(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 104012036 A
(43)申请公布日 2014.08.27

(21)申请号 201280062244.1
(22)申请日 2012.12.17
(30)优先权数据
13/326,837 2011.12.15 US
(85)PCT国际申请进入国家阶段日
2014.06.16
(86)PCT国际申请的申请数据
PCT/US2012/070014 2012.12.17
(87)PCT国际申请的公布数据
WO2013/090881 EN 2013.06.20
(71)申请人 德克萨斯仪器股份有限公司
地址 美国德克萨斯州
(72)发明人 E·T·彼得斯
(74)专利代理机构 北京纪凯知识产权代理有限公司 11245
代理人 赵蓉民 李英
(51)Int.Cl.
H04L 9/32(2006.01)
H04L 9/20(2006.01)

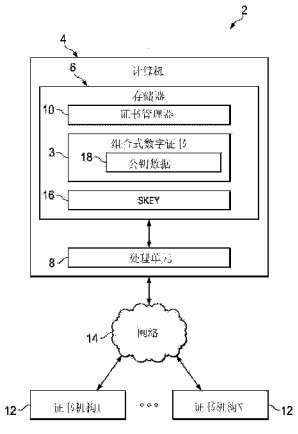
权利要求书3页 说明书8页 附图5页

(54)发明名称

组合式数字证书

(57)摘要

一种系统(2),该系统(2)可包括:存储器(6)以及处理单元(8),该存储器存储计算机可读指令;该处理单元访问该存储器(6)并且执行计算机可读指令。计算机可读指令可包括证书管理器(10),其被配置以请求产生N个随机值,其中N是大于或者等于一的整数;证书管理器(10)可还被配置以从至少两个不同证书机构(12)中的至少一个证书机构(12)请求数字证书。该请求可包括N个随机值中的给定一个。证书管理器(10)可还被配置以产生公私钥对的私钥(16),其中所述私钥(16)是基于至少两个证书机构(12)的每一个的私钥产生的。



CN 104012036 A

1. 一种产生组合式数字证书的方法，该方法包括：

在计算机产生 N 个随机值，其中 N 是大于或者等于二的整数；

从所述计算机向 N 个证书机构中的对应证书机构提供请求，该请求包括所述 N 个随机值中的给定一个；

响应于所述请求，在所述计算机从所述 N 个证书机构中的每一个接收数字证书；

在所述计算机基于从所述 N 个证书机构的每一个接收到的数据的组合产生针对所述计算机的私钥；以及

在所述计算机基于从所述 N 个证书机构的每一个接收到的每一个数字证书的组合产生组合式数字证书。

2. 根据权利要求 1 所述的方法，其中，从所述 N 个证书机构的每一个接收到的每一个数字证书是基于椭圆曲线加密法产生的。

3. 根据权利要求 2 所述的方法，其中，所述 N 个随机值的每一个表示在椭圆曲线上的点。

4. 根据权利要求 3 所述的方法，其中，来自所述 N 个证书机构的给定数字证书包括表示所述椭圆曲线上的点的数字的集合，其中在所述椭圆曲线上的所述点是基于所述 N 个随机值中所述给定一个计算的。

5. 根据权利要求 2 所述的方法，其中，针对所述计算机的所述私钥被配置使得：

$$SKey = (\sum_{i=1}^{N} s_i + r_i e_i) (\mathrm{mod}\, n) \text{ 或}$$

$$SKey = (\sum_{i=1}^{N} (s_i + r_i) \prod_{j \neq i} e_i) (\mathrm{mod}\, n)$$

其中：

SKey 表示针对所述计算机的所述私钥；

r_i 表示由所述计算机产生的所述 N 个随机值的所述给定一个；

e_i 表示在所述 N 个证书机构中的证书机构 i 执行哈希函数的结果；

si 表示由所述证书机构 i 提供的整数；以及

n 表示在所述椭圆曲线上的点的数量。

6. 根据权利要求 1 所述的方法，其中，所述 N 个随机值的所述给定一个是在所述计算机的制造时产生的，并且所述 N 个随机值的剩余部分是在所述计算机的激活之后产生的。

7. 根据权利要求 1 所述的方法，其中，从所述 N 个证书机构的每一个接收到的每一个数字证书是彼此独立地产生的。

8. 一种产生组合式数字证书的方法，该方法包括：

在计算机产生随机值；

将所述随机值提供给两个证书机构中的第一个；

在所述计算机从所述两个证书机构中的第二个接收数字证书，其中所述数字证书基于在所述第一个证书机构产生的数字证书；

在所述计算机基于来自所述两个证书机构的每一个的数字产生针对所述计算机的私钥；以及

在所述计算机基于在所述计算机接收到的所述数字证书中包括的数据产生组合式数据证书。

9. 根据权利要求 8 所述的方法，所述方法还包括：产生与针对所述计算机的所述私钥对应的针对所述计算机的公钥，其中所述公钥基于所述两个证书机构的每一个的公钥。

10. 根据权利要求 8 所述的方法，其中，从所述两个证书机构中的所述第二个接收到的所述数字证书基于椭圆曲线加密法。

11. 根据权利要求 10 所述的方法，其中针对所述计算机的所述私钥被配置使得：

$SKey = e(s_1+r)+s_2 \bmod n$；

其中：

SKey 表示针对所述计算机的所述私钥；

r 表示由所述计算机产生的所述随机值；

s1 表示从所述两个证书机构中的所述第一个证书机构提供的整数；

s2 表示从所述两个证书机构中的所述第二个证书机构提供的整数；

e 表示在所述两个证书机构中的所述第二个证书机构执行的哈希函数的结果；以及

n 表示被采用以计算 s1 和 s2 的椭圆曲线中的点的数量。

12. 根据权利要求 18 所述的方法，所述方法还包括在第三方产生对应于 SKey 的公钥。

13. 一种系统，该系统包括：

存储器，其存储计算机可读指令；以及

处理单元，其用于访问所述存储器并且执行所述计算机可读指令；

其中，所述计算机可读指令包括：

证书管理器，该证书管理器被配置以：

请求产生 N 个随机值，其中 N 是大于或者等于一的整数；

从至少两个不同证书机构中的至少一个证书机构请求数字证书，其中所述请求包括所述 N 个随机值中的给定一个；以及

产生公私钥对的私钥，其中，所述私钥是基于所述至少两个不同证书机构的每一个的私钥产生的。

14. 根据权利要求 13 所述的系统，其中，所述证书管理器采用椭圆曲线加密法来产生所述私钥。

15. 根据权利要求 13 所述的系统，其中，所述至少两个不同证书机构包括至少三个不同证书机构。

16. 根据权利要求 13 所述的系统，其中证书管理器还被配置以从所述至少两个证书机构中的另一个请求另一个数字证书，并且其中，由所述至少两个不同证书机构的每一个产生的针对所述证书管理器的所述数字证书是彼此独立地产生的。

17. 根据权利要求 13 所述的系统，其中，由所述至少两个不同证书机构中的另一个证书机构产生的数字证书是基于从所述至少两个不同证书机构的给定证书机构接收到的数据产生的。

18. 根据权利要求 13 所述的系统，其中，所述系统是加密处理器。

19. 一种非瞬时计算机可读介质，其具有用于执行方法的计算机可执行指令，该方法包括：

请求产生 N 个随机值，其中 N 是大于或者等于一的整数；

从至少两个不同证书机构中的至少一个证书机构请求数字证书，其中所述请求包括所述 N 个随机值中的给定一个；以及

请求产生公私钥对的私钥，其中，所述私钥是基于所述至少两个不同证书机构的每一个的私钥产生的。

组合式数字证书

技术领域

[0001] 本发明一般涉及数字证书，更具体地涉及用于产生组合式数字证书的设备和方法。

背景技术

[0002] 公钥加密是指要求两个不同钥匙的加密系统，一个用于锁定或者加密明码文本，另一个用于解锁或者解密密文。这些钥匙中的一个是公开或者公共的（公钥），另一个保持私有（私钥）。如果锁定 / 加密钥匙是公开的那个，则系统使得能够进行从公众到解锁钥匙的拥有者的私有通信。如果解锁 / 解密钥匙是公开的那个，则系统用作被私钥的拥有者锁定的文档的签名验证器。

[0003] 可以使用若干不同的公钥原语来提供数字签名。一些是基于离散对数问题并且称为基于离散对数的公钥加密系统。公钥加密系统可以在各种方案中用以提供保密性、完整性、认证或者认可功能。可通过诸如公钥数字证书这样的数字证书来实现认可或者认证。公钥数字证书可以包括两部分：数据和数据的签名。数据可包括公钥和受信第三方（证书机构，CA）的订户的唯一标识符。在订户的公钥上的 CA 的签名在订户的公钥和订户的身份（ID）之间传达真实绑定。

发明内容

[0004] 一个示例涉及系统，该系统可包括存储器以及处理单元，该存储器存储计算机可读指令；该处理单元访问该存储器并且执行计算机可读指令。计算机可读指令可包括证书管理器，其被配置以请求产生 N 个随机值，其中 N 是大于或者等于一的整数；证书管理器可还被配置以从至少两个证书机构中的至少一个证书机构请求数字证书。该请求可包括 N 个随机值中的给定一个。证书管理器可还被配置以产生公私钥对的私钥，其中所述私钥是基于至少两个证书机构的每一个的私钥产生的。

[0005] 另一个示例涉及用于产生组合式数字证书的方法。该方法可包括：在计算机产生 N 个值，其中 N 是大于或者等于二的整数；该方法可还包括：从所述计算机向 N 个证书机构中的对应证书机构提供包括 N 个随机值中的给定一个的请求。该方法可还包括：在所述计算机从所述 N 个证书机构中的每个接收数字证书；该方法可还包括：在所述计算机基于从所述 N 个证书机构的每一个接收到的数据的组合产生针对所述计算机的私钥；该方法可还包括：在所述计算机基于从所述 N 个证书机构的每一个接收到的每一个数字证书的组合产生组合式数字证书。

[0006] 再一个示例涉及用于产生组合式数字证书的方法。该方法可包括：在计算机产生随机值。该方法可还包括：将所述随机值从所述计算机提供到两个证书机构中的第一个；该方法可还包括：在所述计算机从所述两个证书机构中的第二个接收数字证书。该数字证书可以基于在第一个证书机构产生的数字证书。该方法可还包括：在所述计算机基于来自所述两个证书机构的每一个的数字产生针对所述计算机的私钥；该方法可还包括：在所述

计算机基于在所述计算机接收到的数字证书中包括的数据产生组合式数字证书。

附图说明

[0007] 图 1 示出用于产生组合式数字证书的系统的示例。

[0008] 图 2A 和图 2B 示出用于产生组合式证书的示例方法的流程图。

[0009] 图 3A 和图 3B 示出用于产生组合式证书的示例方法的另一个流程图。

[0010] 图 4 示出用于产生组合式数字证书的系统的另一个示例。

具体实施方式

[0011] 在一个示例中，可采用计算机，诸如加密处理器来产生并且管理组合式数字证书。组合式数字证书可包括用于产生公钥的数据，该公钥是基于从多个证书机构接收到的数据产生的。另外，计算机还可产生对应的私钥，该私钥可以与组合式数字证书分开（并且安全地）存储。私钥还可基于从多个证书机构提供的数据。这样，即使未许可的用户（例如，黑客）破坏多个证书机构中的一个，这种未许可的用户不能够确定私钥。

[0012] 图 1 示出用于产生和管理组合式数字证书 3 的系统 2 的示例。可通过采用任意离散对数公钥系统诸如，但不限于艾尔伽马而 (El-Gamal) 签名、斯诺尔 (Schnorr) 签名、数字安全算法 (DSA) 或者其变体来产生组合式数字证书 3。这些方案中的任何一个可使用椭圆曲线加密法 (ECC)，其固有地提供低存储和计算要求。系统 2 可包括例如计算机 4，其包括用于存储机器可读指令的存储器 6。计算机 4 可以被实现成例如加密处理器、专用集成电路芯片 (ASIC)、智能卡、智能电话、台式计算机、笔记本计算机等。存储器 6 可以被实现为例如非瞬时性计算机可读介质，诸如，随机存取存储器 (RAM)、闪速存储器、硬盘驱动器等。存储器 6 的一些部分在被请求时可以被外部系统访问。然而，在一些示例中，存储器 6 的一些部分可以是安全的并且仅可由计算机 4 的内部部件访问。计算机 4 可还包括用于访问存储器 6 和执行机器可读指令的处理单元 8。处理单元 8 可以例如实现为处理器核。存储器 6 可包括证书管理器 10，其可产生、修改和 / 或管理组合式数字证书 3，该组合式数字证书 3 可还存储在存储器 6 中。应理解的是在其它示例中，证书管理器 10 可以被存储在另一个系统上，诸如外部系统、服务器或者主机系统，诸如包含计算机 4 的智能电话或者其它装置。

[0013] 证书管理器 10 可响应于满足条件而启动组合式数字证书 3 的产生。例如，如果计算机 4 被实现为加密处理器，则证书管理器 10 可响应于来自另一个系统的激活请求启动数字证书的产生。在其它示例中，证书管理器 10 可以响应于用户输入来启动产生组合式数字证书 3。

[0014] 计算机 4 可通过网络 14 与 N 个证书机构 12 通信，其中 N 是大于等于二的整数。网络 14 可以被实现为例如公共网络（例如，因特网）、私有网络等。N 个证书机构 12 中的每一个证书机构 12 可被实现为发行数字证书的系统。数字证书以证书的命名主体证实对公钥的所有权。这允许其它（第三方）依靠签名或者对应于被认证的公钥的私钥进行的认定。在这种信任关系的模型中，1-N 个证书机构 12 中的每一个是被证书的主体（所有者）和依靠证书的第三方这两者信任的受信第三方。

[0015] 在一个示例中，响应于启动组合式数字证书 3 的产生，证书管理器 10 可请求由处理单元 8 产生 N 个随机数，这些随机数可被称为“r1...rN”。应注意的是在一些示例中，证

书管理器 10 在相对大时间段上可提供产生随机数的分开的请求。例如，证书处理器 10 可被配置以请求在制造时产生 r1。另外，证书管理器 10 可被配置以请求在将计算机 4 提供到客户场所之后产生 r2-rN。作为一个示例，计算机 4 可以嵌入有 r1，并且可被配置以在客户场所激活时请求产生 r2-rN。

[0016] 证书管理器 10 可发送 r1（或者其倍数）到证书机构 1。作为响应，证书机构 1 可返回数字证书 1，其可包括用于产生针对计算机 4 的公钥的数据，其中该公钥与证书机构 1 关联。证书机构 1 还可包括数据，诸如用于产生对应于与证书机构 1 关联的公钥的私钥的整数。应注意在一些示例中，数字证书 1 和用于产生私钥和与证书机构 1 关联的公钥的数据在制造计算机 4 时可被嵌入在计算机 4 中。另外，证书管理器 10 可发送 r2...rN 到 2-N 个证书机构 12 的每一个的对应证书机构 12。作为响应，2-N 个证书机构 12 的每一个可向计算机 4 提供对应的数字证书，以及用于产生公钥和针对计算机 4 的对应私钥的数据，该数据可被称为证书数据，计算机 4 与对应的 2-N 个证书机构 12 关联的。证书管理器 10 和 / 或处理单元 8 可采用由 1-N 个证书机构 12 的每一个提供的证书数据来产生针对计算机 4 的私钥，该私钥可被称为 Skey16。另外，在一些示例中，证书管理器 10 还可提供基于数字证书 1-N 的公钥数据 18 以用于产生针对计算机 4 的对应于 Skey16 的公钥，其可被称为 Pkey。在一些示例中，公钥数据 18 可被提供到第三方。在其它示例中，公钥数据 18 可由第三方通过其它方法（例如，登记服务）知道。在一些示例中，证书管理器 10 还可产生组合式证书 3，其可包括公钥数据 18。在一些示例中，组合式证书 3 还可包括用于标识 1-N 个证书机构 12 的每一个的数据。通过采用这个技术，证书管理器 10 可产生基于由 1-N 个证书机构 12 的每一个提供的数字证书的组合式数字证书 3。另外，通过采用这个技术，1-N 个证书机构 12 的每一个都不需要彼此通信。

[0017] 在另一个示例中，在启动产生数字证书时，证书管理器 10 可请求由处理单元 8 产生一个随机数，该随机数可被称为 r1。证书管理器 10 可发送 r1 到证书机构 1。作为响应，证书管理器 1 可产生数字证书 1 和用于产生针对计算机 4 的公钥和对应私钥的数据（例如，整数）。证书机构 1 可将用于产生私钥的数据转发到计算机 4 并且将数字证书 1 转发到证书机构 2，其中私钥与证书机构 1 关联。另外，证书机构 2 可认证证书机构 1 来确保数字证书 1 源于证书机构 1 而不是未授权的来源（例如，黑客）。证书机构 2 基于数字证书 1 可产生数字证书 2，并且将数字证书 2 转发到证书管理器 10，该数字证书可包括用于产生与证书机构 1 和证书机构 2 关联的 PKey 的公钥数据 18。证书机构 2 还可提供用于产生与证书机构 2 关联的私钥的数据（例如，整数）。证书管理器 10 和 / 或处理单元 8 基于从证书机构 1 和证书机构 2 提供的数据可产生 SKey16，其中 SKey16 对应于 Pkey。证书管理器 10 和 / 或处理单元 8 基于数字证书 2 还可产生组合式数字证书 3。在一些示例中，组合式证书 3 可包括公钥数据 18，其可被用以于 PKey。通过采用这个技术，组合式证书的大小可减小，其可节省存储。

[0018] 在两种技术中，组合式数字证书 3 可基于由 1-N 个证书机构 12 提供的数据。在第一个技术中，即使未授权的用户（例如，黑客）获得对 1-N 个证书机构 12 中任一个的访问权，组合式数字证书 3 也不被损坏。事实上，为了损坏组合式数字证书 3 的安全性，这种未授权的用户将需要损坏全部 1-N 个证书机构 12。在第二个技术中，由于证书机构 1 是由证书机构 2 认证的，所以由证书机构 1 提供的数据可被证书机构 2 信任。因而，组合式数字证

书 3 提供对安全破坏的明显抵抗。另外，这种安全破坏的可能性会在 1-N 个证书机构 12 的每一个上分配。

[0019] 鉴于上述结构和功能特征，参照图 2A、图 2B、图 3A 和图 3B 将更好地理解示例方法。另外，为了简单说明，图 2A、图 2B、图 3A 和图 3B 的示例方法被示出并且描述为连续执行，本示例不限于所例示的顺序，因为在其它示例中一些动作可以按照与此处示出和描述不同的顺序和 / 或并行地进行。

[0020] 图 2A 和图 2B 示出可被采用以产生诸如图 1 示出的组合式数字证书 3 的组合式数字证书的示例方法 200 的示例流程图。

[0021] 在 210，可以启动证书产生。证书启动例如可由证书管理器启动，诸如图 1 例示的证书管理器 10。在这种情形下，证书管理器可在计算机上执行，诸如加密处理器。在方法 200 中，可通过采用来自 ECC 的技术来产生组合式证书。然而，附加地或者另选地可采用其它加密技术。在 ECC 中，沿着曲线 E 的点可限定有限场。在一个示例中，算式 1 可限定用于方法 200 的有限场：

[0022] 算式 1：$y^2 = x^3+ax+b$；

[0023] 其中，

[0024] $P = \{x_P, y_P\}$；$Q = \{x_Q, y_Q\}$；并且 P 和 Q 是在曲线 E 上的点。

[0025] 另外，在 ECC 中，曲线 E 上的点的数量可表示为有限整数“n”。在这种情形下，算式 2 和 3 可表示 n、P 和 Q 之间的关系。

[0026] 算式 2：$nP = P+P+P...+P$

[0027] 算式 3：$Q = nP$

[0028] 在 220，可产生 N 个随机数，例如，由处理器单元，诸如图 1 例示的处理单元 8。N 个随机数的每一个可被计算为曲线 E 上的点。例如，在一个示例中，处理单元可产生随机数 ri，其中 i 是在 1 到 N 之间的整数。处理单元可采用椭圆曲线点乘法来计算 ri.G，其中 G 是在产生器点 G 处限定的曲线 E 上的数点，使得 ri.G 是曲线 E 上的点。在 230，证书管理器可将随机数 ri 提供到对应的证书机构 i，该证书机构 i 可以被实现为图 1 例示的 1-N 个证书机构 12 中的一个。在这种情形下，证书机构 i 可具有被标记为 c_{CAi} 的私钥和标记为 Q_{CAi} 的公钥。在这种情形下，算式 4 可描绘 c_{CAi} 和 Q_{CAi} 之间的关系。应注意的是算式 4 表示椭圆曲线乘法。

[0029] 算式 4：$Q_{CAi} = c_{CAi} \cdot G$

[0030] 在一个示例中，针对每一个订户 A，每一个证书机构 i 可指派不同的标识号码（例如，唯一 ID）。在这种情形下，每一个标识号码可被实现为由 N 个证书机构的每一个贡献的每一个标识号码的和（$ID_A = \Sigma(ID_{Ai})$）。替代地，证书机构 i 中的给定一个可具有由其它证书机构 i 共享的唯一标识号码。在 240，证书机构 i 可计算 $k_i.G$，其中 k_i 是在区间 [1,n-1] 内的随机数。在 250，证书机构 i 可采用算式 5 来计算 P_i。应注意的是算式 5 表示椭圆曲线加法。

[0031] 算式 5：$P_i = r_i \cdot G+k_i \cdot G$

[0032] 在 260，证书机构 i 可采用算式 6 来计算 e_i。

[0033] 算式 6：$e_i = H(P_i||ID)$

[0034] 其中 H 是单向哈希函数；P_i 是在算式 5 中给出的椭圆曲线加法的结果点；并且 ID

是针对计算机的唯一标识符。

[0035] 在270，证书机构 i 可采用算式 7 或者另选的算式 8 来计算 s_i。

[0036] 算式 7 ：$s_i = e_i \cdot k_i - c_{CAi} \pmod n$

[0037] 算式 8 ：$s_i = k_i - e_i \cdot c_{CAi} \pmod n$

[0038] 在280，证书机构 i 可提供数字证书 i 和其它数据到证书管理器，使得至少 Pi、si 和 ei 被提供到证书管理器。在290，可判断是否 i 小于或者等于 N。如果判断是肯定的（例如，是），则方法200可进行到300。如果判断是否定的（例如，否），则方法可进行到310（图2B）。在300，i 的值可增加 1 并且方法可返回到230。

[0039] 在图 2B 的 310，证书管理器可计算针对关联的计算机的私钥，该私钥可被标记为“SKey”。SKey 例如可被存储在计算机的安全存储器中。在采用算式 7 来计算 s_i 的示例中，证书管理器可采用算式 9 来计算 SKey。替代地，在采用算式 8 来计算 s_i 的示例中，证书管理器可采用算式 10 来计算 SKey。

[0040] 算式 9 ：$$SKey = \left(\sum_{i=1}^{N} s_i + r_i e_i \right) (\mathrm{mod}\, n)$$

[0041] 算式 10 ：$$SKey = \left(\sum_{i=1}^{N} (s_i + r_i) \prod_{j \neq i} e_j \right) (\mathrm{mod}\, n)$$

[0042] 在320，证书管理器可确定可被（例如，由第三方）采用以计算对应于针对关联的计算机的 SKey 的公钥的公钥数据，该公钥可被标记为“PKey”。在一些示例中，公钥数据可包括从每一个证书机构 i 提供的 P_i。在一些示例中，通过采用算式 11 和 12，第三方可采用公钥数据来导出 PKey。如算式 11 和 12 所示，PKey 可基于 Q_{CA}，其可被实现为从 1-N 个证书机构接收到的每一个 Q_{CAi} 之和。在其它示例中，第三方可采用算式 12 和 13 来计算 PKey。

[0043] 算式 11 ：$$PKey = \sum_{i=1}^{N} e_i P_i - Q_{CA}$$

[0044] 算式 12 ：$Q_{CA} = \sum_{i=1}^{N} Q_{CAi}$

[0045] 算式 13 ：$$PKey = \sum_{i=1}^{N} \left(P_i \prod_{j \neq i} e_j \right) - \left(\prod_{i=1}^{N} e_i \right) Q_{CA}$$

[0046] 在330，可产生组合式数字证书。组合式数字证书可标识被用以产生组合式数字证书的每一个证书机构 i。另外，在一些示例中，组合式数字证书可包括公钥数据。通过采用方法200，不需要证书机构 i 的每一个之间的交互。此外，通过采用 ECC，与其它加密方案相比，可实现存储器使用的明显减少。

[0047] 图 3A 和图 3B 例示可被采用以产生组合式数字证书，诸如图 1 例示的组合式数字证书 3 的方法 400 的另一个示例的示例流程图。

[0048] 在410，可以启动证书产生。证书启动例如可由证书管理器启动，诸如图 1 例示的证书管理器 10。在这种情形下，证书管理器可在计算机上执行，诸如加密处理器。在方法400 中，可通过采用来自 ECC 的技术来产生组合式数字证书。然而，附加地或者另选地可采用其它加密技术。在一个示例中，可采用算式 1 来限定用于方法 400 的有限场。在这种示例中，椭圆曲线 E 可具有有限数量的点“n”。另外，如算式 1 中标记，点 P 和 Q 可以是曲线 E

上的点。此外，算式 2 和 3 可限定 n、P 和 Q 之间的关系。

[0049] 在 420，可产生随机数，例如，由处理器单元，诸如图 1 例示的处理单元 8 产生。随机数可被计算成曲线 E 上的点。例如，在一个示例中，处理单元可产生随机数 r。处理单元可采用椭圆曲线点乘法来计算 r.G，其中 G 是在产生器点 G 处限定的曲线 E 上的点的数量，使得 r.G 是曲线 E 上的点。在 430，证书管理器可将随机数 r.G 提供到证书机构 1，证书机构 i 可以被实现为图 1 例示的证书机构 1。在这种情形下，证书机构 1 可具有私钥和标记为 Q_{CA1} 的公钥，该私钥可被称为 c_{CA1}。在这种情形下，算式 4 可描绘 c_{CA1} 和 Q_{CA1} 之间的关系。在 440，证书机构 1 可计算 $k_1.G$，其中 k_1 是在区间 [1,n-1] 内的随机数。在 450，证书机构 1 可采用算式 5 来计算 P_1。在 460，证书机构 1 可采用算式 14 来计算 s_1。

[0050] 算式 14 ：$s_1 = k_1 + c_{CA1} \bmod n$

[0051] 在 470，证书机构 1 可向证书管理器提供包括至少 s_1 的数据。在 475，证书机构 1 可被证书机构 2 认证。这种认证可确保从证书机构 1 提供的数据确实实际上是发源于证书机构 1 而不是来自未授权的来源（例如，黑客）。在 480，证书机构 1 可向证书机构 2 提供 P_1 和 s_1。在 490（图 3B），证书机构 2 可计算 $k_2.G$，其中 k_2 是在区间 [1,n-1] 内的随机数。在 500，证书机构 2 可采用算式 15 来计算 P。应注意的是算式 15 采用椭圆点乘法。

[0052] 算式 15 ：$P = k_2 \cdot G + P_1$

[0053] 在 510，证书机构 2 可采用算式 16 来计算 e。

[0054] 算式 16 ：$e = H(P||ID)$

[0055] 其中 H 是单向哈希函数；并且 ID 是针对计算机的唯一标识符。

[0056] 在 520，证书机构 2 可计算 s_2。在一些示例中，证书机构 2 可采用算式 17 来计算 s_2。

[0057] 算式 17 ：$s_2 = e(k_2 + c_{CA2}) \bmod n$

[0058] 在 530，证书机构可向证书管理器提供包括至少 P（算式 15）的数字证书。另外，证书机构可向证书管理器提供 s_2。在 540，处理单元可计算针对计算机的私钥，该私钥可被标记为“SKey”。在采用算式 17 来计算 s_2 的示例中，处理器单元可采用算式 18 来计算 SKey。

[0059] 算式 18 ：$SKey = e(s_1 + r) + s_2 \bmod n$

[0060] 在 550，证书管理器和 / 或处理单元可确定被用以产生针对关联的计算机的公钥的公钥数据，该公钥可被标记为“PKey”。公钥数据可包括从证书机构 2 接收的 P。这样，第三方可采用公钥数据来计算 PKey。例如，在采用算式 18 来计算 SKey 的示例中，第三方可采用算式 19 和 20 来计算 PKey。

[0061] 算式 19 ：$Q_{CA} = Q_{CA1} + Q_{CA2}$

[0062] 算式 20 ：$PKey = e(P + Q_{CA})$

[0063] 在 560，证书管理器可产生并且存储组合式数字证书。在一些示例中，组合式数字证书可包括公钥数据。通过采用方法 400，可实现存储的减少，因为仅仅一个针对 P 的值需要存储在计算机处。另外，通过采用 ECC 可实现附加的存储节省。还有，该方法允许增加安全性，因为组合式数字证书是基于两个不同证书机构的公钥 Q_{CA1} 和 Q_{CA1}。

[0064] 图 4 例示用于产生和管理组合式数字证书 602 的系统 600 的另一个示例。系统 600 可包括主机计算机 604，其中存储了加密处理器 606。加密处理器 606 以类似于图 1 例示的计算机 4 的方式来实现。例如，加密处理器 606 可被实现为用于进行加密操作的芯片

或者微处理器上的专用计算机，嵌入在具有多个物理安全措施的封装体中，因而向加密处理器 606 提供一定的程度的防窜改能力。在一个示例中，加密处理器 606 可被实现为受信平台模块 (TPM)。主机计算机 604 可包括用于存储机器可读指令的存储器 607（例如，非瞬时计算机可读介质，诸如 RAM、闪速存储器、硬盘驱动器等）。主机计算机 604 可还包括用于访问存储器 607 和执行机器可读指令的处理单元 608。处理单元 608 可包括处理器核。在一些示例中，主机计算机 604 可被实现为智能电话、台式计算机、笔记本计算机、服务器等。

[0065] 主机计算机 604 通过网络 612 可与 N 个证书机构 610 通信。网络 612 可以被实现为例如因特网、私有网络或者其组合。在图 4 中，详细示出证书机构 1 的部件。应理解的是 2-N 个证书机构 610 以类似方式实现。证书机构 1 可被实现为计算机，诸如数字证书的受信发行方。

[0066] 证书机构 1 可包括用于存储机器可读指令的存储器 614。存储器 614 可被实现为例如 RAM、闪速存储器、硬盘驱动器等。认证机构 1 可还包括用于访问存储器 614 和执行机器可读指令的处理单元 618。存储器 614 可包括针对认证机构 1 的私钥、c_{CA1}620。证书机构 1 还可包括针对认证机构 1 的公钥、Q_{CA1}622。

[0067] 主机计算机 604 的存储器 607 可包括证书管理器 616，其可启动产生组合式数字证书 602。产生组合式数字证书 602 的启动可以响应于用户输入。响应于启动产生组合式数字证书 602，证书管理器 616 可请求加密处理器 606 产生一个或者更多个随机数，诸如相对于图 2A、图 2B、图 3A 和图 3B 描述的随机数。

[0068] 如关于图 2A、图 2B、图 3A 和图 3B 中例示的方法 200 或者 400 描述的，响应于启动产生组合式数字证书 602，证书管理器 616 可从 1-N 个证书机构 610 接收至少 K 个数字证书 624，其中 K 是大于或者等于 1 的整数，以及来自 1-N 个证书机构 610 中的每一个的数据（例如，$s_1 \ldots s_n$）。证书管理器 616 可向加密处理器 606 提供用于产生私钥 (SKey)626 的数据（例如，证书数据）和用于加密处理器 606 基于从 1-N 个证书机构 610 提供的数据（例如，$s_1 \ldots s_n$ 和 $P_1 \ldots P_n$）产生对应的公钥 (PKey)629 的公钥数据 628。另外，加密处理器 606 可采用由证书管理器 616 提供的数据以产生组合式证书 602。在一些示例中，组合式证书 602 可包括公钥数据 628。组合式证书 602 可包括例如组合式数字证书 602 所基于的 N 个证书机构 610 的每一个的标识。

[0069] 在一些时间点，主机计算机 604 可采用组合式证书来数字地签署文档 630。在这种情形下，证书管理器 616 可将文档 630 连同针对数字签名 632 的请求提供到加密处理器 606。在一个示例中，加密处理器 606 可采用摘要算法来创建摘要，摘要由文档 630 的一部分组成。加密处理器 606 可采用 SKey626 来签署文档 630 的摘要，经签署的摘要可以是数字签名 632。

[0070] 第三方 634（例如，计算机系统）可请求文档 630。文档 630、组合式证书 602 连同数字签名 632 和 N 个证书机构 610 的给定证书机构 610 的公钥 (Q_{CAi}) 一起可被提供到第三方 634。组合式证书还可包括用于计算文档 630 的摘要的摘要算法。另外，第三方 634 可基于公钥数据 628 产生 PKey629。

[0071] 第三方 634 可与给定证书机构 610 通信以验证给定证书机构 610 的公钥 (Q_{CAi})。这样，第三方 634 可信任 PKey629 是基于给定证书机构 610 的私钥 (c_{CAi}) 产生的。另外，第三方 634 可采用摘要算法来重产生文档 630 的摘要。第三方 634 可以用组合式数字证书 602

中包括的PKey629验证数字签名632，其可得到经验证的摘要。第三方634可将重产生的数字摘要与经验证的摘要比较以确定文档630是由加密处理器606签署的并且自从产生针对文档630的数字签名632以来文档630没有改变。

[0072] 本发明所属领域的技术人员将认识到在要求保护的本发明的范围内，可以对所描述的示例进行修改，并且可能有很多其它实施例。

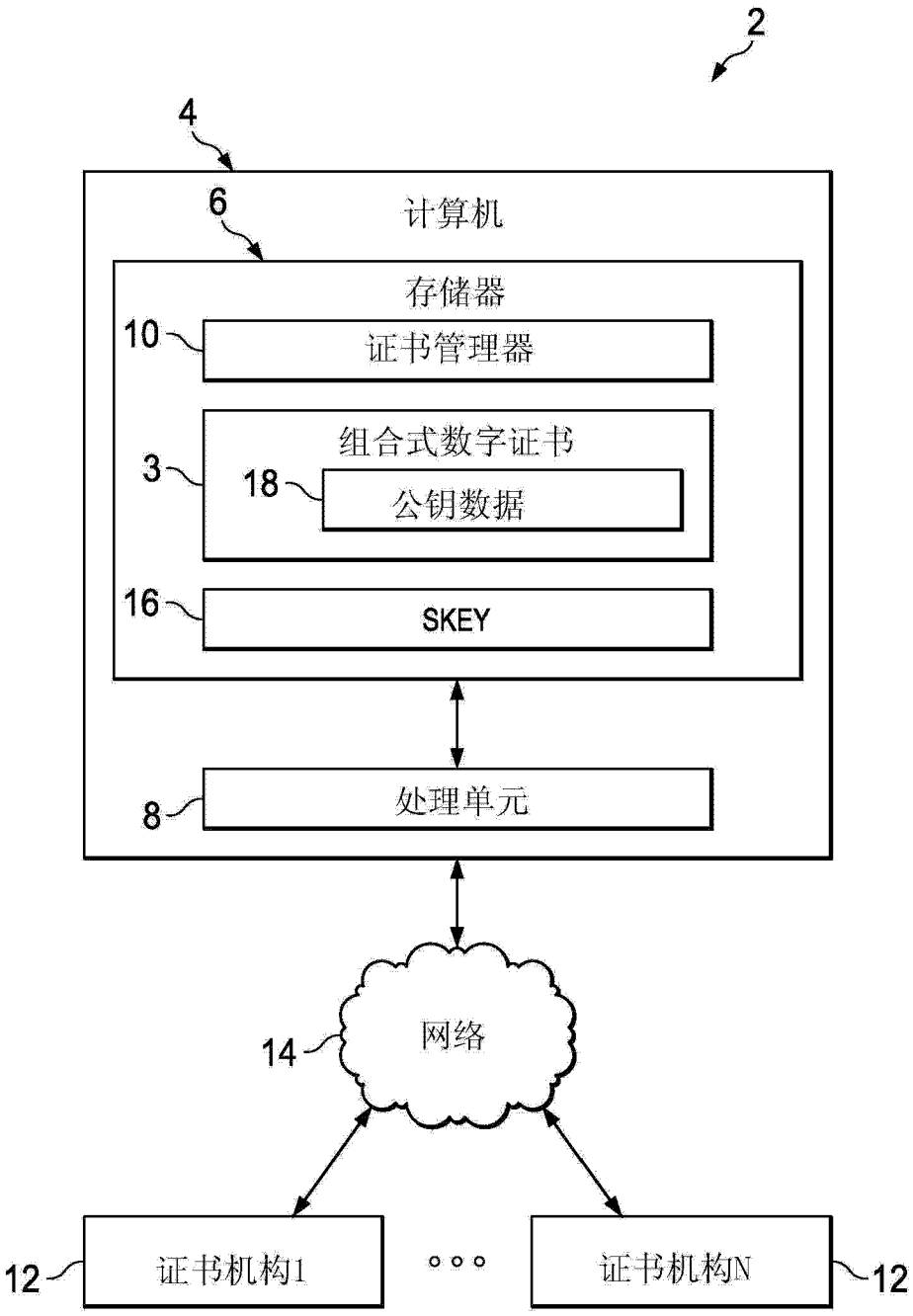

2
4
6
计算机
存储器
10
证书管理器
3
18
组合式数字证书
公钥数据
16
SKEY
8
处理单元
14
网络
12
证书机构1
证书机构N
12

图 1

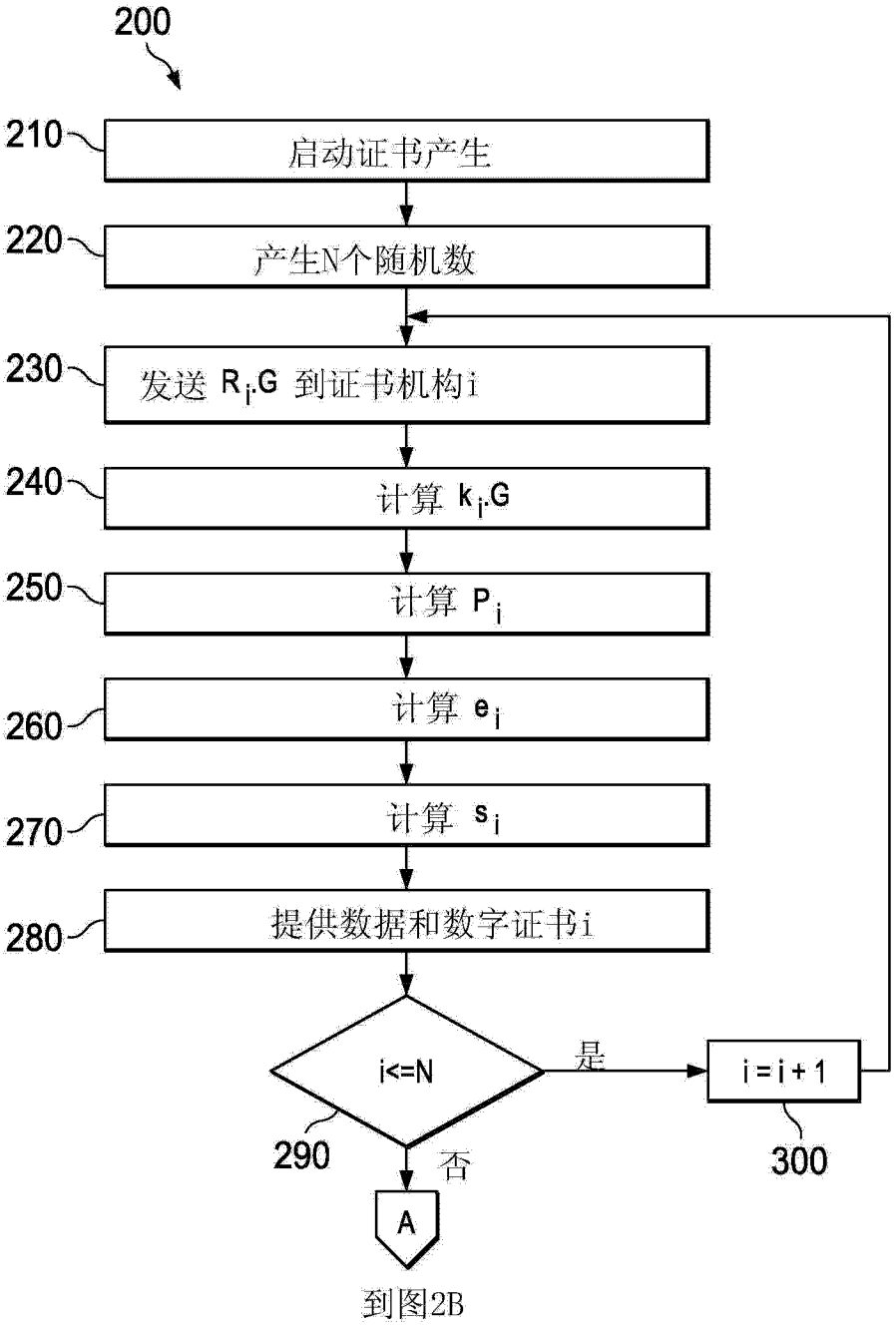

200
210
启动证书产生
220
产生N个随机数
230
发送 $R_i.G$ 到证书机构i
240
计算 $k_i.G$
250
计算 P_i
260
计算 e_i
270
计算 s_i
280
提供数据和数字证书i
i<=N
是
i = i + 1
290
300
否
A
到图2B

图 2A

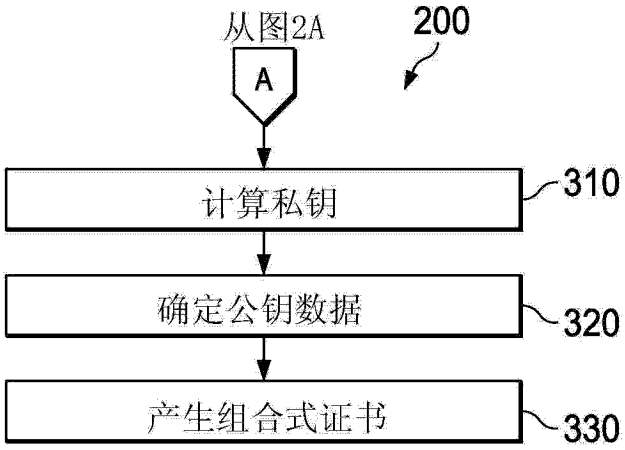


图 2B

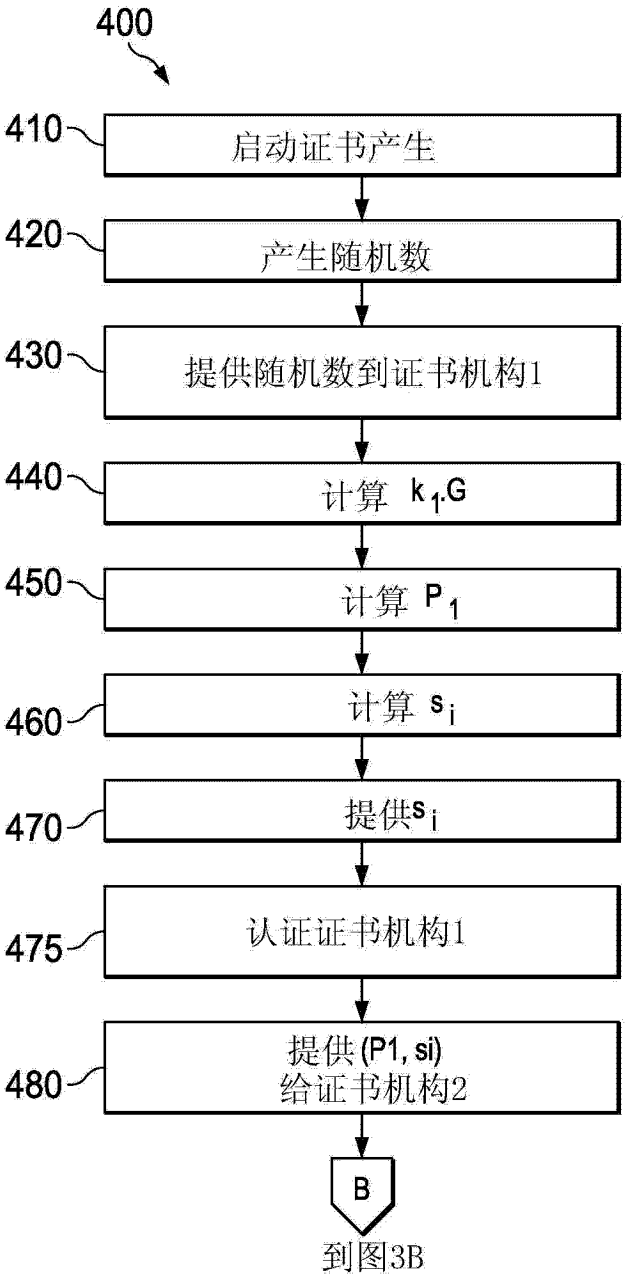

400
410
启动证书产生
420
产生随机数
430
提供随机数到证书机构1
440
计算 $k_1.G$
450
计算 P_1
460
计算 s_i
470
提供s_i
475
认证证书机构1
480
提供(P1, si)
给证书机构2
B
到图3B

图 3A

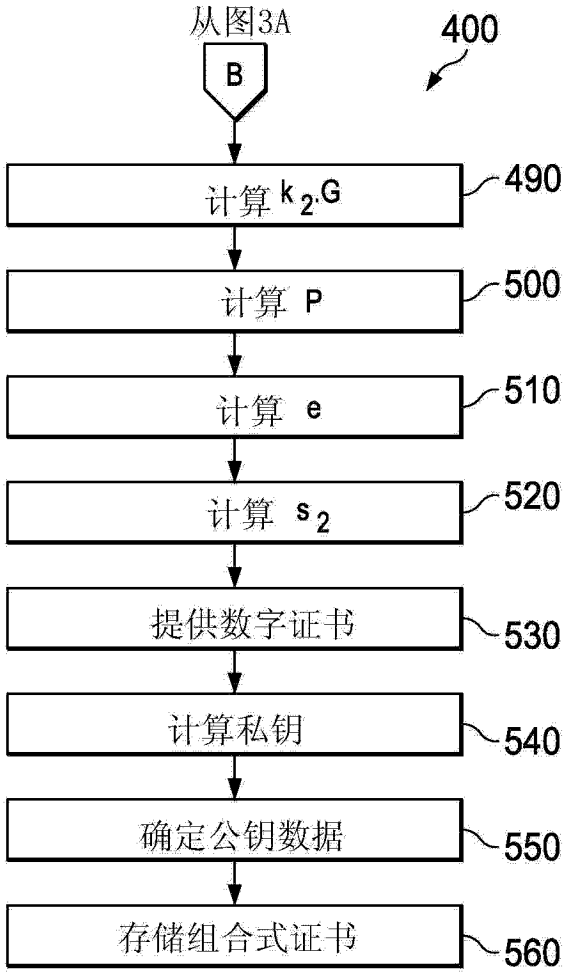

从图3A
B
400
计算 $k_2.G$
490
计算 P
500
计算 e
510
计算 s_2
520
提供数字证书
530
计算私钥
540
确定公钥数据
550
存储组合式证书
560

图 3B

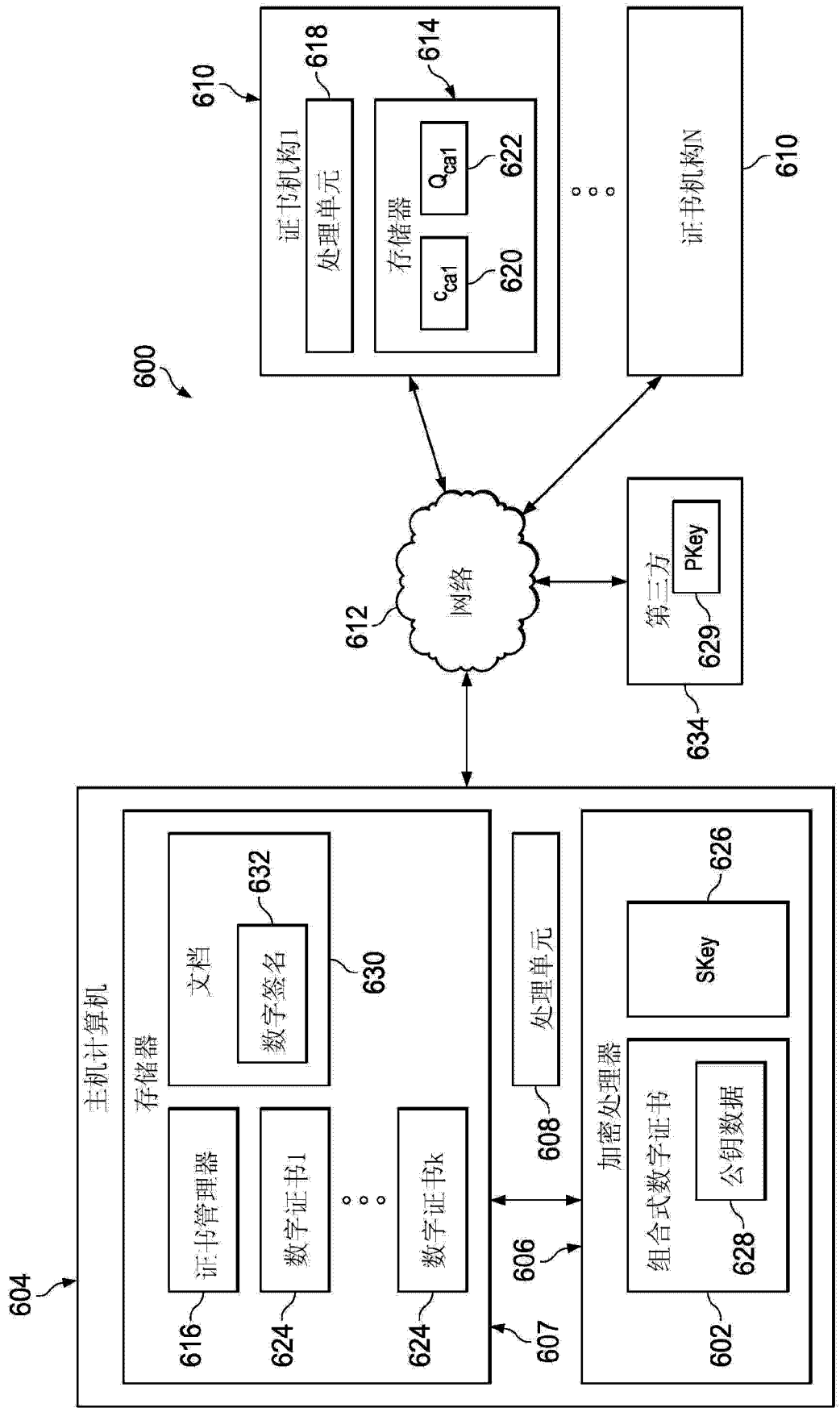

600
610
证书机构1
处理单元
618
存储器
614
Q_{ca1}
622
c_{ca1}
620
证书机构N
610
612
网络
第三方
PKey
629
634
604
主机计算机
存储器
文档
632
数字签名
630
证书管理器
616
数字证书1
624
数字证书k
624
处理单元
608
606
607
加密处理器
SKey
626
组合式数字证书
公钥数据
628
602

图 4