



[12] 发明专利申请公开说明书

[21] 申请号 01811981.6

[43] 公开日 2003 年 8 月 27 日

[11] 公开号 CN 1439207A

[22] 申请日 2001.6.14 [21] 申请号 01811981.6

[30] 优先权

[32] 2000. 6. 28 [33] US [31] 09/605,605

[86] 国际申请 PCT/US01/19223 2001. 6. 14

[87] 国际公布 WO02/01794 英 2002. 1. 3

[85] 进入国家阶段日期 2002. 12. 27

[71] 申请人 英特尔公司

地址 美国加利福尼亚州

[72] 发明人 C·埃利森 J·苏顿二世

[74] 专利代理机构 中国专利代理(香港)有限公司

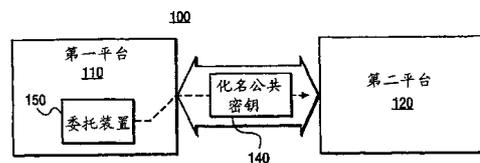
代理人 吴立明 罗 朋

权利要求书 2 页 说明书 6 页 附图 4 页

[54] 发明名称 用于建立可核查身份而又保密的平台和方法

[57] 摘要

在一个实施方案中,描述了一种利用一个化名来保护平台和用户身份的方法。该方法包括产生一个包括一个公共化名密钥的化名。该公共化名密钥被放置到一个证明模板中。对证明模板进行一个散列运算,产生一个证明散列值,从平台上对其进行变换。随后,向该平台返回一个签署结果。该签署结果是该变换的证明散列值的一个数字签名。对该签署结果进行一个逆变换后,就恢复了该证明散列值的一个数字签名。该数字签名可以用于此后利用该化名进行的通讯中的数据完整性检查。



10. 依照权利要求 9 的方法，其中在接收数字签名之前，该方法进一步包括：
将签署的证明请求和装置证明传送到一个第二平台
11. 依照权利要求 1 的方法，进一步包括：
5 存储该证明散列值得数字签名，用于此后与一个远处的平台进行通讯。
12. 一种装置，包括
一个处理单元；和
一个永久存储器，包括一个第一密钥对和至少一个化名，用来与
10 一个远方装置通讯和确定一个包含该装置的平台是安全的。
13. 依照权利要求 12 的装置，其中该至少一个化名包括一个第二密钥对。
14. 依照权利要求 13 的装置，其中在一次与远方装置的通讯对话结束后删除该第二密钥对。
15. 依照权利要求 12 的装置，进一步包括：
一个数字发生器，辅助产生该至少一个化名。
16. 一种平台，包括：
一个收发器；和
一个与该收发器通讯的装置，该装置包括一个永久存储器，来存
20 储一个永久密钥对、至少一个在装置内部产生的化名、和一个数字证明链的散列值的数字签名，该数字证明链包含化名的一个公共化名密钥。
17. 依照权利要求 16 的平台，其中装置进一步包括：
一个处理单元，（i）将公共化名写入到一个证明模板中，（ii）
25 对该证明模板进行一个散列运算，产生一个证明散列值；（iii）对该证明散列值进行一个变换。
18. 依照权利要求 17 的平台，其中装置的处理单元利用一个永久密钥对，进一步至少产生变换的证明散列值的一个数字签名
19. 依照权利要求 16 的平台，其中装置的处理单元进一步利用该
30 变换的证明散列值的数字签名附加一个装置证明。
20. 依照权利要求 19 的平台，其中该装置证明是一个数字证明链。

1. 一种方法，包括：
在一个平台中产生一个包含一个公共化名密钥的化名；
5 将该公共化名密钥放入一个证明模板中；
对该证明模板进行一个散列运算，产生一个证明散列值；
对该证明散列值进行一个变换，用于从平台向外的传送；
接收一个签署结果，该结果是用于变换的证明散列值的数字签名；和
10 对该签署结果进行一个反变换，恢复该证明散列值的一个数字签名。
2. 依照权利要求 1 的方法，其中产生化名的步骤包括产生公共化名密钥和一个对应于该公共化名密钥的私用化名密钥。
3. 依照权利要求 1 的方法，其中将该公共化名密钥放入一个证明
15 模板中的步骤包括将该公共化名密钥写入到证明模板的一个字段中。
4. 依照权利要求 1 的方法，其中进行变换的步骤包括：
利用一个伪随机数对证明散列值进行一个逻辑运算，产生一个不同于证明散列值的值。
5. 依照权利要求 4 的方法，其中该伪随机数是升高到由一个伪随
20 机值指定的相反幂次的预定数值。
6. 依照权利要求 5 的方法，其中该伪随机值被存储在安全存储器中。
7. 依照权利要求 4 的方法，其中进行反变换的步骤包括利用伪随机数的倒数对签署结果进行一个逻辑运算。
- 25 8. 依照权利要求 1 的方法，其中在接收数字签名之前，该方法包括：
利用第一平台的一个私用密钥，数字签署一个包括变换的散列值证明请求，来产生一个签署的证明请求。
9. 依照权利要求 8 的方法，其中在接收数字签名之前，该方法进
30 一步包括：
与该签署的证明一起，获得一个装置证明，即一个包括一个第一平台的一个公共密钥的数字证明链。

用于建立可核查身份而又保密的平台和方法

5 发明领域

本发明涉及的是数据安全领域。特别是，本发明涉及一种平台和方法，通过建立和使用化名来保护该平台的身份。

发明背景

技术的发展，为许多不同于传统贸易方式的应用提供了许多机会。
10 电子商务（e-commerce）和企业对企业（B2B）的交易越来越普及，以很快的速度达成全球市场。不幸的是，在诸如计算机的电子平台为用户提供方便有效的贸易、通讯和交易的同时，也容易受到肆无忌惮的攻击。这一弱点在很大程度上使内容提供者不愿意以一种下载的数字形式来提供其内容。

15 当前，已经提出了多种验证一个平台身份的机制。这对于确定平台是否是一个“委托”装置，即该平台是否配置为防止在未授权的情况下以一种非加密的格式来拷贝数字内容，是特别有用的。一种验证方法包括使用一个分配给一个平台的唯一的序列号来识别该平台。另一完全不同于上述方法或与上述方法协同操作的验证方法包括采用一个永久密钥对。该密钥对包括（i）一个识别该平台的唯一公共密钥，
20 和（ii）一个私用密钥，永久存储在该委托装置的存储器中。该私用密钥是秘密的，不向委托装置的外部提供。但是，这些验证方法都有一些缺陷。

例如，这些验证方法仍会受到数据收集攻击。“数据收集”涉及
25 对一段时间内从一个平台发送的数据的采集和分析。这样，采用平台序列号和永久密钥来进行识别，近来已经产生对用户秘密的担忧。而且，对于上述两种机制，一个用户不能方便和可靠地以一种通用形式访问和使用平台身份。

附图简述

30 根据下面对本发明的详细描述，可以清楚地了解本发明的特征和优势，其中：

图 1 是利用本发明的一个系统的说明性实施方案的模块图。

图 2 是图 1 中的第一个平台所采用的委托逻辑的说明性实施方案的模块图。

图 3 是描述图 1 中的第一个平台中产生的化名的分配和使用的说明性实施方案的流程图。

5 图 4 和 5 是产生和验证化名的说明性实施方案的流程图。

详细说明

本发明涉及一种平台和方法，通过产生和使用化名来保护平台的身份。此处，阐明了某些细节，以便对本发明的有一个透彻的理解。但是，显然，对于本领域的技术人员来讲，可以通过许多不同于所描述的实施
10 方案的实施方案来实施本发明。为了避免对本发明造成不必要的混淆，对于众所周知的电路和加密技术不做详述。

在下面的描述中，利用一些术语来讨论本发明的某些特征。例如，一个“平台”包括处理信息的硬件和/或软件。平台的例子包括，但不局限于或限制于下列任何情况：一台计算机（如台式机、膝上型电脑、
15 手提式电脑、服务器、工作站等）；数据传输设备（如路由器、转换器、传真机等），无线设备（如移动电话基站、电话送受话器等等）；或者电视机顶盒。“软件”包括代码，当被执行时，实施某一功能。“信息”定义为一个或多个数据、地址和/或控制的位。

关于加密功能，一种“加密运算”是用于在信息上附加安全性的运算。这些运算可能包括加密、解密、散列计算等等。在某些情况下，
20 加密运算需要使用一个密钥，即一个位序列。对于不对称密钥加密术，将一个装置与包含一个公共密钥和一个私用密钥的唯一永久密钥对相关。

此外，不对称密钥加密术通常利用一个根证明。一个“根证明”是最初产生一个数字证明链时的一个公共密钥，并为随后所有的数字证明提供一个起始点。通常，一个“数字证明”包括用来验证一个信息发送者的信息。例如，根据 CCITT Recommendation X.509: The Directory-Authentication Framework (1988)，一个数字证明可以包括关于一个被验证的，即利用一个认证授权的私用密钥进行加密的
30 个人或团体的信息（如一个密钥）。一个“认证机关”的例子包括一个原始设备制造商（OEM）、一个软件销售者、一个商贸协会、一个政府机构、一个银行或其它委托公司或个人。一个“数字证明链”包括

一个如下所述的为认证而安排的两个或多个数字证明的规则序列，其中每个连续的证明代表先前证明的发出者。

5 一个“数字签名”包括利用其签署人的一个私用密钥签署的数字信息，来保证该数字信息在数字签名后没有被非法修改过。可以以其完整形式，或者以一个由单向散列运算产生的一个散列形式来提供该数字信息。

10 一个“散列运算”是将信息单向变换为一个被称为一个“散列值”的固定长度的表示。通常，该散列值在尺寸上充分小于原始信息。在有些情况下，可以进行一个 1:1 的原始信息变换。术语“单向”是指没有反函数来恢复该固定长度的散列值的原始信息中任何可辨别的部分。一个散列函数的例子包括 California Redwood City 的 RSA Data Security 提供的 MD5，或 Secure Hash Algorithm (SHA-1)，被指定为 1995 年出版的标题为“Federal Information Processing Standards Publication”的 Secure Hash Standard FIPS 180-1 (1995
15 年 4 月 17 日)。

20 参考图 1, 图中显示了一个利用本发明的系统 100 的说明性实施方案模块图。系统 100 包括一个第一平台 110 和一个第二平台 120。第一平台 110 是通过一个连接 130 与第二平台 120 进行通讯。一个“连接”被概括定义为一个或多个信息传送媒体(如电线、光纤、电缆、总线或无线信号技术)。当用户需要时，第一平台 110 产生并向第二平台 120 发送一个化名公共密钥 140(下面描述)。在响应中，当可利用时，第二平台负责确认该化名公共密钥 140 是在第一平台 110 中由一个委托装置 150 来产生的。

25 现在参考图 2, 在一个实施方案中，委托装置 150 包括硬件和/或保护的软件。当采用访问控制策略来防止未授权的软件的任何程序和子程序进行访问时，确信软件是“受保护的”。更确切地讲，装置 150 是一个或多个防止其它逻辑的窜改和窃取的集成电路。可以将该集成电路放置在一个单一集成电路(IC)插件或多 IC 插件中。一个插件提供附加的窜改保护。当然，如果不需附加的保护，可以采用没有
30 IC 插件的装置 150。

这里，装置 150 包括一个处理单元 200 和一个永久存储器 210 (如非易失存储器、电池支持的随机访问存储器“RAM”等等)。处理单元

200 是由内部处理信息的软件来控制的硬件。例如，处理单元 200 可以进行散列运算、进行逻辑运算（如乘法、除法等等）、和/或通过使用数字签名算法进行数字签署信息来产生一个数字签名。永久存储器 210 包含一个在制造过程中编程的唯一的不对称密钥对 220。用于核实化名，不对称密钥对 220 包括一个公共密钥（PUKPI）230 和一个私用密钥（PRKPI）240。永久存储器 210 可以进一步包括第二平台 120 的一个公共密钥 250 (PUKP2)，尽管如果可适用的话，它可以被放置在装置 150 中的易失存储器（如 RAM、寄存器组等等）中。

在该实施方案中，装置 150 进一步包括多个发生器 260，如一个随机数发生器，或一个伪随机数发生器。数据发生器 260 负责产生一个比特流，至少部分地用于产生一个或多个化名。一个“化名”是一个另外的密钥对形式的别名身份，该密钥对用来建立与另一个平台之间的受保护的通讯，并确认其平台包括了委托装置 150。化名还支持一个询问/响应协议和一个许可绑定、保密和其它对特定平台的访问控制信息。但是，数据发生器 260 也可从装置 150 的外部使用。在这种情况下，如果数据发生器 260 和装置 150 之间的通讯是受到保护的，则通过平台 110 可以实现更大的安全性。

参考图 3，图中显示了说明一个化名的分配使用的说明性实施方案。为了全面保护用户的机密，用户应当能够切实地控制化名的产生、分配和删除。这样，在用户明确应允后，产生一个新的化名（模块 300 和 310）。而且，为了访问用来核实一个现有化名的信息（如标记、公共密钥等），需要用户明确的应允（模块 320 和 330）。可以通过向委托装置提供一个许可短语（如包含文字和数字的字符串）、一个符号和/或一个生物统计特征，来给出明确的用户应允。例如，在一个实施方案中，可以通过一个用户输入装置（如键盘、鼠标、袖珍键盘、操纵杆、触摸垫、跟踪球等等）来输入一个用户许可短语，并将其传送到委托装置。在另一个实施方案中，逻辑电路外部的存储器可以包含具有用户的许可短语的一个散列值加密的化名。这些化名都可以通过再次提供用户的许可短语来解密。

一旦产生了化名并配置为用来与一个远方平台进行通讯，对于平台/平台的通讯，只要用户选择保持该化名，那么该化名就代表该平台的身份（模块 340, 350 和 360）。

参考图 4 和 5, 图中显示了产生和验证化名的说明性实施方案的流程图。开始时, 接收到一个用户的请求后, 立即由装置结合一个数字产生化名 (模块 400)。一个化名公共密钥 (PPUKP1) 被放置到一个数字证明模板中 (模块 405)。该数字证明模板可以存储在第一平台内部, 或由第二平台根据第一平台的验证请求来提供。因此, 该数字证明模板经过一个散列运算, 产生一个证明散列值 (模块 410)。

随后, 该验证散列值经过一个类似于美国专利 No. 4, 759, 063 和 4, 759, 064 中所描述的变换, 来创建一个“不可见的”证明散列值 (模块 415)。特别是, 将该证明散列值乘以一个伪随机数 (例如, 将一个预定数据提升到一个伪随机选择的幂次)。该伪随机幂在第一平台中是保密的 (如放置在图 2 中的永久存储器 210 中)。

产生一个至少包括该变换的 (或不可见的) 证明散列值的验证请求 (模块 420)。该验证请求是利用第一平台的私用密钥 (PRKP1) 来数字签署的 (模块 425)。取回或产生一个装置证明, 即第一实施方案中的包含公共密钥 (PUKP1) 的一个数字证明链, 与签署的验证请求放在一起 (模块 430)。在该实施方案中, 装置证明的特征是拥有一个包含 PUKP1 的高层证明和包括根证明的最低层证明。当然, 该装置证明可以是一个包含 PUKP1 的单一数字证明。签署的验证请求和装置证明都利用第二平台的公共密钥 (PUKP2) 来加密, 然后传送到第二平台 (模块 435 和 440)。

在第二平台中, 利用第二平台的私用密钥 (PRKP2) 解密后恢复签署的验证请求和装置证明 (模块 445)。可以利用负责签署装置证明的证明管理部门的一个公共密钥来获得第一平台的公共密钥 (PUKP1) (模块 445)。如果第二平台可以恢复证明请求, 则第二平台对装置证明一直向回验证到根证明 (模块 455 和 460)。如果恢复了证明请求并验证了装置证明, 则数字签署变换的 (或不可见的) 证明散列值, 以产生一个“签署结果” (模块 465)。否则, 如果不能确定变换的 (或不可见的) 证明散列值, 或不能验证装置证明, 则向第一平台返回一个出错信息 (模块 470)。

从第二平台接收到签字的结果之后, 第一平台对该信号结果进行一个反变换。例如, 在该说明性实施方案中, 第一平台将签署的信号除以一个伪随机数的倒数 (例如预定的数据的伪随机数的相反幂次),

来恢复一个证明散列值的数字签名（模块 475 和 480）。该数字签名与一个或多个化名一同存储，用于以后与其它平台的通讯，来确定第一平台包括一个委托装置。

5 至此，参照说明性的实施方案对本发明进行了描述，但该说明并不是一个限制。显然对于本领域的熟练人员而言，只要不超出本发明的宗旨和范围，可以对该说明性实施方案进行多种修正，以及采用其它的实施方案。

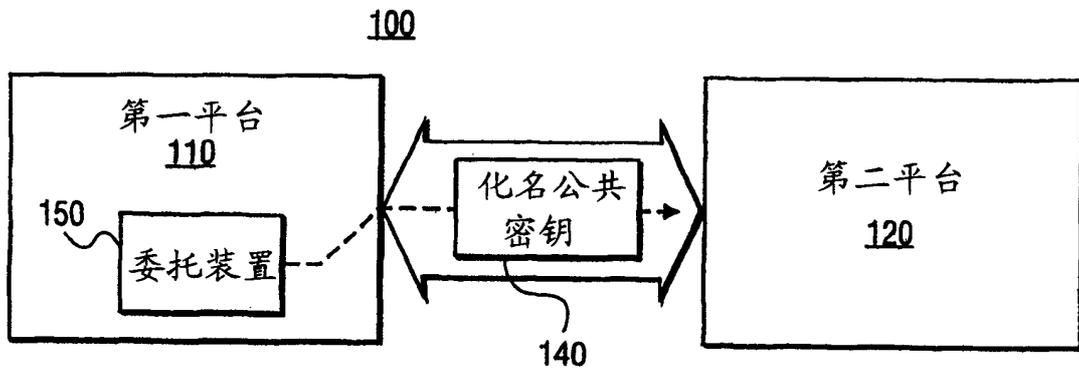


图 1

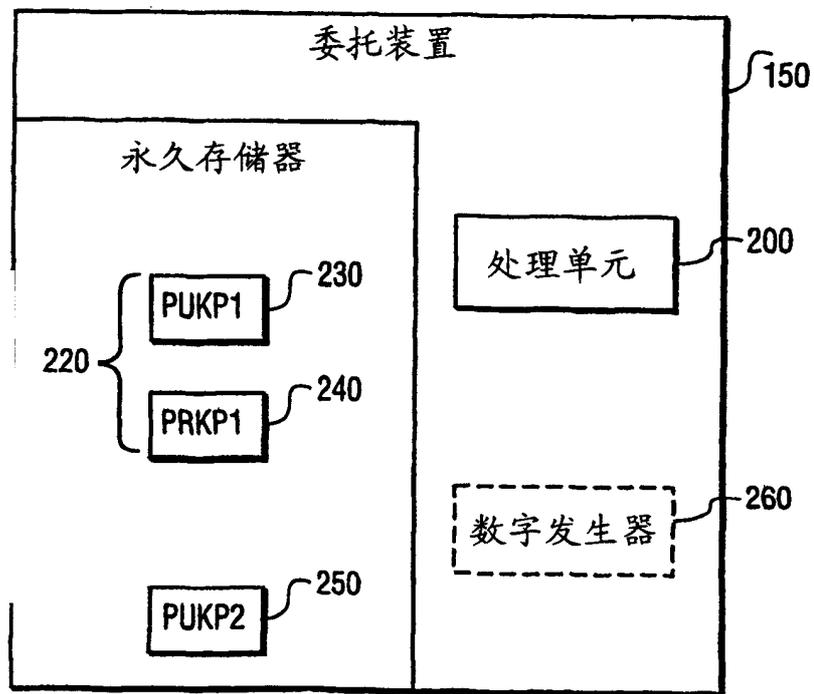


图 2

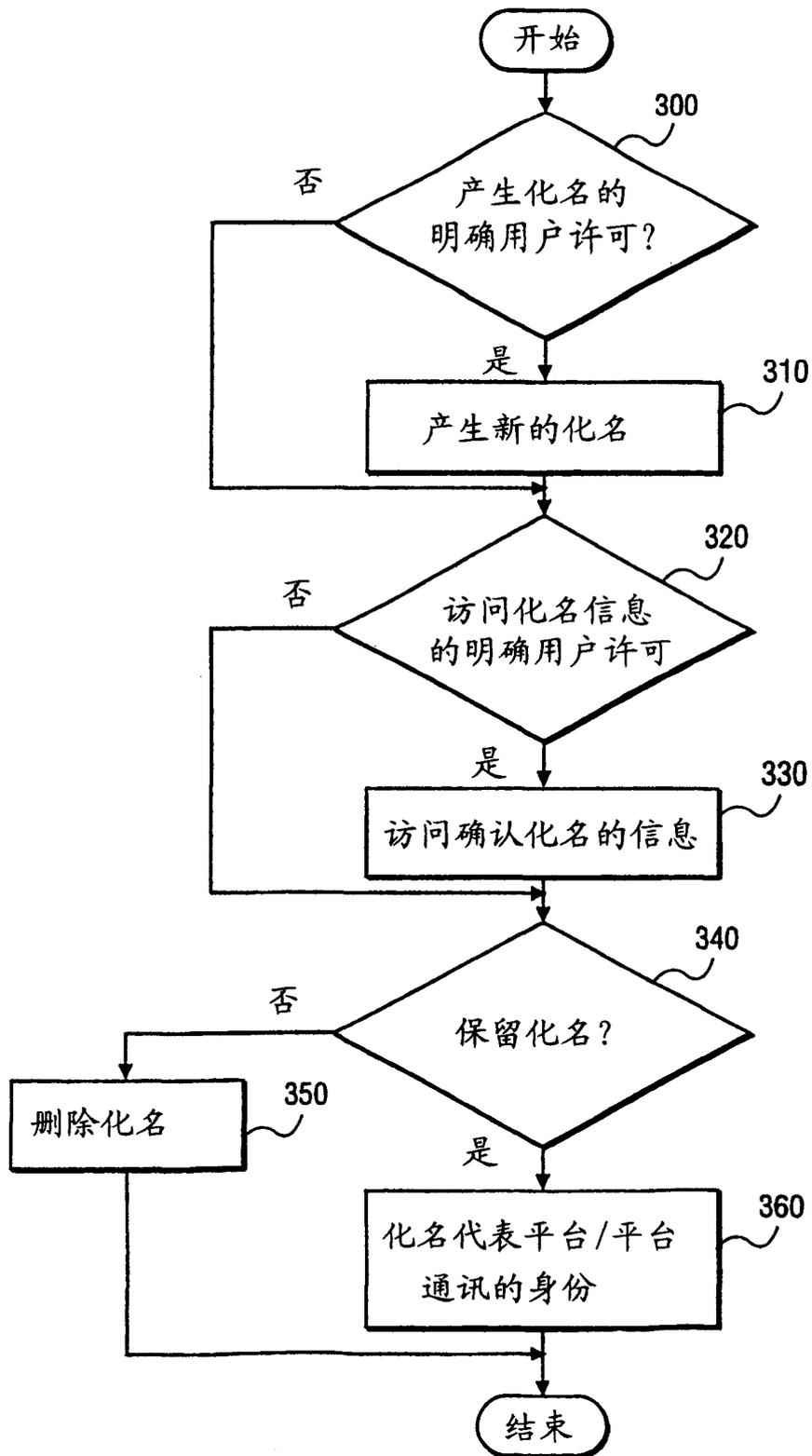


图 3

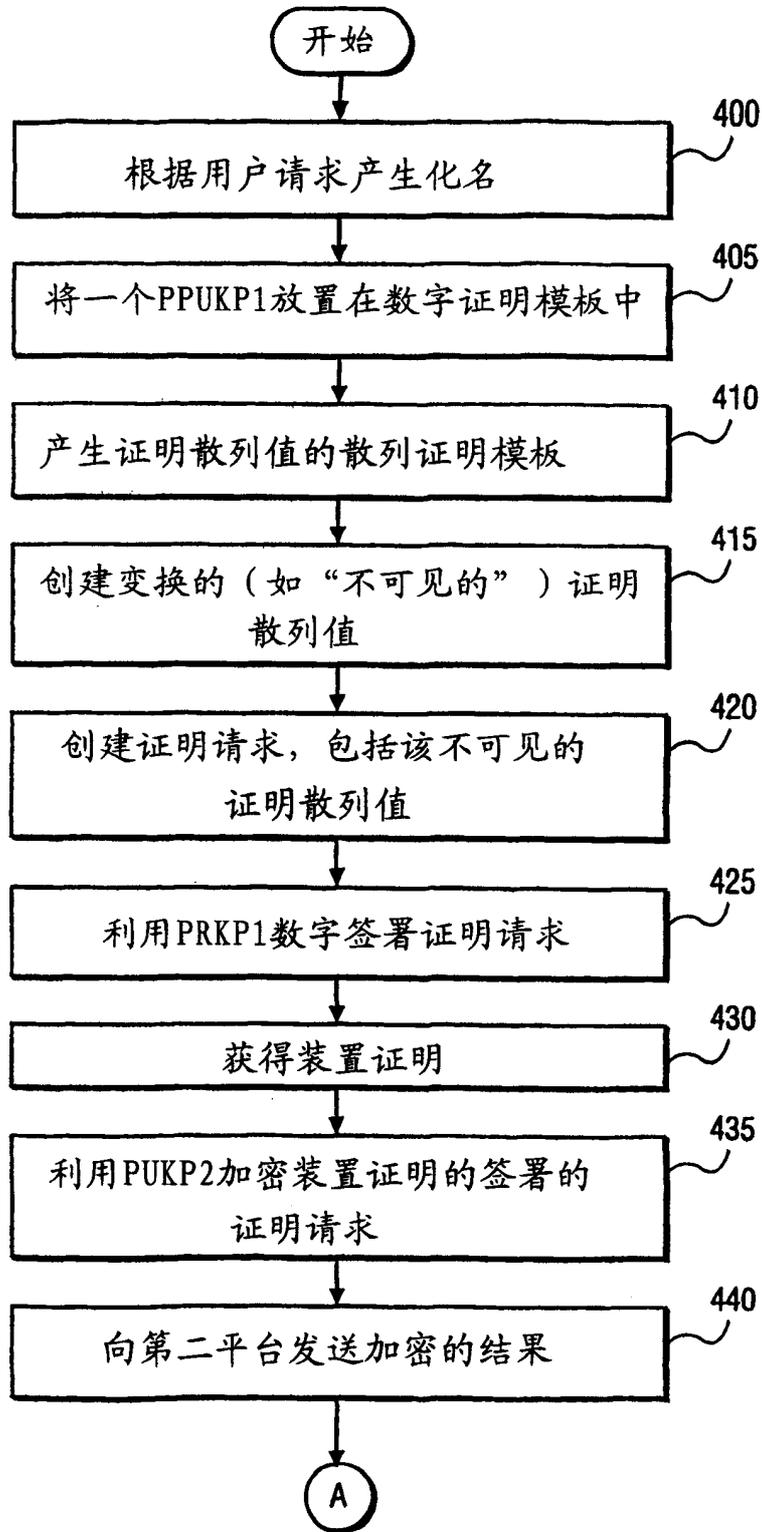


图 4

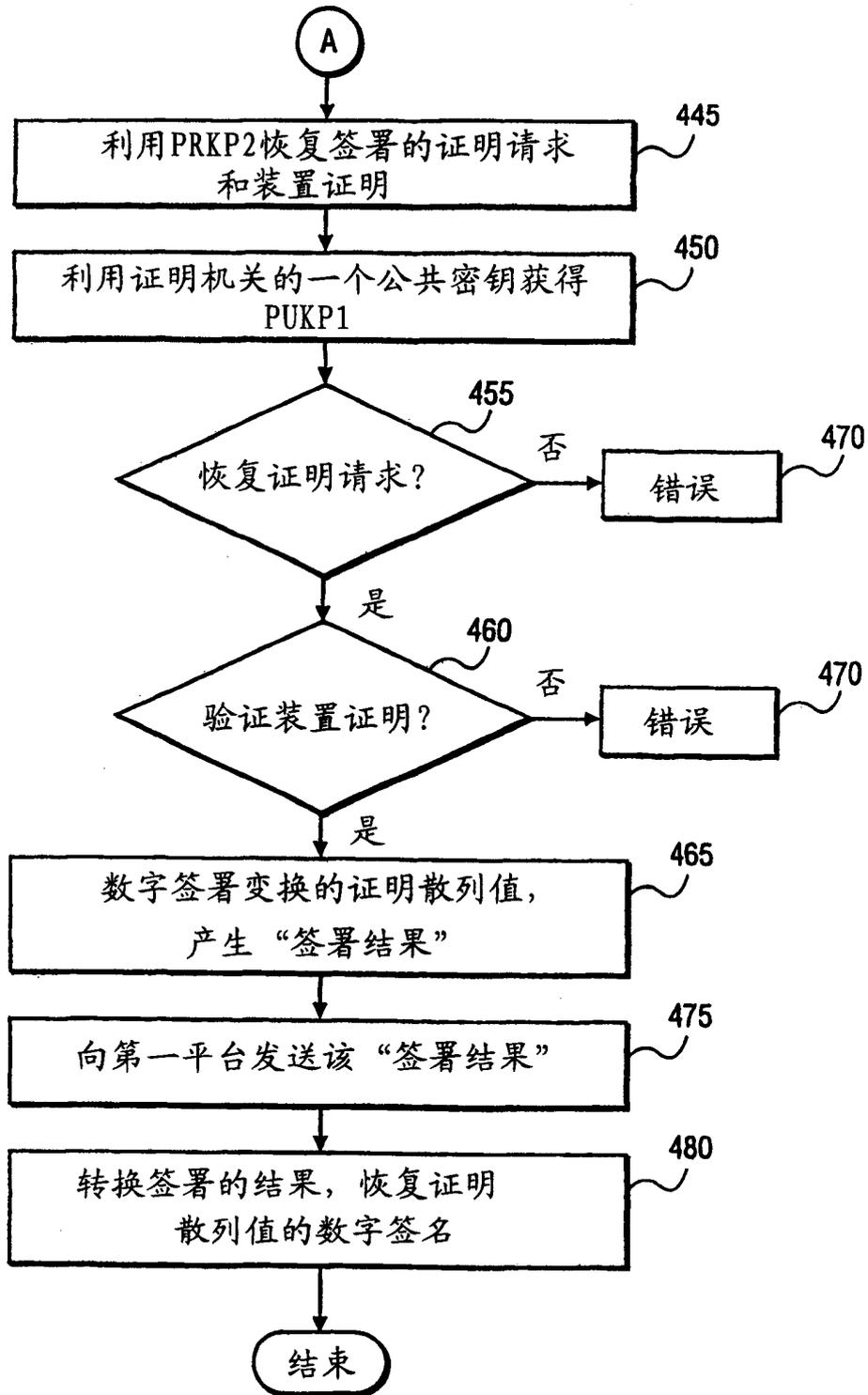


图 5