

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 9/32 (2006.01)



[12] 发明专利申请公开说明书

[21] 申请号 200380104208.8

[43] 公开日 2006 年 1 月 4 日

[11] 公开号 CN 1717895A

[22] 申请日 2003.11.6

[74] 专利代理机构 北京英特普罗知识产权代理有限公司
代理人 齐永红

[21] 申请号 200380104208.8

[30] 优先权

[32] 2002.11.27 [33] US [31] 10/306,336

[86] 国际申请 PCT/US2003/035498 2003.11.6

[87] 国际公布 WO2004/051923 英 2004.6.17

[85] 进入国家阶段日期 2005.5.26

[71] 申请人 英特尔公司

地址 美国加利福尼亚州

[72] 发明人 厄尼·布里克尔

权利要求书 5 页 说明书 9 页 附图 7 页

[54] 发明名称

用于在不泄露身份的情况下建立信任的系统
和方法

[57] 摘要

本发明的实施方案的一个方面提供了向挑战者证明证明者设备具有来自设备制造者的签名，而无需向所述挑战者泄露所述签名的方法、系统和设备。根据一种实施方式，向挑战者提供了由证明者设备持有的秘密的单向函数的结果。在证明者设备和挑战者之间利用交互证明来向挑战者证明在所述单向函数中使用的秘密已经被签上了设备签名，而无需向挑战者泄露所述秘密或者所述设备签名或者证明者设备的身份。

1. 一种方法，包括：
从挑战者设备接收验证请求；以及
5 从证明者设备向所述挑战者设备发送信息；以及
使所述挑战者设备相信所述证明者设备知道合法的签名，而无需向所述挑战者设备泄
露所述签名。
- 10 2. 如权利要求 1 所述的方法，其中，被发送到所述挑战者设备的信息包括用于所述证
明者设备的设备证书。
- 15 3. 如权利要求 1 所述的方法，进一步包括：
基于单向函数生成 k 值；以及
在所述证明者设备中生成私钥-公钥对，所述私钥-公钥对包括私钥和公钥，其中 k 值
和所述公钥被包括在发送给所述挑战者设备的所述信息中。
- 20 4. 如权利要求 3 所述的方法，其中，所述 k 值被定义为 $k = h^m \bmod P$ ，其中 h 是由
所述证明者设备生成的独有数字，m 是随机生成的数字，并且 P 是一个大的质数。
- 25 5. 如权利要求 1 所述的方法，其中，“使所述挑战者设备相信所述证明者设备知道合
法的签名，而无需向所述挑战者设备泄露所述签名”的步骤包括：
向所述挑战者设备发送所述证明者设备知道所述签名的交互证明，而无需向所述挑战
者设备泄露所述签名。
- 30 6. 如权利要求 1 所述的方法，进一步包括：
使所述挑战者设备相信所述证明者设备知道所述合法签名，而无需泄露所述证明者设
备的身份。
- 35 7. 如权利要求 1 所述的方法，其中，
使所述挑战者设备相信所述证明者设备所知道的签名不是在受损害设备签名的废止
列表中，而无需泄露所述证明者设备所知道的签名。
8. 一种方法，包括：
使挑战者相信证明者具有已知实体的合法签名，而无需泄露所述签名；以及
使所述挑战者相信所述签名不是在受损害签名的废止列表中，而无需泄露所述签名。
9. 如权利要求 8 所述的方法，其中“使挑战者相信证明者具有已知实体的合法签名，
而无需泄露所述签名”的步骤包括：
基于单向函数生成 k 值；以及

在所述证明者设备中生成私钥-公钥对，所述私钥-公钥对包括私钥和公钥，其中所述 k 值和所述公钥被包括在发送给所述挑战者的信息中。

5 10. 如权利要求 8 所述的方法，其中“使挑战者相信证明者具有已知实体的合法签名，而无需泄露所述签名”的步骤包括：

向所述挑战者发送所述证明者知道所述合法签名的交互证明，而无需向所述挑战者泄露所述签名。

10 11. 如权利要求 8 所述的方法，其中“使所述挑战者相信所述签名不是在废止列表中”的步骤包括：

保存一个废止列表，该列表中的信息对应于被认为受到损害的一个或多个证明者，以及

将所述证明者的信息与所述废止列表中的信息进行比较。

15 12. 如权利要求 8 所述的方法，其中使挑战者相信证明者具有已知实体的合法签名意味着在概率上有可能所述证明者知道所述签名，并且不向所述挑战者泄露所述签名意味着对于所述挑战者而言，基于所述证明者所泄露的信息计算出所述签名在计算上是不可行的。

20 13. 一种方法，包括：

使第一挑战者设备相信第二设备具有合法签名，而无需将所述签名透露给所述第一设备；以及

使第三挑战者设备相信所述第二设备具有合法签名，而无需将所述签名透露给所述第三设备，其中由所述第二挑战者设备提供给所述第一挑战者设备和所述第三挑战者设备的信息不足以让所述第一挑战者设备和所述第三挑战者设备确定它们正在与相同的第二设备进行通信。

30 14. 如权利要求 13 所述的方法，其中“使所述第一挑战者相信所述第二设备具有合法的签名，而无需透露所述签名”的步骤包括：

基于单向函数生成 k 值；以及

在所述证明者设备中生成私钥-公钥对，所述私钥-公钥对包括私钥和公钥，其中所述 k 值和所述公钥被包括在发送给所述挑战者的信息中。

35 15. 如权利要求 13 所述的方法，其中由所述第二设备提供给所述第一挑战者设备的信息中至少有一部分是不同于由所述第二设备提供给所述第三挑战者设备的信息。

16. 一种方法，包括：

向第一挑战者平台泄露由证明者平台持有的秘密的单向函数的结果；以及

向所述第一挑战者平台证明所述秘密具有合法的签名，而无需向所述第一挑战者平台

泄露所述秘密。

17. 如权利要求 16 所述的方法，进一步包括：

向第二挑战者平台泄露由所述证明者平台持有的所述秘密的单向函数的结果；以及

5 向所述第二挑战者平台证明所述秘密具有所述合法的签名，而无需向所述第二挑战者平台泄露所述秘密，并且使得所述第一挑战者和第二挑战者无法确定它们正在与相同的证明者平台进行通信。

18. 如权利要求 16 所述的方法，进一步包括：

10 向所述第一挑战者平台发送所述证明者平台知道所述合法的签名的交互证明，而无需向所述挑战者泄露所述签名。

19. 如权利要求 16 所述的方法，进一步包括：

使所述第一挑战者平台相信所述证明者平台的未泄露的签名不在废止列表中。

15 20. 如权利要求 16 所述的方法，其中向所述第一挑战者平台证明所述秘密具有合法的签名意味着在概率上有可能所述证明者平台知道所述秘密，并且向所述第一挑战者平台证明此情况，而无需向所述第一挑战者平台泄露所述秘密意味着对于所述第一挑战者平台而言，基于所述证明者平台所泄露的信息计算出所述秘密在计算上是不可行的。

20 21. 一种方法，包括：
第一次使挑战者相信证明者具有已知实体的合法签名，而无需泄露所述签名；以及
第二次使同一挑战者相信所述证明者具有已知实体的合法签名，而无需泄露所述签名，其中所述挑战者不能确定在所述第一次和第二次期间使用的是相同的签名。

25 22. 如权利要求 21 所述的方法，进一步包括：
向所述挑战者发送所述证明者知道所述合法签名的交互证明，而无需向所述挑战者泄露所述签名。

30 23. 如权利要求 21 所述的方法，进一步包括：
使所述挑战者相信所述证明者的签名不在废止列表中。

35 24. 一种方法，包括：
在第一设备中生成第一签名密钥对，所述第一签名密钥对包括公共签名密钥和私有签名密钥；
向第一挑战者提供所述第一公共签名密钥；以及
向所述第一挑战者证明所述第一设备具有已签名的秘密，而无需泄露被用来签名所述秘密的签名或者泄露所述私有签名密钥。

25. 如权利要求 24 所述的方法，进一步包括：

向所述第一挑战者发送所述第一设备知道所述已签名的秘密的交互证明，而无需向所述第一挑战者泄露所述已签名的秘密。

5 26. 如权利要求 24 所述的方法，其中向所述第一挑战者证明所述第一设备具有被用来
签名所述秘密的签名意味着在概率上有可能所述证明者设备知道所述秘密，并且向所述第
一挑战者证明此情况，而无需向所述第一挑战者泄露被用来签名所述秘密的签名或者泄露
所述私有签名密钥意味着对于所述第一挑战者而言，基于所述证明者设备所泄露的信息来
计算出所述秘密、被用来签名所述秘密的签名、或者所述私有密钥在计算上是不可行的。

10

27. 如权利要求 24 所述的方法，进一步包括：

向所述第一挑战者证明所述第一设备具有已签名的秘密，而无需泄露所述设备的身份。

15

28. 一种设备，包括：

通信端口；以及

处理单元，所述处理单元被配置来：

通过所述通信端口与挑战者平台进行通信，以及

使所述挑战者平台相信所述设备知道秘密，而无需泄露所述设备的身份。

20

29. 如权利要求 28 所述的设备，其中“使所述挑战者平台相信所述设备知道秘密，而
无需泄露所述设备的身份”包括：

向所述挑战者平台证明它具有已知实体的合法签名，而无需泄露所述签名，以及

将与所述秘密相关的值绑定到与所述挑战者平台之间的通信，使得在不违背所述证明
的情况下，不同的值无法被替换。

25

30. 如权利要求 28 所述的设备，其中向所述挑战者证明所述设备知道所述秘密意味着
在概率上有可能所述证明者设备知道所述秘密。

30

31. 一种系统，包括：

挑战者设备；以及

通信地耦合到所述挑战者设备的证明者设备，所述证明者设备被配置来：

使所述挑战者相信所述证明者设备具有已知实体的合法签名，而无需泄露所述
签名。

35

32. 如权利要求 31 所述的系统，其中“使所述挑战者设备相信所述证明者设备具有已
知实体的合法签名，而无需泄露所述签名”包括：

向所述挑战者设备泄露所述证明者设备所持有的秘密的单向函数的结果，以及

向所述挑战者设备证明所述秘密具有合法签名，而无需向所述挑战者设备泄露所述秘

密。

33. 如权利要求 31 所述的系统，其中所述证明者设备被进一步配置来：

使所述挑战者设备相信所述签名不是在受损害签名的废止列表中，而无需泄露
5 所述签名。

34. 如权利要求 33 所述的系统，其中“使所述挑战者设备相信所述签名不是在废止列
表中”包括：

保存一个废止列表，该列表中的信息对应于被认为受到损害的一个或多个证明者设
10 备，以及

将所述证明者设备的信息与所述废止列表中的信息进行比较。

用于在不泄露身份的情况下建立信任的系统和方法

5 技术领域

本发明的各种实施方案一般属于安全通信领域。更具体地，至少本发明的一种实施方案涉及使得第一设备能够向第二设备证明它具有合法的签名，而不必泄露所述签名。

10 背景技术

在很多现代通信系统中，包括计算机网络在内，被交换信息的可靠性和安全性是一件很重要的事情。

15 例如，在可信（trusted）计算平台联盟（TCPA）模型中，每台计算机（PC）都具有被称为可信平台模块（TPM）的可信硬件设备。在一种实现方案中，TPM 可以记录有关 PC 的软件和硬件环境的信息。每个 TPM 都具有唯一的背书密钥（EK）。有一个证书被发给 EK，它包含了有关 TPM 和平台的信息。当一个外部方（此后被称为挑战者（challenger））想要了解 PC 的软件和/或硬件环境时，该挑战者可以让 TPM 给出报告。
20 挑战者想要确信所述报告真的来自合法的 TPM。PC 的所有者想要保持尽可能多的保密性（privacy）。具体地说，PC 的所有者想要能够向两个不同的挑战者给出报告，而这些挑战者又不能确定这些报告来自同一个 TPM。

25 由 TCPA 提出的一种解决方案是建立可信第三方（TTP）。TPM 将会创建一个证明身份密钥（AIK），并将会把由 EK 签名的证书请求中的密钥的公共部分发送到 TTP。TTP 将会检查 EK 是合法的，签名是完好的，并且将会为 AIK 发出证书。TPM 然后将会在从挑战者接收到请求后使用 AIK 和 TTP 的证书。这些都将和 EK 无关，因此挑战者不会获得有关 EK 的任何信息。这种方法的问题在于它需要建立 TTP。实际上，识别可用作 TTP 的各方以及用于这种方法的可行商业模型已经证明是实质性的障碍。

30 因此，在 TCPA 体系结构中需要 TTP 一直是个问题。然而，尚未有人提出一种无需使用 TTP 而实现匿名和安全要求的密码协议。

附图说明

35 图 1 图示了根据本发明的实施方案可以实现直接证明方案的系统。
图 2 是图示了根据本发明的一种实施方案包括可信平台模块的平台的一种实施方案的框图。
图 3 图示了根据本发明的一种实施方案，在制造过程中建立 TPM 的过程。

图 4 图示了为根据本发明的一种实施方案而制造的每个平台所执行的建立过程。

图 5 图示了根据本发明的一种实施方案，供一个平台（证明者（prover））向挑战者证明它知道验证信息，而不用泄露这一信息的交互证明方法。

图 6 是图示了在挑战者和平台之间实现图 5 的交互证明（IP1）的一种方法的流程图。

5 图 7 是图示了在挑战者和平台之间实现图 5 的交互证明（IP2）的一种方法的流程图。

图 8 图示了根据本发明的一种实施方案，如何在有限数量的轮次中实现直接证明，从而加速验证过程。

具体实施方式

10

在对本发明各实施方案的以下详细描述中，阐述了很多具体的细节，以提供对本发明一种或多种实施方案的各个方面完整理解。然而，在没有具体细节的情况下也可以实现本发明的一种或多种实施方案。此外，没有详细描述公知的方法、过程和/或组件，以免不必要地模糊了本发明的各个实施方案。

15

在以下描述中，使用某些术语来描述本发明的一种或多种实施方案的某些特征。例如，“平台”包括任何类型的设备、计算机、处理单元等。术语“挑战者”是指在向请求者透露或者提供所请求的信息之前，向所述请求者请求对可靠性或权限进行某种检验的任何个人、平台、系统、软件和/或设备。术语“证明者”（例如证明者设备）是指已被请求对其权限（authority）、合法性（validity）和/或身份（identity）提供某种证明的任何个人、平台、系统、软件和/或设备。术语“设备制造者”（例如设备制造者 C）是指制造或者配置一个设备或平台（例如可信平台模块）的任何个人、平台、系统、实体、软件和/或设备。术语“设备制造者”可以与术语“证实（verifying）制造者”互换使用。术语“HASH”是指任何散列函数或算法或其等同物。

20
25

在下面讨论的对本发明各种实施方案的描述和图示中，系数、变量以及其他符号用相同的标号或名称来表示。因此，当一个符号（例如 h）出现在不同的解释部分中时，在全篇中指的是同一符号。

30

本发明的一种实施方案的一个方面提供了在不使用可信第三方（TTP）的情况下，向验证系统提供设备的匿名的方式。

本发明的一种实施方案的一个方面提供了向挑战者证明一个证实平台或设备具有来自设备制造者的签名，而不用向挑战者泄露所述签名的方法、系统和设备。

35

本发明的一种实施方案的另一方面提供了向挑战者提供证明者设备（例如，发出请求的设备）所持有的秘密的单向函数（one-way function）的结果，并且向挑战者证明在所述单向函数中使用的秘密已经被签上了设备签名，而不用将所述秘密或签名泄露给挑战者的方法、系统和设备。

使用在这里，“证明（prove）”或者“使挑战者相信”证明者具有或者知道签名或秘密意味着基于透露给挑战者的信息和证明，非常在概率上有可能 (probabilistically likely) 证明者具有所述签名或秘密。向挑战者证明这一情况，而不用向挑战者“泄露”或“透露”签名或
5 秘密意味着基于透露给挑战者的信息，要确定所述签名或秘密在计算上是不可行的 (computationally infeasible)。

这样的证明此后被称为直接证明。术语“直接证明”是指交互证明和/或零知识证明，这些类型的证明在本领域中是公知的。
10

图 1 图示了其中可以实现根据本发明一种实施方案的直接证明方案的系统。平台 A 102 (挑战者) 请求平台 B 104 (证明者) 提供有关其自身的一些信息，并且平台 B 104 提供所述所请求的信息。然而，平台 A 102 想要确认所请求的信息是来自由设备制造者 C 制造的设备。因此，平台 A 102 对平台 B 104 发出挑战，让平台 B 104 表明它具有设备制造者 C 所生成的签名。平台 B 104 通过提供使平台 A 102 相信平台 B 104 具有设备制造者 C 所生成的签名来对这样的请求做出应答，而不用泄露所述签名的信息。
15

在本发明的一种实施方案中，平台 B 104 可以包括可信平台模块 (TPM) 106。它是由设备制造者所制造的，使得它执行这一发明所需的功能，并且遵守这里所描述的协议的操作。
20 总地来说，TPM 应当被制造为保持这里所描述的安全特性。例如，在下面进行描述并且在图 6 中图示的协议 IP1 中，TPM 使用指定的值来执行指定的功能。TPM 应当被制造或配置为使用不会在协议中产生安全缺陷（例如，使得设备的身份有可能被确定，等等）的值（例如，上面所指定的值）。

图 2 是图示了根据本发明一种实施方案的、具有可信平台模块 (TPM) 204 的设备或平台 200 (例如平台 B 104) 的一种实施方案的框图。设备 200 可以包括耦合到 TPM 204 的处理单元 202。在一种实现方式中，存储设备 206 也可以被包括在设备 200 中，从而允许存储有关设备 200 的信息（例如硬件信息、软件信息等）。在本发明的各种实现方式中，平台或设备 200 可以是诸如计算机、移动设备等的电子设备。
25

图 3 图示了根据本发明的一种实施方案，为每个平台类 (platform class) 所执行的建立过程。一个平台类可由设备制造者定义为包括一种或多种类型的平台或设备。例如，一个平台类可以是具有相同的安全相关信息的所有平台的集合。每个平台都具有一组有关该平台的安全相关信息。这一信息可能包含了被包括在 TCPA 模型中的 EK 或 AIK 证书中的
35 信息的一部分。它还可能包括特定平台或设备的制造者号和型号。

对于每个平台类，设备制造者都创建该制造者为这一平台类所使用的密码参数。设备制造者创建一个签名密钥 (signature key)，它使用该签名密钥来签名它所制造的设备（例如设备 200）的秘密。

在本发明的一种实施方案中，设备制造者采用 RSA 算法（由 Ronald Rivest、Adi Shamir 和 Leonard Adelman 定义的公钥密码系统），利用公共模数 n、公共指数 d 和私有指数 e 来创建 RSA 公钥、私钥（public key, private key）对（在 302 中）。这可以使用公知的方法来创建，例如在由 Bruce Schneier, John Wiley & Sons 出版的《应用密码学》第 2 版（1995 年 10 月 18 日，ISBN: 0471117099）中所描述的方法。模数 n 应当被选定得足够大，使得它对因数 n 在计算上是不可行的。

在 304 中设备制造者指定参数 Z，这是一个位于 0 和 n 之间的整数。

10

在 306 中设备制造者指定安全参数 W，这是一个位于 0 和 n 之间的整数。然而，将 W 挑选得过小或过大都会导致安全性问题。在一种实现方式中，可以建议将 W 选定在 2^{160} 和 $n/2^{160}$ 之间。因此，将 W 选定为约等于 \sqrt{n} 可能是一个合理的选择。

15

在本发明的一种实施方案中，设备制造者计算出一个质数 P，使得 $P=u*n+1$ （在 308 中）。除了 $u*n+1$ 是一个质数外，u 的值没有什么特殊的。例如，可以使用最小的这种 u 值。一般地，P 值应当足够大，使得计算离散的对数 mod P 在计算上是不可行的。

20

设备制造者生成平台类证书，该证书包括密码参数 e、n、u、P、Z、W，该平台类的安全相关信息，以及所述设备制造者的名称（在 310 中）。在一种实施方案中，参数 u 和 P 两者不会全都包括进来，这是因为给定了 n 和这两个参数之一后，另一个参数可以通过 $P=u*n+1$ 计算出来。

25

在本发明的一种实施方案中，设备制造者对几个不同的平台类使用相同的 e、n、u、P、W，针对不同的平台只是改变 Z 值而已。在这种情形下，Z 的值应当被选定为相差至少 4W。

一旦生成了平台类证书，设备制造者就将所述类证书提供给它所制造的、属于那一特定平台类的设备（在 312 中）。

30

在不偏离本发明的一种或多种实施方案的情况下，可以用多种方式完成平台类证书从证明者设备或平台（例如图 1 中的平台 A）到挑战者的分发。这些密码参数（即平台类证书）应当以下列方式被分发给挑战者，所述方式要使得挑战者相信所述类证书是由设备制造者生成的。有多种广为采用的标准方法来通过直接向挑战者分发所述参数，或者通过让证实机构来签名所述平台类证书而完成这项工作。在后一种情形中，证实机构的公钥必须被分发给挑战者，并且已签名的平台类证书可被提供给所述平台类中的每个设备或平台（例如证明者设备）。然后所述设备可以将已签名的平台类证书提供给挑战者。

图 4 图示了为根据本发明的一种实施方案而制造的证明者平台或设备所执行的建立过程。证明者设备选定一个随机数 m，使得 $0 < m - Z < W$ （在 402 中）。证明者设备可以在

将这个随机数 m 发送给证实制造者以获得签名前，将它隐蔽起来（在 404 中）。在这种情形下，证明者设备在 1 和 $n-1$ 之间选定一个随机数 B （在 406 中），并且计算 $A=B^e \bmod n$ （在 408 中）。证明者设备计算 $m'=m*A \bmod n$ （在 410 中）。

5 如果所述设备没有将 m 隐蔽起来，则该设备使用 $m'=m$ 和 $A=1$ （在 412 中）。

证明者设备将 m' 发送给证实制造者（在 414 中）。证实制造者计算 $c'=m'^d \bmod n$ （在 416 中），并且将 c' 提供给所述设备（在 418 中）。所述设备计算 $c=c'*B^{-1} \bmod n$ （在 420 中）。注意，这意味着 $c=m^d \bmod n$ 。然后数字 c 和 m 被存储在 TPM 中（在 422 中）。

10 c 和 m 构成的对被称为设备制造者的签名。

图 5 图示了根据本发明的一种实施方案，证明者设备向挑战者证明它具有来自证实制造者的签名，而不用泄露所述签名的方法。挑战者（例如平台 A 102）可以发送消息，向具有 TPM 的证明者设备索要（seeking）合法性（例如，确认该设备的合法性）（在 502 中）。这个消息可以包含挑战者的名称。证明者设备将包括数字 n 的设备证书（例如平台类证书）发送给挑战者（在 504 中）。证明者设备中的 TPM 创建 AIK 私钥-公钥对（在 506 中）。所述私钥-公钥对包括公钥和私钥。在一种实施方案中，TPM 可能已在早些时候创建了 AIK 私钥-公钥对。TPM 创建或生成值 h （在 508 中）。可以用多种方式来确定值 h ，包括随机地生成值 h ，以及按照确定的方式来生成值 h 。 h 值应当具有以下性质，即 $h^n=1 \bmod P$ ，并且 TPM 为每个挑战者使用不同的 h 值。

在本发明的一种实施方案中，可以以随机或伪随机的方式生成值 h 。例如，TPM 可以在 1 和 $n-1$ 之间选择一个随机数 j ，并且计算 $h=j^u \bmod P$ 。

25 TPM 计算 k 值， $k=h^m \bmod P$ （在 510 中）。证明者设备然后向挑战者发送计算出的值 h 和 k 以及 AIK 公钥（在 512 中）。

在本发明的另一种实施方案中，可以用确定的方式生成值 h 。例如，TPM 可以由挑战者的名称，以确定的方式来计算 h 。这样做的一种方法就是针对几个值计算 $H_i=\text{HASH}(i, 30$ 挑战者的名称），其中的几个值例如是 $i=1, 2, 3, \dots, 10$ 的 10 个值，然后令 $j=H_1||H_2||H_3||\dots||H_{10}$ 的级联（concatenation）。然后，如上所述，TPM 计算 $h=j^u \bmod P$ ，其中 u 如前面定义的 $u=(P-1)/n$ 。TPM 计算 k 值， $k=h^m \bmod P$ 。证明者设备然后向挑战者发送计算出的值 k 以及 AIK 公钥。TPM 的用户想要确保单个 h 不由多方使用，因为这将会破坏这个 TPM 与这些多方之间的匿名关系。因此，TPM 或者证明者设备可能会保存它已使用的所有 h 35 值的列表，从而它能够禁止重复使用，或者至少能通知用户一个值是否被重复。在本发明的一种实现方式中，证明者设备还可以显示挑战者的名称，使得证明者设备的用户将会知道该名称。在这种实施方案中，挑战者确信对于每个 TPM 密钥，TPM 在证明中所能具有的只有一个 $k=h^m \bmod P$ 。所以如果挑战者连同 AIK 一起存储了 k ，那么挑战者可以确信单个 TPM 未曾创建一个以上的 AIK。这种方法可以被称为每个挑战者单个 h 的方法。

单个服务提供者可能建立多个挑战者，每一个都具有自己的名称，因而具有自己的 h。不同的挑战者将无法将来自一个 TPM 的多个 AIK 关联起来。是否在其事务内允许有多个挑战者，这是由服务提供者在实现当中来决定的。

5

然后，证明者设备进行和挑战者之间的交互证明（IP1）（在 514 中），该证明 IP1 的内容是它知道一对值 c 和 m，这对值满足 $m = c^e \bmod n$ 和 $k = h^m \bmod P$ 。证明者设备还进行在第二交互证明（IP2）中与挑战者之间的交互证明，所述第二交互证明指示出以 h 为底 k 的离散对数值位于 Z 和 Z+W 之间（在 516 中）。图 6 和 7 给出了这两个交互证明 IP1 和 10 IP2 的示例性实施方案。

图 6 是图示了在挑战者和证明者设备之间根据本发明的一种实施方案实现图 5 的交互证明 IP1 的一种方法的流程图。IP1 可被用来证明 TPM 知道 c 和 m 值，其满足 $m = c^e \bmod n$ 和 $k = h^m \bmod P$ ，而不用 TPM（证明者设备的一部分）泄露 c 或 m。挑战者向证明者设备提供保证参数（AP），例如在 10 和 40 之间的值（在 602 中）。然后 TPM 随机地选择一个值 $x \bmod n$ （在 604 中）。TPM 计算 y 值，使得 $x^*y=c \bmod n$ ，并且计算 v 值，使得 $v = h^{(x^* \bmod n)} \bmod P$ （在 608 中）。TPM 将 v 值发送给挑战者（在 610 中）。TPM 计算 HASH(AIK 公钥, x) 和 HASH(AIK 公钥, y) 的值（在 611 中）。然后挑战者选择接收 x 或 y 之一（在 612 中）。如果挑战者选择接收 x，则 TPM 将 x 发送给挑战者（在 614 中）。挑战者检验 $v = h^{(x^* \bmod n)} \bmod P$ 并且检验 HASH(AIK 公钥, x) 已被正确发送（在 616 中）。否则，如果挑战者选择接收 y（在 618 中），则 TPM 将 y 发送给挑战者，并且挑战者检验 $k = h^{(y^* \bmod n)} \bmod P$ 并且检验 HASH(AIK 公钥, y) 已被正确发送（在 620 中）。在本发明的一种实施方案中，这个检验方案被执行 AP 次（在 622 中）。

25 图 7 是图示了在挑战者和证明者设备之间根据本发明的一种实施方案实现图 5 的交互证明 IP2 的一种方法的流程图。IP2 可被用来证明 TPM 知道 m 值，满足 $Z-W < m < Z+2*W$ 以及 $k = h^m \bmod P$ ，而无需 TPM 泄露 m。

挑战者向证明者设备提供保证参数(AP)，例如在 10 和 40 之间的值（在 701 中）。TPM（证明者设备的一部分）随机地选择一个数 t，满足 $0 < t < W$ （在 702 中）。TPM 计算 $g_0 = h^t \bmod P$ （在 704 中）以及 $g_1 = g_0 * h^{(t-W)} \bmod P$ （在 706 中）。TPM 生成两个随机的 30 160 位值 R₀ 和 R₁（在 708 中），计算 H₀=HASH(AIK 公钥, g₀, R₀) 以及 H₁=HASH(AIK 公钥, g₁, R₁)（在 710 中），并且按随机顺序将 H₀ 和 H₁ 发送给挑战者（在 712 中）。

35

挑战者从两个选择中挑选一个，例如 0 或 1 选择。

如果挑战者挑选 0 选择，则 TPM 将 t、R₀、R₁ 以及 H₀ 和 H₁ 的排序发送给挑战者（在 716 中）。挑战者计算 $g_0 = h^t \bmod P$ 和 $g_1 = h^{(t-W)} \bmod P$ （在 718 中）。挑战者检查 $0 < t < W$ （在 720 中）。挑战者还检查 H₀=HASH(AIK 公钥, g₀, R₀) 以及 H₁=HASH(AIK 公钥, g₁,

R_1) (在 722 中)。如果所有这些检查都通过的话, 挑战者接受 (在 724 中)。

如果挑战者挑选 1 选择, 那么如果 $m+t$ 处于 Z 和 $Z+W$ 之间的话 (在 726 中), 则 TPM 5 发送 $m' = m + t$ 、 g_0 和 R_0 (在 728 中), 并且通知挑战者使用 H_0 。挑战者检查 $H_0 = \text{HASH}(\text{AIK}$

公钥, g_0 , R_0), m' 处于 Z 和 $Z+W$ 之间的区间中, 以及 $g_0 * k = h^{m'} \bmod P$ (在 730 中)。如果 $m+t > Z+W$, 则 TPM 发送 $m' = m - W + t$ 、 g_1 和 R_1 (在 732 中), 并且通知挑战者使用 H_1 。挑战者检查 $H_1 = \text{HASH}(\text{AIK 公钥}, g_1, R_1)$, $Z < m' < Z+W$, 以及 $g_1 * k = h^{m'} \bmod P$ (在 734 中)。如果以上检查全都通过的话, 挑战者接受 (在 724 中)。

10 在 IP2 的一种实施方案中, 以上过程被重复 AP 次 (在 723 中)。注意, 如图 6 中的标号 622 处一样重复 IP1 的过程, 和/或如图 7 中的标号 723 处一样重复 IP2 的过程, 将使得未经授权的或欺骗性的证明者成功地向挑战者提供充分证明的可能性更低。也就是说, 重复证明 (例如 IP1 或 IP2) AP 次迫使证明者在每一轮都要成功, 这只有 2^{-AP} 分之一的机会。

15 在 TPM 已经成功地完成上述 IP1 和 IP2 过程后, 挑战者相信证明者设备/TPM 知道 m 和 c 值, 这两个值满足 $Z-W < m < Z+2*W$ 并且 $c = m^d \bmod n$ 。换言之, c 是 m 的签名。对于所述区间中给定的值计算出 m 的签名, 这等同于破坏了 RSA。在不知道模数 n 的因数分解的情况下计算出所述区间中的任何值的签名, 这是一项困难的计算问题。

20 在图 6 和 7 中描述的协议具有以下不足, 即在 TPM (证明者设备) 和挑战者之间需要多轮次通信。然而, 在本发明的另一种实施方案中, 这些协议可以被转换成有限轮次的协议。

25 图 8 图示了根据本发明的一种实施方案, 如何在有限数量的通信中实现直接证明, 从而加速验证过程。TPM 生成 AIK 私钥-公钥对, 其包括 AIK 公钥和 AIK 私钥, 并且将 AIK 公钥 (或者只是 AIK 公钥的 HASH) 发送给挑战者 (在 802 中)。挑战者选择保证参数 (AP) (在 804 中), 选择一组 $2*AP$ 个随机位 (CHOICES) (在 806 中), 并且选择 320 个随机位的附加随机填充位 (在 808 中)。然后, 挑战者设置 $\text{RAND} = \text{CHOICES} \parallel \text{随机填充位}$ 30 (在 810 中), 计算出 $\text{Commitment} = (\text{AIK 公钥} \parallel \text{RAND})$, 并且将 Commitment 的 HASH 发送给 TPM, TPM 将该值存储起来 (在 812 中)。

TPM 使用上述方法之一来确定与这个挑战者之间使用的 h 值, 即或者使用随机方法生成 h , 或者在每个挑战者单个 h 的方法中由挑战者的名称生成 h (在 818 中)。

35 不再如图 6 和 7 中所示地一次串行地计算出一个循环的值, TPM 现在对于两个交互证明 (IP1 和 IP2) 生成所述方法所有轮次 (循环) 的所有计算结果, 并且将为所有轮次计算出的所有值都发送给挑战者 (在 820 中)。这组计算出的值将包括 k , h ; 由每一轮次的 IP1 得到的 v , $\text{HASH}(\text{AIK 公钥}, x)$ 和 $\text{HASH}(\text{AIK 公钥}, y)$; 以及由每一轮次的 IP2 得到的

H₀ 和 H₁。然后，挑战者将 RAND 的值发送给 TPM（在 822 中）。TPM 检验 Commitment 的初始位是 AIK 公钥的 hash，并且将 RAND 的初始 2*AC 位用作挑战者在协议期间的选择（在 824 中）。TPM 基于这些选择准备所有轮次的响应，然后将所有这些响应发送回挑战者。

5

在有限通信版本的一种实施方案中，HASH(AIK 公钥, x)和 HASH(AIK 公钥, y)不被发送给挑战者。类似地，H₀ 的值是 H₀=HASH(g₀, R₀)而不是 H₀=HASH(AIK 公钥, g₀, R₀)，并且 H₁ 的值是 H₁=HASH(g₁, R₁)而不是 H₁=HASH(AIK 公钥, g₁, R₁)。

10

在某些实现方式中，如果确定或怀疑 TPM 或其密钥已被损害（compromised），则可能期望允许挑战者废止该 TPM。

15

挑战者可以确定证明者设备的 TPM 已被损害的一个实例是用于受损害 TPM 的密钥(c 和 m)可能被广泛地散布，例如万维网上的公布（posting）。在这种情况下，挑战者可以废止该 TPM。例如，假设 c₀ 和 m₀ 是受损害 TPM 的已被公布的密钥。无论何时挑战者看到了 h 值，挑战者都要计算 k₀ = h^{m₀} mod P。如果这与证明者所给出的 k 值匹配，则挑战者得知由证明者使用的 m 与受损害 TPM 的 m₀ 相匹配，因而挑战者将不会接受它。

25

在废止的另一种实施方案中，假设挑战者一直与 AIK 值一起存储着 h 和 k 值。那么当挑战者接收到受损害的密钥 c₀ 和 m₀ 时，挑战者可以进行检查，以发现已收到的 h 和 k 值中是否有使用所述受损害的密钥 c₀ 和 m₀ 而计算出的值。挑战者通过计算 k₀ = h^{m₀} mod P，并且进行检查以发现这个值是否与他从 TPM 接收到的 k 值相匹配，从而完成上述操作。如果是的，则他废止对应的 AIK 值。如果正在使用每个挑战者单个 h 的方法，则由挑战者完成的计算要容易一些，这是因为挑战者只需计算出 k₀ 并且发现这个值是否与挑战者接收到的任何 k 值相匹配即可。

30

在挑战者可以确定密钥已被损害的另一个实例中，挑战者可以检测 TPM 的使用模式，该模式指示出已受到损害。例如，从不同证明者设备同时到挑战者的两个连接可以指示出一个受损害的密钥。如果使用的是每个挑战者单个 h 的方法，则挑战者将会得知两个连接使用了相同的 m，因为与两个连接相关联的是相同的 k = h^m mod P。挑战者可以判定秘密值可能已受到损害，因而挑战者将不再接受使用该 k 值的任何直接证明。然后，来自所述 TPM 的秘密值可以不再与所述挑战者一起使用。然而，由于这个挑战者不知道 m 的值，所以该挑战者不能告诉任何其他挑战者不要使用来自所述 TPM 的秘密值，

35

在本发明的另一种实施方案中，如果一组挑战者中有一个挑战者判定某一 TPM 的秘密值可能已被损害，那么这组挑战者可以决定他们全都想要能够废止这些秘密值。要实现这一特性，需要对前面已经描述的本发明的实施方案进行修改。修改包括如何确定 h 的值。形成一个可信废止机构（TRA）。TRA 具有公共检验、私有签名密钥对（例如标准 RSA 密钥对）。使用某种安全的分发方法将 TRA 公钥提供给 TPM，所述方法例如是让制造者

在制造期间将所述密钥放入 TPM 中。

5 TRA 生成 g 值，使得 $g^n = 1 \pmod{P}$ 。TRA 可以通过生成 1 和 P 之间的 g' 值，然后计算 $g = g'^u \pmod{P}$ 而生成 g 值。然后对于所述组的每一个挑战者，TRA 将在 1 和 n 之间随机地挑选一个指数(EXP)，并且计算 $h = g^{\text{EXP}} \pmod{P}$ 。然后，TRA 用这个挑战者的名称以及这个 h 值在证书中为该证书签名。TRA 安全地存储用来为每个挑战者创建 h 的 EXP。

10 当 TPM 与所述组的某个挑战者之间发起直接证明时，所述挑战者发送对于所述 h 值的这个证书。TPM 通过检查 TRA 的签名来验证这个证书。如果合法，则 TPM 使用这个 h 值，而不用像在先前实施方案中所描述的那样生成一个 h 值。直接证明的其他方面保持不变。

15 当将 h_i 作为其 h 值的挑战者_i宣告它想要废止创建了 $k_i = h_i^m \pmod{P}$ 的 TPM 时，TRA 获得 EXP 值 EXP_i，该值被用来计算 $h_i = g^{\text{EXP}_i} \pmod{P}$ 。注意，挑战者_i和 TRA 都不会知道挑战者_i想要废止的 TPM 中的 m 值。为了告诉挑战者_i将废止的 k 值，TRA 计算 $b_i = \text{EXP}_i^{(-1)} \pmod{n}$ ，然后计算 $k_i = k_i^{(\text{EXP}_i * b_i)} \pmod{P}$ 。注意， $k_i = h_i^m \pmod{P}$ 。注意，TRA 在这一计算过程中没有计算 m； k_i 然后被发送给挑战者_i，然后挑战者_i可以废止 k_i ，如果它想要这么做的话。

20 虽然在附图中已经示出并且描述了本发明的某些示例性的实施方案，但是可以理解的是，这些实施方案对于本发明各种实施方案的宽广方面而言仅仅是示例性的而非限制性的，这些实施方案不被限制在所示出并描述的具体解释和布置中，因为各种其他修改都是可能的。可以用硬件、可编程器件、固件、软件或它们的组合来实现本发明的多种实施方案或者它们的某些特征。

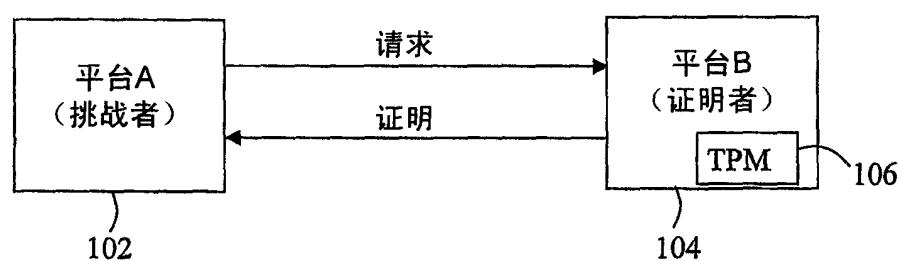


图 1

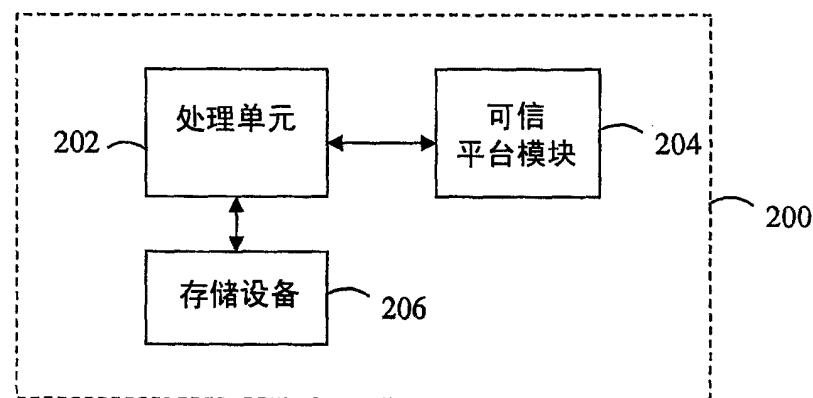


图 2

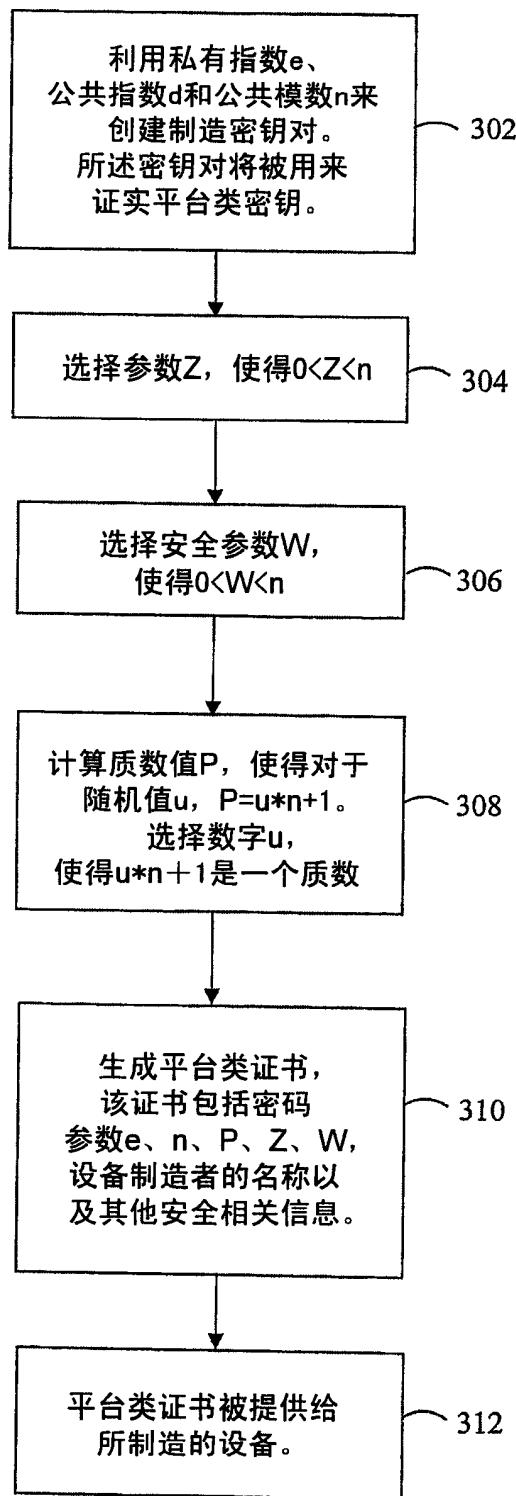


图 3

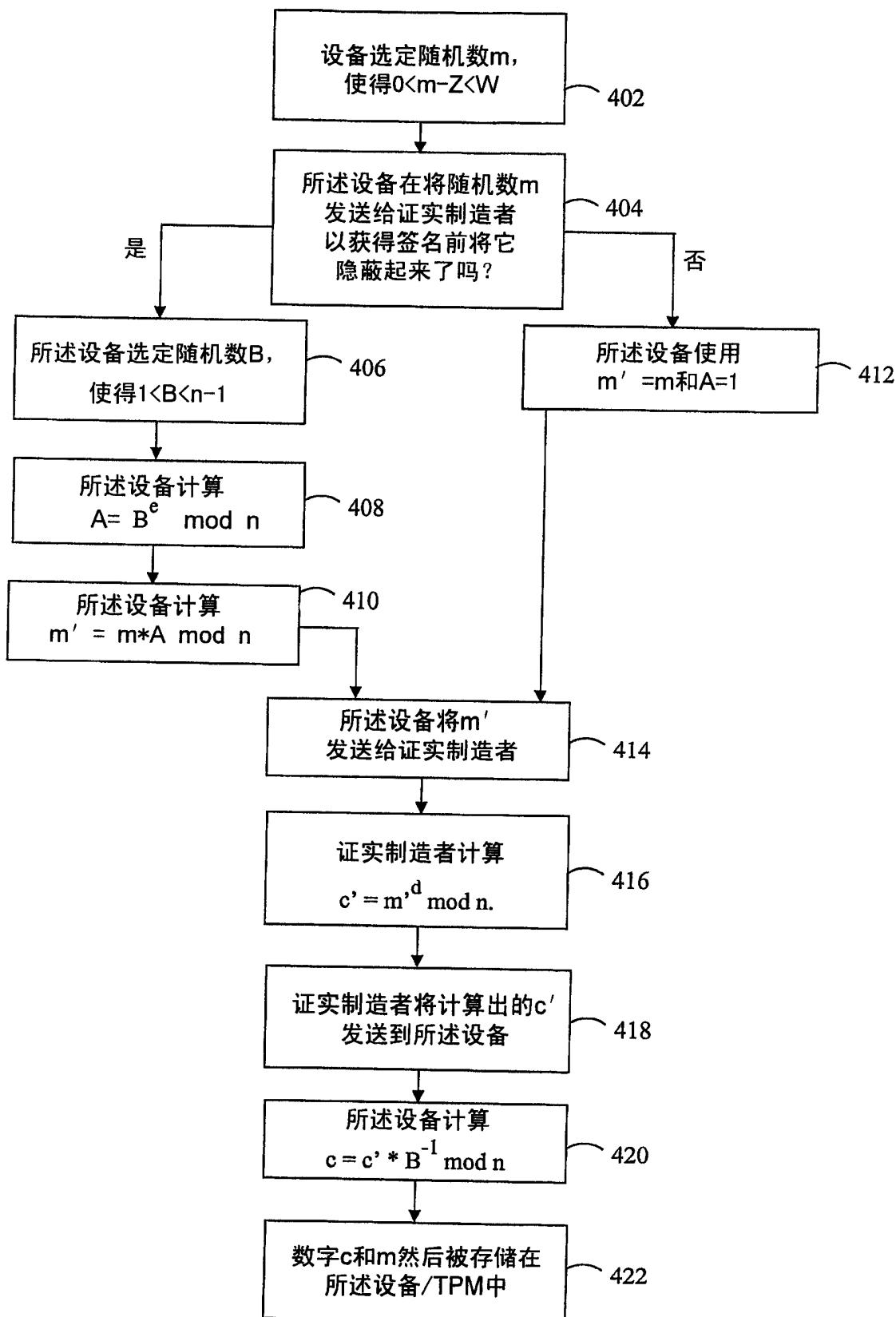


图 4

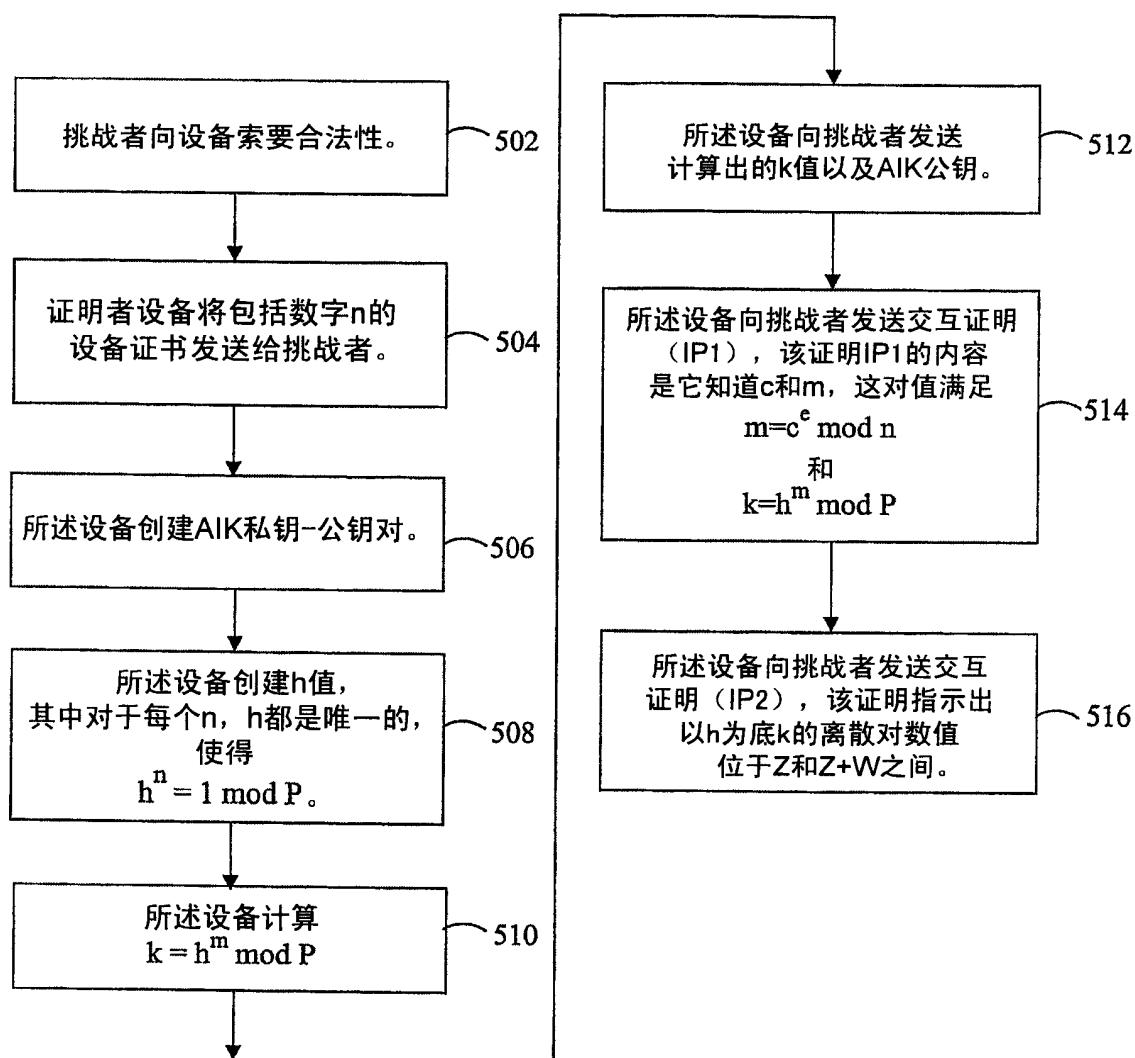


图 5

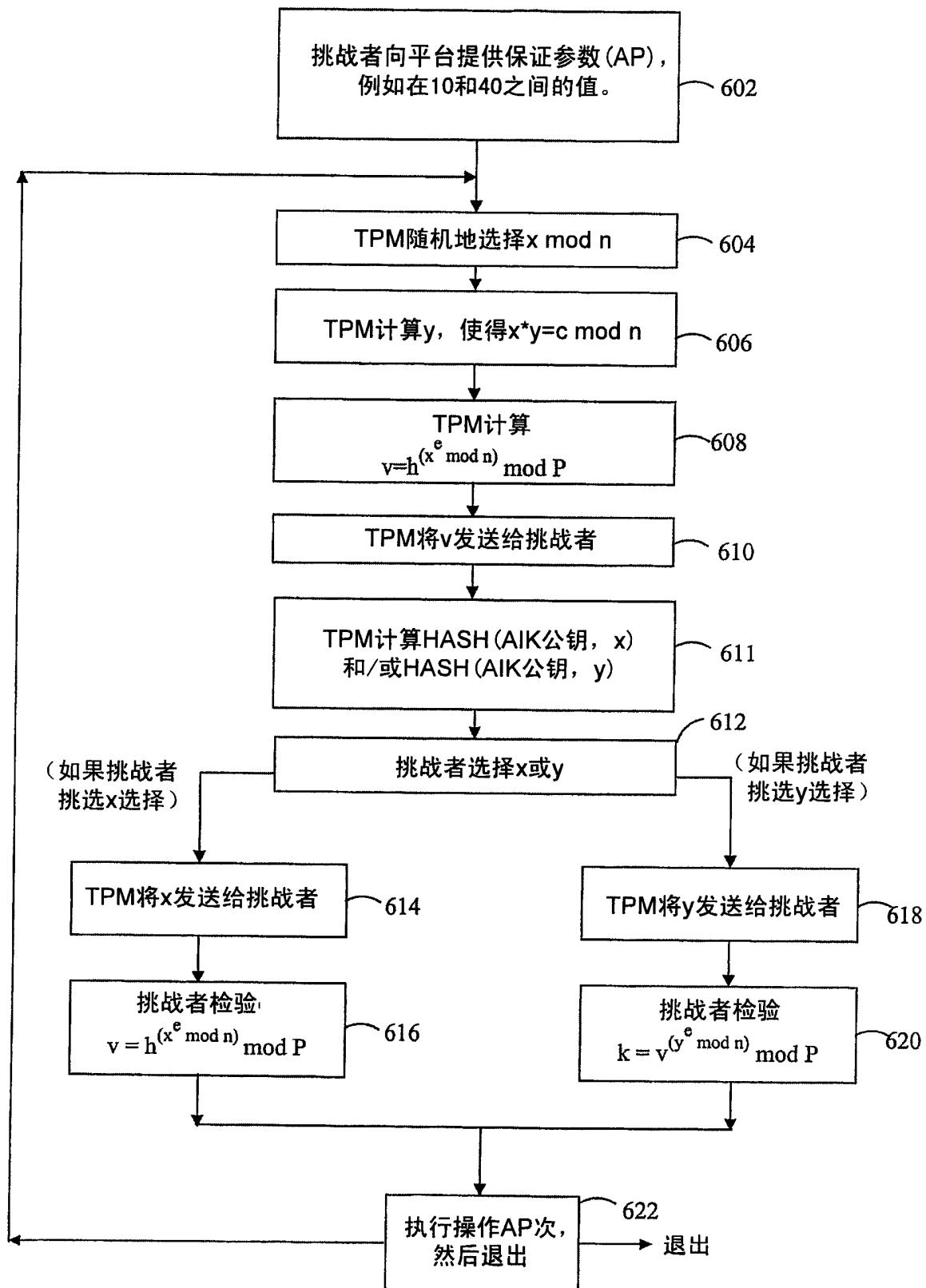
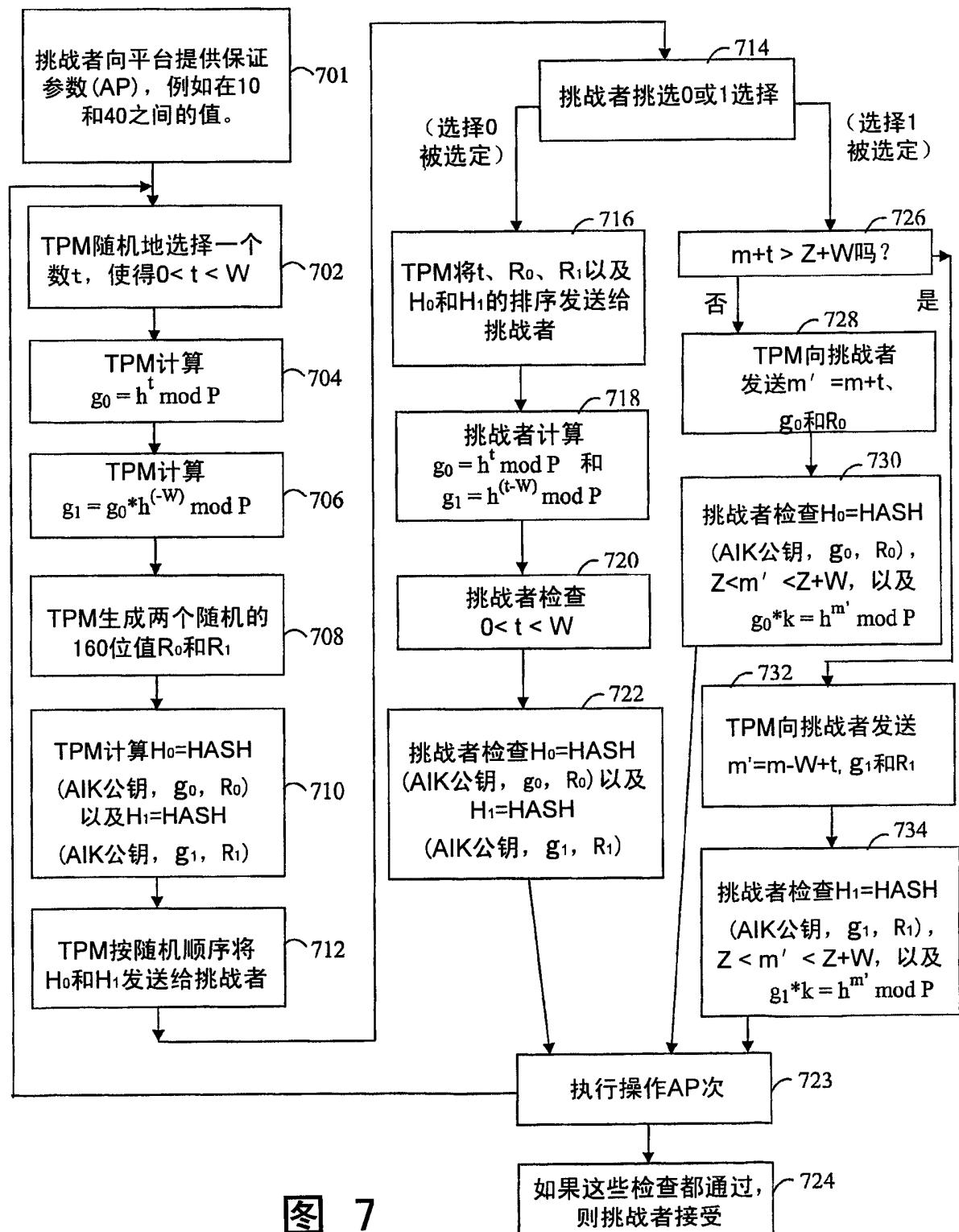


图 6



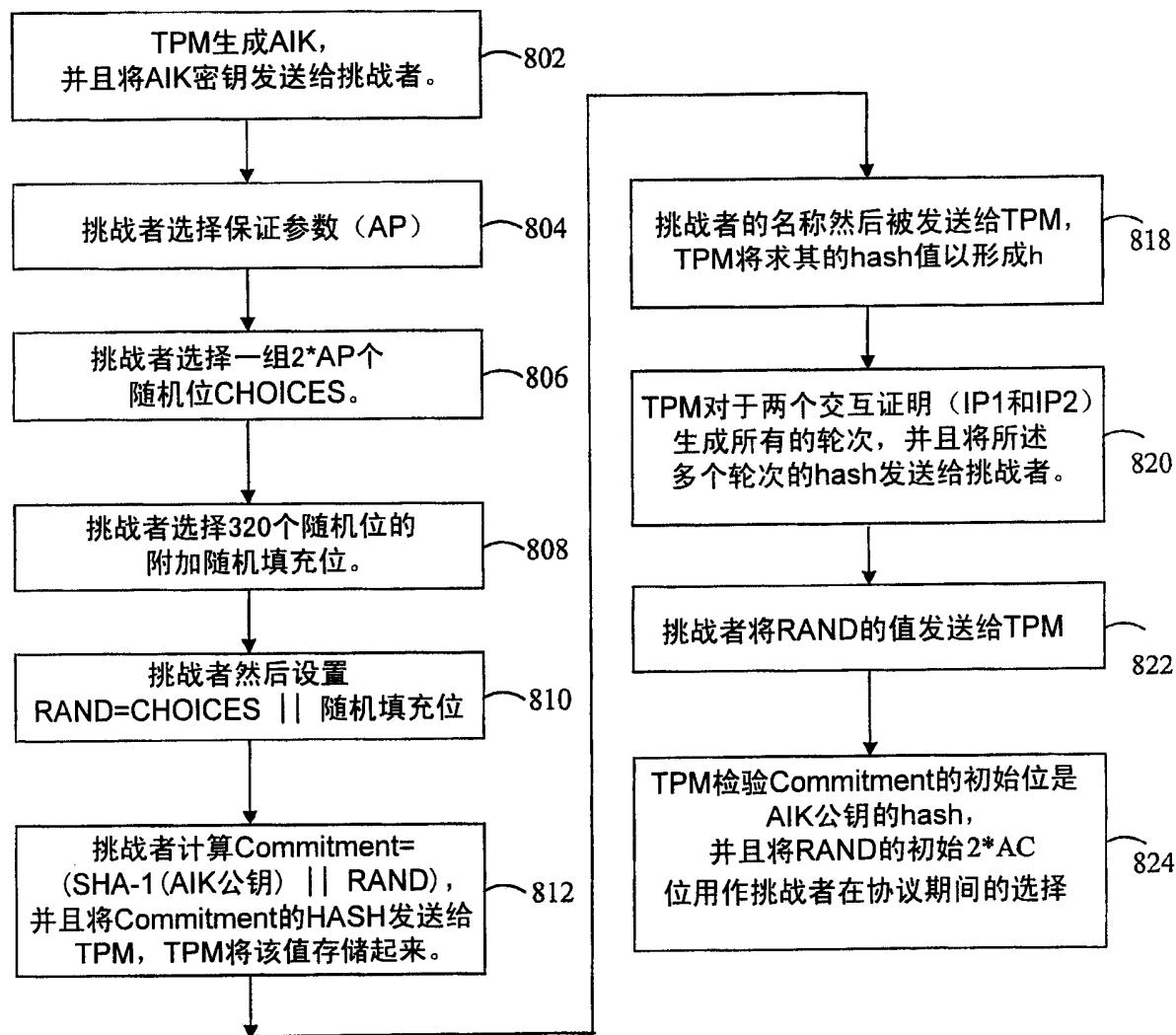


图 8