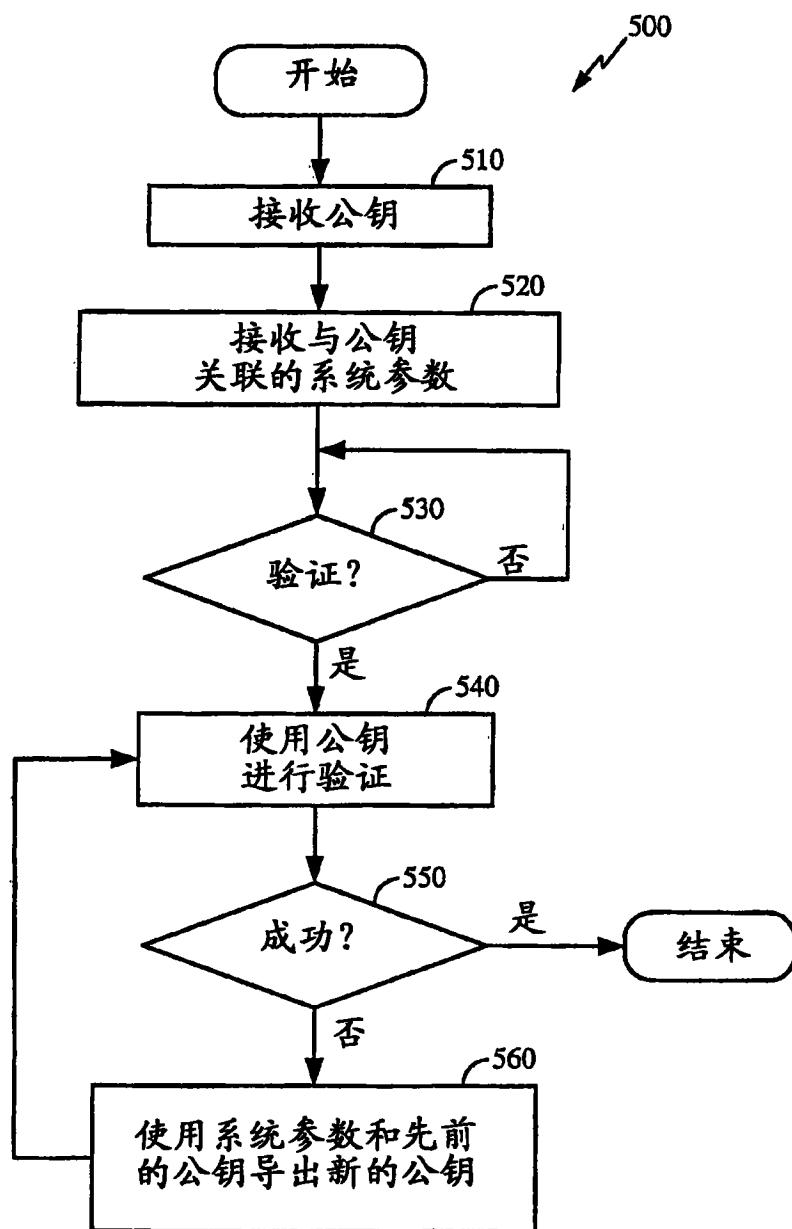


图 5