



[12] 发明专利申请公布说明书

[21] 申请号 200580019058.X

[43] 公开日 2007 年 5 月 16 日

[11] 公开号 CN 1965530A

[22] 申请日 2005.5.13

[21] 申请号 200580019058.X

[30] 优先权

[32] 2004.6.10 [33] US [31] 10/866,252

[86] 国际申请 PCT/US2005/016559 2005.5.13

[87] 国际公布 WO2006/001916 英 2006.1.5

[85] 进入国家阶段日期 2006.12.11

[71] 申请人 英特尔公司

地址 美国加利福尼亚州

[72] 发明人 E·布莱克尔

[74] 专利代理机构 上海专利商标事务所有限公司
代理人 陆 嘉

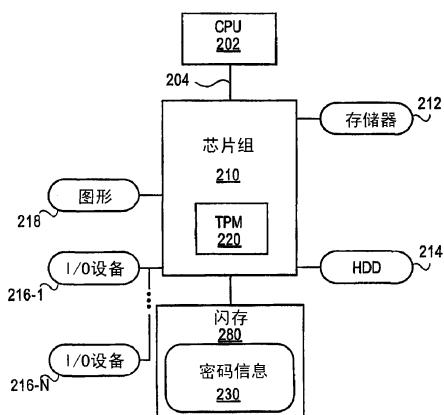
权利要求书 7 页 说明书 12 页 附图 9 页

[54] 发明名称

证实否认直接证明签名的装置和方法

[57] 摘要

在一些实施例中，描述了用于证明对否认直接证明签名的方法和装置。在一个实施例中，可信硬件设备在无需揭示可信硬件设备的唯一的设备标识信息或密码信息的情况下使验证者确信该可信硬件设备拥有该密码信息。一旦验证者确信硬件设备拥有密码信息，则验证者可向该可信硬件设备发出包括至少一个被泄漏的直接证明签名的否认签名请求。作为响应，可信硬件设备通过向验证者证实该可信硬件设备所持有的密码密钥未被用于形成该至少一个被泄漏的直接证明签名来发出对该被泄漏的直接证明签名的否认。还描述并要求保护其它实施例。



计算机系统 200

1. 一种方法，包括：

使验证者确信硬件设备拥有密码信息而无需公开所述密码信息或所述硬件设备的任何唯一的设备标识信息；以及

使所述验证者确信所述密码信息未被泄漏。

2. 如权利要求 1 所述的方法，其特征在于，使所述验证者确信所述硬件设备拥有所述密码信息包括：

由所述硬件设备执行直接证明以证实一密码密钥被存储在所述硬件设备内，所述直接证明包括多个取幂，至少一个是在没有曝露所述硬件设备的所述密码密钥的情况下将所述密码密钥作为指数进行的。

3. 如权利要求 1 所述的方法，其特征在于，使验证者确信硬件拥有密码信息包括：

使用所述密码信息计算假名 K；以及

将所述假名 K 提供给所述验证者。

4. 如权利要求 3 所述的方法，其特征在于，使所述验证者确信所述密码信息未被泄漏包括：

从所述验证者接收包括可疑签名的基数值 B_0 和假名值 K_0 的否认签名请求；以及

使所述验证者确信存储在所述硬件设备内用于构造所述假名 K 的密码密钥不匹配用于形成所述可疑签名的未知的可疑密钥 F_0 。

5. 如权利要求 1 所述的方法，其特征在于，使所述验证者确信所述密码信息未被泄漏包括：

选择随机指数值 R；

将根据从所述验证者接收的可疑基数值 B_0 和可疑假名值 K_0 、所述硬件设备的模数值 P 以及所述随机指数值 R 计算出的一个或多个值发送给所述验证者；

由所述硬件设备执行证明以否认存储在所述硬件设备内的密码密钥 F 被用于创建可疑直接证明签名，所述证明包括多个取幂，每一个是在没有曝露所述密码密钥 F、所述随机指数值 R 和其它随机指数值的情况下使用所述密码密钥 F、所述随机指数值 R 和所述其它随机指数值之一进行的。

6. 如权利要求 5 所述的方法，其特征在于，执行所述证明包括：

在无需暴露关于 R 的任何有用信息的情况下，使所述验证者确信存在所述值 R，使得：

$$S = B_0^R \bmod P \text{ 且 } T = K_0^R \bmod P; \text{ 以及}$$

在无需暴露关于 F 的任何有用信息的情况下，使所述验证者确信存在值 F，使得：

$$U = S^F \bmod P \text{ 且 } K = B^F \bmod P.$$

7. 如权利要求 5 所述的方法，其特征在于，如果 $U \neq T \bmod F$ 则所述验证者确信存储在所述硬件设备内的所述密码密钥 F 未被用于创建所述可疑直接证明签名。

8. 如权利要求 1 所述的方法，其特征在于，使所述验证者确信所述密码信息未被泄漏包括：

从所述验证者接收包括可疑签名的可疑基数值 B_0 和可疑假名值 K_0 的否认签名请求；

接收与所述可疑签名相关联的取消标识符作为可疑取消标识符；以及

如果所述可疑取消标识符匹配随来自所述验证者的签名请求接收到的取消标识符，则由所述硬件设备执行直接证明来否认所述硬件设备内的密码密钥 F 匹配所述未知可疑密钥 F_0 。

9. 如权利要求 1 所述的方法，其特征在于，使所述验证者确信所述密码信息未被泄漏包括：

(a) 从所述验证者处接收包括至少一个可疑直接证明签名的否认签名请求；

(b) 根据存储在所述硬件设备内的一个或多个取消权威机构的一个或多个公共密钥确定所述否认签名请求是否由预定的取消授权机构批准；以及

(c) 如果所述请求是由预定取消授权机构签署的，则执行直接证明来否认存储在所述硬件设备内的密码密钥被用于所述验证者用于形成所述可疑直接证明签名的直接证明中。

10. 如权利要求 8 所述的方法，其特征在于，还包括：

对多个可疑直接证明签名重复 (a) - (c)；以及

如果所述多个可疑直接证明签名超出可疑直接证明签名限值，则通知所述验证者所述验证者超出了所述可疑直接证明签名限值。

11. 一种方法，包括：

在无需揭示硬件设备的任何唯一的设备标识信息的情况下验证所述硬件设备拥有密码信息；以及

验证所述硬件设备的密码密钥未被用于生成验证者所持有的至少一个可疑签名，其中用于生成所述可疑签名的可疑密钥在没有确定所述硬件设备的任何唯一的设备标识信息的情况下对所述验证者是未知的。

12. 如权利要求 11 所述的方法，其特征在于，在验证所述硬件设备拥有密码信息之前，所述方法包括：

由所述验证者检测被泄漏的内容；

确定用于接收所述泄漏的内容的可疑直接证明签名的基数 B_0 和假名 K_0 ；以及

将所述 B_0 和假名 K_0 作为使用未知的可疑密钥 F_0 生成的可疑直接证明签名存储。

13. 如权利要求 11 所述的方法，其特征在于，验证所述硬件设备拥有密码信息包括：

从所述硬件设备接收证明以验证有一密码密钥被存储在所述硬件设备内，所述证明包括多个取幂，至少一个是在不暴露所述密码密钥的情况下使用所述密码密钥作为指数而进行的。

14. 如权利要求 11 所述的方法，其特征在于，验证所述硬件设备拥有密码信息包括：

由所述硬件设备使用所述密码密钥计算假名 K ；以及

从所述硬件设备接收所述假名 K 。

15. 如权利要求 14 所述的方法，其特征在于，验证所述密码密钥未被用于生成所述可疑签名包括：

向所述硬件设备提供签名否认请求，包括使用未知、可疑密钥 F_0 生成的可疑直接证明签名的基数 B_0 和假名 K_0 ，所述基数 B_0 和假名 K_0 具有相关联的取消标识符；以及

从所述硬件设备接收直接证明以使所述验证者确信，如果在数字签名请求期间向所述硬件设备提供的取消标识符匹配与所述可疑直接证明签名相关联的取消标识符，则用于构造所述假名 K 的所述硬件的密码密钥 F 不匹配所述可疑的被泄漏的密钥 F_0 。

16. 如权利要求 11 所述的方法，其特征在于，验证所述密码密钥未被用于生成所述可疑签名包括：

(a) 向所述硬件设备提供包括使用未知可疑密钥 F_0 形成的可疑签名的基数 B_0 和假名 K_0 的否认签名请求;

(b) 在无需标识所述硬件设备的所述密码密钥 F 的情况下, 验证所述硬件设备的密码密钥不匹配所述可疑的被泄漏的密钥 F_0 。

17. 如权利要求 16 所述的方法, 其特征在于, 验证还包括:

在无需标识关于 R 的任何有用信息的情况下, 从所述硬件设备接收存在使得下式成立的值 R 的证明:

$$S = B_0^R \bmod P \text{ 且 } T = K_0^R \bmod P;$$

在无需标识关于 F 的任何有用信息的情况下, 从所述硬件设备接收存在使得下式成立的值 F 的证明:

$$U = S^F \bmod P \text{ 且 } K = B^F \bmod P; \text{ 以及}$$

如果 $U \neq T \bmod P$, 则标识所述硬件设备的所述密码密钥为未被泄漏。

18. 如权利要求 17 所述的方法, 其特征在于, 还包括:

如果 $U = T \bmod P$, 则标识所述硬件设备的密码密钥 K 为已被泄漏的。

19. 如权利要求 16 所述的方法, 其特征在于, 还包括:

对预定数目的可疑直接证明签名重复 (a) 和 (b); 以及

如果所述预定数目超出可疑直接证明签名限值, 则对作为由所述硬件设备的证书制造商定义的平台族的成员的硬件设备重新配置密钥。

20. 如权利要求 11 所述的方法, 其特征在于, 验证所述硬件设备拥有密码信息包括:

将包括所述硬件设备的验证者的取消标识符的签名请求发送给所述硬件设备;

接收所述硬件设备的包括所述取消标识符的数字签名; 以及

根据所述硬件设备的制造商的公共密钥认证所述硬件设备的所述数字签名。

21. 一种装置, 包括:

闪存, 用于存储来自证书制造商的密码信息; 以及

可信平台模块, 用于在无需公开所述密码信息或硬件设备的任何唯一的设备标识信息的情况下, 使验证者确信所述硬件设备拥有来自证书制造商的密码信息, 并使所述的验证者确信所述密码信息未被泄漏。

22. 如权利要求 21 所述的装置, 其特征在于, 所述可信平台模块包括:

认证逻辑, 用于根据包括多个取幂的直接证明证实有一密码密钥被存储在所

述硬件设备内，所述多个取幂的至少其中之一是在没有暴露所述密码密钥的情况下使用所述密码密钥作为指数进行的。

23. 如权利要求 21 所述的装置，其特征在于，所述可信平台模块包括：

否认签名逻辑，用于接收包括来自所述验证者的可疑签名的基数值 B_0 和假名值 K_0 的否认签名请求，并使所述验证者确信存储在所述硬件设备内并用于构造假名 K 的密码密钥不匹配用于形成所述可疑签名的未知的可疑密钥 F_0 。

24. 如权利要求 21 所述的装置，其特征在于，所述可信平台模块包括：

密钥逻辑，用于从所述装置的证书制造商接收唯一的秘密对 (c, F) ，其中 F 是所述硬件设备的 $c^e \bmod P$ 形式的签名密钥，其中所述对 (e, P) 是所述证书制造商的公共密钥。

25. 如权利要求 24 所述的装置，其特征在于，所述可信平台模块包括：

用于存储所述唯一的秘密对 (c, F) 的闪存。

26. 一种系统，包括：

耦合至网络的验证者平台；以及

耦合至所述网络的证实者平台，包括：

总线，

耦合至所述总线的处理器，

耦合至所述总线的包括可信平台模块的芯片组，响应于经由所述网络接收的质询，所述可信模块在无需揭示密码信息或所述硬件设备的标识设备信息的情况下使验证者确信所述硬件设备拥有所述密码信息，并使所述验证者确信所述密码信息未被泄漏。

27. 如权利要求 26 所述的系统，其特征在于，所述芯片组包括图形控制器。

28. 如权利要求 26 所述的系统，其特征在于，所述网络包括广域网。

29. 如权利要求 26 所述的系统，其特征在于，所述可信平台模块包括：

否认签名逻辑，用于从所述验证者接收包括可疑签名的基数值 B_0 和假名值 K_0 的否认签名请求，并使所述验证者确信存储在所述硬件设备内并用于构造假名 K 的密码密钥 F 不匹配用于形成所述可疑签名的未知的可疑密钥 F_0 。

30. 如权利要求 26 所述的系统，其特征在于，所述可信平台模块包括：

密钥逻辑，用于从所述装置的证书制造商接收唯一的秘密对 (c, F) ，其中 F 是所述硬件设备的 $c^e \bmod P$ 形式的签名密钥，其中所述对 (e, P) 是所述证书制造商的公共密钥；以及

闪存，用于存储所述唯一的秘密对 (c,F)。

31. 一种包括其上存储指令的机器可读介质的制品，这些指令可用于对系统编程以执行一种方法，所述方法包括：

在没有揭示密码信息或硬件设备的任何唯一的设备标识信息的情况下，使所述验证者确信所述硬件设备拥有所述密码信息；以及
使所述验证者确信所述密码信息未被泄漏。

32. 如权利要求 31 所述的制品，其特征在于，使验证者确信硬件设备拥有密码信息包括：

使用所述密码信息来计算假名 K；以及
将所述假名 K 提供给所述验证者。

33. 如权利要求 31 所述的制品，其特征在于，使所述验证者确信所述密码密钥不匹配所述未知的被泄漏的密钥 F_0 包括：

选择随机指数值 R；

将根据从所述验证者接收的所述可疑基数值 B_0 和所述可疑假名值 K_0 、所述硬件设备的模数值 P 和所述随机指数值 R 计算得到的一个或多个值发送给所述验证者；

由所述硬件设备执行证明以否认存储在所述硬件设备内的密码密钥 F 被用于创建直接证明可疑签名，所述证明包括多个取幂，每一个是在没有暴露所述密码密钥 F、所述随机指数值 R 和其它指数值的情况下使用所述密码密钥 F、所述随机指数值 R 和所述其它指数值之一作为指数而进行的。

34. 如权利要求 33 所述的制品，其特征在于，执行所述证明包括：

在无需揭示关于 R 的任何有用信息的情况下，使所述验证者确信，存在值 R 使得：

$S = B_0^R \bmod P$ 且 $T = K_0^R \bmod P$ ；以及

在无需揭示关于 F 的任何有用信息的情况下，使所述验证者确信，存在值 F 使得：

$U = S^F \bmod P$ 且 $K = B^F \bmod P$ 。

35. 如权利要求 34 所述的制品，其特征在于，如果 $U \neq T \bmod P$ 则所述验证者确信存储在所述硬件设备内的所述密码密钥 F 未被用于创建所述可疑直接证明签名。

36. 一种包括其上存储指令的机器可读介质的制品，所述指令可用于对系统

编程以执行一种方法，所述方法包括：

在无需揭示硬件设备的任何唯一的设备标识信息的情况下，验证所述硬件设备拥有密码信息；以及

验证所述硬件设备的密码密钥未被用于生成验证者所持有的至少一个可疑签名，其中用于生成所述可疑签名的可疑密钥对所述验证者未知。

37. 如权利要求 36 所述的制品，其特征在于，验证所述硬件设备拥有密码信息包括：

从所述硬件设备接收证明以验证有密码密钥被存储在所述硬件设备内，所述证明包括多个取幂，至少一个取幂是在没有暴露所述密码密钥的情况下使用所述密码密钥作为指数而进行的。

38. 如权利要求 36 所述的制品，其特征在于，验证所述密码密钥未被用于生成所述可疑签名包括：

(a) 向所述硬件设备提供包括使用未知可疑密钥 F_0 形成的可疑直接证明签名的基数 B_0 和假名 K_0 的否认签名请求；

(b) 在无需标识所述硬件设备的所述密码密钥 F 的情况下，验证所述硬件设备的密码密钥 F 不匹配所述可疑被泄漏的密钥 F_0 。

39. 如权利要求 38 所述的制品，其特征在于，验证还包括：

在无需标识关于 R 的任何有用信息的情况下，从所述硬件设备接收存在使下式成立的值 R 的证明：

$$S = B_0^R \bmod P \text{ 且 } T = K_0^R \bmod P;$$

在无需标识关于 F 的任何有用信息的标识的情况下，从所述硬件设备接收存在使下式成立的值 F 的证明：

$$U = S^F \bmod P \text{ 且 } K = B^F \bmod P; \text{ 以及}$$

如果 $U \neq T \bmod P$ ，则将所述硬件设备的所述密码密钥标识为未被泄漏。

40. 如权利要求 39 所述的制品，其特征在于，还包括：

如果 $U = T \bmod P$ ，则将所述硬件设备的所述密码密钥 F 标识为被泄漏的。

证实否认直接证明签名的装置和方法

发明领域

本发明的一个或多个实施例一般涉及密码学领域。更具体地，本发明的一个或多个实施例涉及用于证实否认直接证明签名的方法和装置。

发明背景

对众多现代通信系统，交换的信息的可靠性和安全性是重要的问题。为解决该问题，可信计算平台联盟（TCPA）为各平台开发了安全性解决方案。根据 2002 年 2 月 22 日左右发布的名为“主规范 1.1b 版”的 TCPA 规范，每一个人计算机（PC）可使用被称为可信平台模块（TPM）的可信硬件设备实现。每一 TPM 包含唯一的背书密钥对（EK），其特征在于具有公共 EK 密钥（PUBEK）和私人 EK 密钥（PRIVEK）。TPM 一般具有由制造商签署的 PUBEK 的证书。

在操作期间，外部一方（被称为验证者）可请求对 TPM 的认证。这创造了两个对立的安全问题。首先，验证者需要确定被请求的认证信息是真正来自有效 TPM 的。其次，包含 TPM 的 PC 的所有者想要尽可能多地维护私密性。具体地，PC 的所有者想要能够在验证者不能确定认证信息来自同一 TPM 的情况下将认证信息提供给不同的验证者。

对这些安全问题所提出的一种解决方案是建立可信第三方（TTP）。例如，TPM 可创建证据标识密钥对（AIK），即公共 AIK 密钥和私人 AIK 密钥。公共 AIK 密钥可置于以 PRIVEK 签署的证书请求中，随后被发送给 TTP。PUBEK 的证书也可被发送给 TTP。一旦证书被接收之后，TTP 可检查所签署的证书请求是否有效，且如果有效，则 TTP 可向 TPM 发出证书。

一旦证书被发出之后，TPM 然后可在从验证者接收到请求时使用公共 AIK 和由 TTP 发出的证书。由于 AIK 和证书与 EK 无关，因此验证者不能获得关于 TPM 或以 TPM 实现的 PC 的身份的信息。实际上，上述方法是成问题的，因为它要求建立 TTP。标识和建立可用作 TTP 的各方被证实是主要的障碍。

提出的另一解决方案在共同待审查的 2002 年 11 月 27 日提交的美国申请第

10/306,336 号中描述，该申请也为本申请的受让人所有。所提出的解决方案利用直接证明方法，借此 TPM 可无需可信的第三方而直接证实 AIK 由有效的 TPM 创建而无需揭示 TPM 的身份。在这种解决方案中，每一 TPM 具有唯一的私人密钥。不幸地，对手可选一 TPM 并使用复杂的手段从 TPM 中提取该唯一的私人密钥。

在直接证明方法中，给出能够取消已从 TPM 移除的密钥的方法。在直接证明协议期间，TPM 获取基数 h ，计算并显示 $k=h^f \bmod n$ ，其中 n 是公共密钥的一部分，而 f 是由 TPM 持有的唯一密钥的一部分。因此，如果验证者接收到已从 TPM 移除的值 f_0 ，则验证者可通过执行计算 $k_0=h^{f_0} \bmod n$ ，并检查 $k=k_0$ 是否成立来检查直接证明是否使用该值 f_0 创建。如果 $k=k_0$ ，则直接证明是使用 f_0 创建的，而如果 k 不等于 k_0 ，则直接证明是使用某个其它的私人密钥创建的。

这种方法的一种限制在于，它需要验证者获取 f_0 的值。可以想象，对手可从 TPM 获取该秘密的唯一值，并以验证者不能获取 f_0 的值但可知道对特定的 k_0 ， f_0 的值已经从 TPM 移除的方式来利用它。在美国申请第 10/306,336 号中，为处理该问题提供了一种方法。它需要验证者为每一 TPM 提供基数 h 的值以便当与该验证者交互时使用。这具有允许验证者能够关联与该验证者的所有交互的特性。

附图简述

本发明的各实施例作为示例而非限制在附图中示出，附图中：

图 1 示出了将以根据一个实施例操作的可信平台模块（TPM）实现的平台为特征的系统。

图 2 示出了包括图 1 的 TPM 的平台的第一实施例。

图 3 示出了包括图 1 的 TMP 的平台的第二实施例。

图 4 示出了以图 2 的 TMP 实现的计算机的示例性实施例。

图 5 示出了根据一个实施例在制造期间设置 TPM 的过程的流程图。

图 6 示出了设置根据一个实施例制造的每一平台的过程的流程图。

图 7 是根据一个实施例示出用于验证在可信硬件设备内存储的密码密钥是未被泄露的方法的流程图。

图 8 是根据一个实施例示出以零知识证明来显示两个离散对数是相同的方法的流程图。

图 9 是根据一个实施例示出用于概念性示出两个离散对数相同的证明的验证的方法的流程图。

图 10 是根据一个实施例示出用于使验证者确信存储在可信硬件设备内的密码密钥是未被泄露的方法的流程图。

详细描述

描述了用于证实否认直接证明签名的方法和装置。在一个实施例中，可信硬件设备使验证者确信其拥有密码信息而不会泄漏可信硬件设备的唯一的设备标识信息或该密码信息。这是无需使用可信第三方 (TTP) 而完成的。相反，它是由“直接证明”方法完成的，该方法中 TPM 进行的计算涉及使用密码密钥作为指数的取幂。在一个实施例中，可信硬件设备向验证者证实直接证明中所使用的数字签名（“直接证明签名”）是基于未被泄露的密码密钥的。

在一个实施例中，验证者可向可信硬件设备发出否认签名请求，以证实该可信硬件设备所持有的密码密钥未被用来形成疑似已泄漏的直接证明签名(可疑直接证明签名)。对一个实施例，被配置成向验证者证实来自 TPM 的信息（例如，密码密钥、数字签名、数字证书等）是未被泄漏的 TPM 的功能被部署为固件。然而，构想到这样的功能可被部署为专用硬件或软件。形成固件或软件的指令或代码被存储在机器可读介质上。

此处，“机器可读介质”可包括但不限于，软盘、硬盘、光盘（例如，CD-ROM、DVD、mini-DVD 等）、磁光盘、诸如只读存储器 (ROM)、随机存取存储器 (RAM)、任何类型的可编程只读存储器（例如，可编程只读存储器“PROM”、可擦可编程只读存储器“EPROM”、电可擦可编程只读存储器“EEPROM”或闪存）的半导体存储器、磁卡或光卡等。构想到，由于软件可作为下载的信号的一部分或在经由通信链路的传播期间被临时存储，因此信号本身和/或通信链路可被视作机器可读介质。

在以下描述中，某些术语用来描述本发明的一个或多个实施例的某些特征。例如“平台”被定义为适于发送和接收信息的任何类型的通信设备。各种平台的示例包括但不限于或约束于，计算机、个人数字助理、蜂窝式电话、机顶盒、传真机、打印机、调制解调器、路由器等。“通信链路”被宽泛地定义为适合于平台的一个或多个信息携带介质。各种类型的通信链路的示例包括但不限于或约束于电线、光纤、电缆、总线迹线 (trace) 或无线信号发送技术。

“验证者”指的是向另一实体请求某种可靠性或权限的验证的任何实体（例如，个人、平台、系统、软件和/或设备）。正常地，这是在公开或提供所请求的

信息之前执行。“证实者”指的是被请求提供对其权限、有效性和/或身份的某种证明。“设备制造者”可与“证书制造者”互换使用，它指的是制造或配置平台或设备的任何实体（例如，可信平台模块）。

如此处所使用的，向验证者“证实”或“使之确信”证实者拥有或了解某些密码信息（例如，签名密钥、私人密钥等）意味着，基于向验证者公开的信息和证明，证实者具有该密码信息的可能性很高。向验证者对此进行证实而不向验证者“泄漏”或“公开”该密码信息意味着，基于对验证者所公开的信息，验证者计算上无法确定密码信息。这样的证明此处被称为直接证明。术语“直接证明”指的是零知识证明，如本领域中公知的那种类型的证明。

后文讨论的各个实施例的描述和说明中，系数、变量和其它符号（例如，“ h ”）全部由相同的标号或名称指示。从而，当符号在一个公式的不同部分以及不同公式或函数描述中出现时，引用的是同一符号。

I. 一般体系结构

图 1 示出了根据一个实施例的将以可信硬件设备（称之为“可信平台模块”或“TPM”）实现的平台为特征的系统 100。第一平台 102（验证者）经由网络 120 向第二平台 200（证实者）发送认证请求 106。响应于请求 106，第二平台 200 提供认证信息 108。在一个实施例中，网络 120 形成局域网或广域网和/或常规网络基础架构，诸如公司的内联网、因特网或其它类似的网络的一部分。

此外，为加强安全性，第一平台 102 可能需要验证证实者平台 200 是由所选的一个或一组设备制造商（后文中称之为“设备制造商 110”）制造的。在一个实施例中，第一平台 102 质询第二平台 200 要求它示出其具有由设备制造商 110 生成的密码信息（例如，私人签名密钥）。第二平台 200 通过以回复的方式提供认证信息来回复该质询以使第一平台 102 确信第二平台 200 具有由设备制造商 110 生成的密码信息而不揭示该密码信息或任何唯一的设备/平台标识信息。

图 2 是进一步示出使验证者确信平台 200 拥有未被泄漏的密码信息而无需公开该密码信息或任何唯一的设备标识信息的包含 TPM 220 的平台 200 的框图。代表性地，计算机系统 200 包括用于在处理器（CPU）202 和芯片组 210 之间传输信息的处理器系统总线（前侧总线（FSB））204。如此处所使用的，术语“芯片组”以统指耦合至 CPU202 以执行期望的系统功能的各个设备的方式使用。

代表性地，图形块 218、硬盘驱动器设备（HDD）214 和主存储器 212 可被耦

合至芯片组 210。在一个实施例中，芯片组 210 被配置成包括存储器控制器和/或与 I/O 设备 216 (216-1,...216-N) 通信的输入/输出 (I/O) 控制器。在替换实施例中，芯片组 210 被配置成或可被配置成包含图形块 218，并作为图形存储器控制器集线器 (GMCH) 操作。在一个实施例中，主存储器 212 可包括但不限于，随机存取存储器 (RAM)、动态 RAM (DRAM)、静态 RAM (SRAM)、同步 DRAM (SDRAM)、双倍数据速率 (DDR) SDRAM (DDR-SDRAM)、Rambus DRAM (RDRAM) 或能够支持数据的高速缓冲的任何设备。

图 3 还根据一个实施例示出了第二平台 200 的可信平台模块 (TPM) 220。TPM 220 是由设备制造商 110 制造的密码设备。在一个实施例中，TPM 220 包括含有封装在包装内的少量芯片内存储器的处理器单元 222。在一个实施例中，所封装的存储器可用于存储从证书制造商接收的密码密钥 230。TPM 220 被配置成向第一平台 102 提供认证信息，这可使其确定该认证信息是从有效 TPM 发送的。所使用的认证信息非唯一的数据，这使得 TPM 或第二平台的身份很有可能被确定，它在此处被称为“唯一的设备标识信息”。

在一个实施例中，TPM 220 还包括非易失性存储器 224 (例如，闪存) 来允许存储密码信息，诸如：密钥、散列值、签名、证书等中的一个或多个。在一个实施例中，密码信息是从证书制造商接收的密码密钥。如以下所示，“X”的散列值可被表示为“Hash (X)”。当然，构想到这样的信息可被存储在平台 200 的外部存储器 280 内以代替闪存 224。密码信息可被加密，尤其当存储在 TPM 200 之外时。

在一个实施例中，TPM 220 包括响应来自验证者平台的认证请求的认证逻辑 240。在一个实施例中，认证逻辑 240 使验证者平台确信或向其证实 TPM 220 已经存储了由证书设备制造商生成的密码信息，而无需揭示该密码信息或任何唯一的设备/平台标识信息。结果，认证逻辑 240 在保护证实者平台的身份的同时执行所请求的认证。参考图 4 进一步示出了认证逻辑 240。

如图所示，直接证明逻辑 250 被配置成参与将在以下详细描述的直接证明，以使验证者确信证实者平台包含来自证书制造商的密码信息，而无需揭示该密码信息。如下所述，密钥逻辑 270 执行 TPM 220 的平台设置，以接收唯一、秘密的私人对 (c, F)，其中 F 是私人签名密钥， $F = c^e \bmod n$ ，其中 e 、 n 是 TMP 220 的证书制造商的公共密钥。

如将在以下详细描述，如由直接证明逻辑 250 所执行，否认签名逻辑 260 提供下述附加的功能，以使验证者平台确信或向其证实该设备所持有的私人签名密钥

在直接证明期间未被用于生成可疑签名（可疑直接签名证明）。可以理解，某些实现可能需要比上述更少或更好配置的计算机。从而，取决于众多因素，诸如价格约束、性能要求、技术改进和/或其它情况，平台 200 的配置随实现而变化。

II. 平台设置

“平台族”可由设备制造商定义来包括一种或多种平台或设备。例如，平台族可以是含有相同安全性相关信息的所有平台（成员）的集合。该安全性相关信息可包含 TCPA 模型中的 EK 或 AIK 证书中所包括的信息中的某些。它也可包括特定平台或设备的制造商或型号编号。对每一平台族，设备制造商创建该制造商为该平台族使用的密码参数。如图 5-6 中所示，设备制造商创建它用于签署它所制造的设备（例如，平台 200 或 TPM 220）的秘密的签名密钥。

图 5 是根据一个实施例示出形成平台族证书 (PFC) 的方法 400 的流程图。在一个实施例中，设备制造商利用公共密钥密码函数（例如，Rivest、Shamir and Adelman (RSA) 函数）来以公共模数 n 、公共指数 e 和私人指数 d 创建 RSA 公共/私人密钥对（框 402）。公共密钥是基于值 e 、 n 的，而私人密钥是基于 d 、 n 的。这可使用公知方法创建，如 Bruce Schneier 编写的由 John Wiley & Sons 出版的 Applied Cryptography 第二版 (1996)，ISBN: 0471117099 中所述的那些。在一个实施例中，应选择足够大的模数 n ，使得在无法在计算上分解出 n 。

设备制造商指定参数 Z ，它是零 (0) 与 n 之间的整数（框 404）。设备制造商指定安全参数 W ，它是零 (0) 与 n 之间的整数（框 406）。然而，选取过小或过大的 W 可导致安全故障。在本发明的一个实施例中，选择接近于 2^{160} 的 W 。推荐选择在 2^{80} 到 n 的平方根之间的 W 。在本发明的一个实施例中，设备制造商计算质数 P ，使得 $P=u*n+1$ （框 408）。可使用能使 P 为质数的 u 的任何值；然而，为了保持可接受等级的安全性，值 P 应足够大，使得计算离散对数 “mod P ” 在计算上不可行。

在一个实施例中，设备制造商的直接证明公共密钥由密码参数 e 、 n 、 u 、 P 、 Z 、 W 构成。这些参数可由验证者使用来验证由设备创建的直接证明签名。设备制造商生成包括密码参数 e 、 n 、 u 、 P 、 Z 、 W 、平台族的安全性相关信息以及设备制造商名字的平台族证书（框 410）。在一个实施例中，参数 u 和 P 不会都被包括，因为给定 n 和这两个参数之一，另一个可通过 $P=u*n+1$ 计算出。在一个实施例中，设备制造商对若干不同的平台族使用相同的密码参数 e 、 n 、 u 、 P 、 W ，而仅对不

同的平台变化值 Z。在这种情况下，Z 的值可被选择为相差大约或至少 4W，尽管所选差是一种设计选择。

一旦生成了平台族证书之后，设备制造商向它所制造的属于该特定平台族的平台或设备提供该平台族证书（框 412）。与平台族证书相关联的密码参数从证实者（例如，图 1 中的第二平台 200）到验证者的分发可按照各种方式实现。然而，这些密码参数应以使验证者确信该平台族证书由该设备制造商生成的方式向验证者分发。

例如，一种公认的方法是将参数直接分发给验证者。另一种公认的方法是分发由证书权威机构签署的平台族证书，作为一个示例，证书管理机构可以是设备制造商。在后一方法中，证书权威机构的公共密钥应分发给验证者，经签署的平台族证书可给予该平台族中的每一平台成员（证实者平台）。证实者平台然后可向验证者提供经签署的平台族证书。

图 6 是示出由如图 4 中所示的密钥逻辑 270 对根据一个实施例制造的证实者平台执行的建立的方法 500 的流程图。证实者平台的 TPM 选择随机数 F，使得 $0 < F - Z < W$ （框 502）。TPM 可在将其发送给证书制造商签署之前隐蔽该随机数 F（框 504）。该隐蔽操作被执行来使证书制造商不能了解随机数 F 的确切内容。在一个实施例中，TPM 选择随机值 B，其中 $1 < B < n-1$ （框 506），并计算 $A = B^e \bmod n$ （框 508）。然后，TPM 计算 $F' = F * A \bmod n$ （框 510）。如果 TPM 没有隐蔽 F，则 TPM 使用 $F' = F$ 和 $A' = 1$ （框 512）。

当执行这些计算之后，TPM 将 F' 发送给证书制造商（框 514）。证书制造商计算 $c' = F'^d \bmod n$ （框 516），并将 c' 提供给证实者（框 518）。证实者的 TPM 计算 $c = c' * B^{-1} \bmod n$ （框 520）。注意到，这暗示 $c = F^d \bmod n$ 。值 c 和 F 随后被存储在 TPM 或证实者内的外部存储中（框 522）。如此处所述，F 被称为 TPM 的签名密钥，而秘密对 c, F 被称为密码信息，此处也被称为“成员密钥”。如此处所使用的，F 可被称为“假名指数”。

在共同待审的 2003 年 9 月 30 日提交的美国申请第 10/675,165 号中描述了 TPM 执行直接证明以使验证者确信硬件设备拥有来自证书制造商的密码信息的操作。在直接证明方案中，直接证明中所使用的证实者的签名（“直接证明签名”）使用平台制造商（发行方）的公共密钥来确认。因此，所有的成员可使用相同的公共密钥来确认其签名。可证实，由成员创建的直接证明签名不标识是哪一个成员创建了该直接证明签名。

为向验证者证实 TPM 包括唯一的秘密对，TPM 可获取 B 的值以根据随机基数选择用作基数。例如，TPM 可响应于签名请求计算 $k=B^F \bmod N$ ，并向验证者给出 B、k。从而，如此处所述，值 k 被称为直接证明签名的“假名”，B 被称为直接证明签名的“基数”。TPM 然后构造一无需泄漏关于 F 和 c 的任何额外信息而证实 TPM 拥有使得 $F=c^e \bmod n$ 且 $k=B^F \bmod P$ 的 F、c 的直接证明签名。构造直接证明签名的方法在共同待审查的美国申请第 10/306,336 中给出，该申请也由本申请的受让人所有。TPM 每次创建新的直接证明签名时可使用不同的 B 值，以使得根据随机基数选择，验证者不能了解它们从同一 TPM 接收证明。

再次参考图 4，在一个实施例中，TPM 220 包括对否认签名逻辑 260 以处理取消成员密钥。成员密钥被保存在硬件中，但密钥有可能被移除。在这种情况下，验证者可取消任何被移除的密钥，并停止接受使用被取消（未知可疑）密钥生成的直接证明签名。作为签名过程的一部分，成员选择随机基数 B 和证书成员的公共密钥（e,n）来计算 $k=B^F \bmod P$ 。B 和 k 的值作为签名的一部分被揭示。证实了如果使用了随机基数，则给定两个不同的签名，确定这两个签名是使用同一假名指数 F 还是使用不同的假名指数 F' 来创建的在计算上不可行。

然而，如果对手已经从某些硬件设备（例如，F1、F2、F3）中移除了秘密的假名指数 F'，且如果验证者具有这些假名指数，则验证者可通过检查 $K=B^{F1} \bmod P$ 或 $B^{F2} \bmod P$ 或 $B^{F3} \bmod P$ 是否成立来判断给定的签名是否使用这些假名指数之一创建。这对其中验证者具有从硬件设备移除的秘密 F' 的情况可行。但对其中验证者怀疑成员密钥被从硬件设备中移除但它没有该成员密钥尤其是指数 F 的情况不可行。

为了给予验证者取消它怀疑已被泄漏的成员密钥的能力，直接证明方法支持指定基数选择。在一个实施例中，根据指定基数选择，验证者可提供基数 B，在一个实施例中基数 B 是从验证者的名字获得的。成员可在直接证明签名中使用该基数 B 来代替挑选随机的 B。只要验证者使用同一基数，则验证者可判断向其发送的两个签名是否使用了同一假名指数 F，因为两个签名将产生相同的假名 $B^F \bmod P$ 。

因此，如果使用指定基数选择的验证者接收到直接证明签名，并怀疑用来创建该签名的成员密钥已被泄漏，则只要验证者使用同一指定的基数，它即能够拒绝该成员密钥的其它签名。然而，验证者有效使用指定基数选择的仅有方式是长时间使用同一指定基数。这从私密性角度出发不甚理想，因为它使得验证者能够将由一

成员执行的所有事务与该验证者所指定的基数关联。

图 7 是根据本发明的一个实施例，示出由验证者平台执行的用于证实存储在 TPM 内的密码密钥未被泄漏的方法 500 的流程图。代表性地，在处理框 510 处，验证者平台确定它是否察觉到使用未知的可疑密钥生成的可疑直接证明签名。假定验证者平台察觉到使用未知可疑密钥生成的某些可疑直接证明签名。令 B_0 为基数， K_0 为从可疑直接证明签名之一中接收的假名。在一个实施例中，验证者平台对每一可疑直接证明签名重复下述过程。

在所述实施例中，验证者平台不包含已用于计算 $K_0 = B_0^{F_0} \bmod P$ 的可疑密钥 F_0 的副本。从而，在处理框 520 处，验证者平台发送使用未知的可疑密钥 F_0 生成的可疑直接证明签名的基数 B_0 和假名 K_0 。作为响应，验证者平台将从证实者平台接收使用 B_0 和 K_0 计算出的一个或多个值。

在一个实施例中，如参考处理框 540-560 所示地形成对存储在证实者平台内的密码密钥的确认。证实者平台将生成随机值 R 。在一个实施例中，随机值 R 被选中在某个指定的区间中，诸如 0 到 W 的区间。在处理框 540 处，验证者平台从证实者平台接收值 S 和 T 以及存在使下式成立的值 R 的证明：

$$S = B_0^R \bmod P \text{ 且 } T = K_0^R \bmod P. \quad (\text{公式 1})$$

在一个实施例中，所接收的对值 R 的存在性的证明是零知识证明的形式。证实两对 (S, B_0) 和 (T, K_0) 具有相同的离散对数的这样的零知识证明的一个实施例在图 8 中给出。在处理框 550 处，验证者平台接收存在使下式成立的值 F 的证明：

$$U = S^F \bmod P \text{ 且 } K = B^F \bmod P. \quad (\text{公式 2})$$

再一次，对值 F 的存在性的证明可使用零知识证明进行。用于证实两对 (U, S) 和 (K, B) 具有相同的离散对数的这样的零知识证明的一个实施例在图 8 中给出。

从而，一旦使验证者平台确信值 R 和 F 的存在性之后，在一个实施例中，验证者平台检查 U 和 T 的值。如果 $U = T \bmod P$ ，则验证者知道证实者平台密钥 F 等于该未知的可疑密钥 F_0 。如果：

$$U \neq T \bmod P \quad (\text{公式 3})$$

则验证者知道证实者平台密钥 F 不等于该未知的可疑密钥 F_0 。这很容易看出，因为 $B_0^{RF} = S^F = U \bmod P$ 且 $B_0^{RF_0} = K_0^R = T \bmod P$ 。因此，当且仅当 $F = F_0 \bmod n$ 时， $U = T \bmod P$ 。

如果 $U \neq T \bmod P$ ，则证实者平台密钥 F 不等于该未知的可疑密钥 F_0 。从而，在处理框 570 处，验证者接收对证实者签名密钥 F 被用于生成可疑直接证明签名

的否认，此处被称为“证实对直接证明签名的否认”。否则， $U=T \bmod P$ ，则验证者平台接收到证实者平台为该直接证明签名的确使用了泄漏的密钥 F0 的确认。

在一个实施例中，证实者平台通过使用标准零知识证明否认证实者的签名密钥 F 被用于形成该可疑的直接证明签名。如此处所述，如下提供用于证实两对具有相同的离散对数的标准零知识证明。具体地，给定一组整数 k_1, h_1, k_2, h_2 和模数 P，零知识证明将证实存在 e 使得 $k_1 = h_1^f \bmod k_2$ ，且 $h_2^f = W^e \bmod P$ ，而无需揭示关于 f 的任何信息。

示出两个离散对数相同的零知识证明的一个实施例在共同待审查的美国申请第 10/306,336 中给出，该申请也由本申请的受让人所有。图 8 是示出该零知识证明的流程图 600。假定 f 位于 Z 到 Z+W 的区间中。（Z 可以是 0，如以上公式 1 的情况中。）令 $B=W*2^{Sp+HASH_Length}$ ，其中 Sp 是安全性参数，HASH_Length 是散列函数 HASH 的输出中的位长。在一个实施例中，选择了足够大的 Sp，例如 Sp=60，使得以下计算出的 s 的值不揭示关于 f 的有用信息。

在处理框 610 处，TPM 随机选择位于区间[0,B]中的值 t。TPM 然后可在处理框 620 处，计算 $j_1=h_1^t \bmod P$ 和 $j_2=h_2^t \bmod P$ 。TPM 然后可在处理框 630 处计算 $r=HASH(h_1, k_1, h_2, k_2, j_1, j_2)$ 。在处理框 640 处，TPM 可计算 $s=Z+t-f*r$ 。最后，在处理框 650 处，TPM 可将 s、 h_1 、 k_1 、 h_2 、 k_2 、 j_1 、 j_2 发送给验证者。根据一个实施例，验证者然后可验证该证明。

图 9 是根据一个实施例，概念性示出对两个离散对数相同的证明的验证的流程图 700。在处理框 710 处，质询者可计算 $r=HASH(h_1, k_1, h_2, k_2, j_1, j_2)$ 。质询者然后可在处理框 720 处检查 $j_1*h_1^z=k_1^r*h_1^s \bmod P$ 和 $j_2*h_2^z=k_2^r*h_2^s \bmod P$ 。如果通过了处理框 720 的检查，则质询者可在处理框 730 处接受该证明。

图 10 是示出证实者平台响应于密钥确认请求的接收而执行的方法 600 的流程图。如此处所使用的，验证者平台一旦确信存储在硬件设备内的密码密钥的存在性之后，即可验证所存储的密码密钥是否未被泄漏。根据一个实施例，如参考图 2 和 3 所示，这样的功能由 TPM 220 的认证逻辑 240 的密钥确认逻辑 260 提供。代表性地，在处理框 810 处，证实者平台确定是否接收到否认签名请求。一旦接收到，则执行处理框 620-670 的功能。

在处理框 820 处，验证者平台接收到在对未知的可疑密钥 F0 的证明中接收的可疑签名（可疑直接证明签名）的基数 B0 和假名 K0。在处理框 830 处，证实者平台将计算所得的值 $S=B_0^R \bmod P$ 、 $T=K_0^R \bmod P$ 、 $U=B_0^{RF} \bmod P$ 和 $K=B^F \bmod$

P发送给验证者。在处理框840处，证实者向验证者平台发送存在值R使得 $S=B_0^R \bmod P$ 且 $T=K_0^R \bmod P$ 的证明。在处理框850处，证实者平台向验证者平台发送直接证明以使验证者平台确信存在F使得 $U=S^F \bmod P$ 且 $K=B^F \bmod P$ 。

如上所述，在一个实施例中，如图8中所述地根据零知识证明进行证明。也如上所述，假定公式(3)为真，则在处理框860处，证实者密钥F不等于未知的可疑密钥 F_0 ，并执行处理框870。在处理框870处，证实者将否认该可疑直接证明签名是使用该证实者平台的签名密钥F生成的。否则，如果公式(3)为假，则证实者密钥F等于未知的可疑密钥 F_0 。结果，证实者平台将不能证实对可疑直接证明签名的否认。从而，验证者平台不能认证证实者平台，因为证实者平台正使用被泄漏的密钥。

从而，一个实施例向上述指定基数选择提供了增强的安全性能力。然而，在一个实施例中，验证者平台被禁止向证实者平台提交之前接收的所有签名。即，通过向证实者平台提交之前接收的所有签名，可要求之前提交过签名的证实者平台标识相应的签名。结果，验证者平台可能将来自证实者平台的所有之前的签名关联在一起。在一个实施例中，提供了若干方法来防止由此处的一个或多个实施例描述的取消能力的滥用。

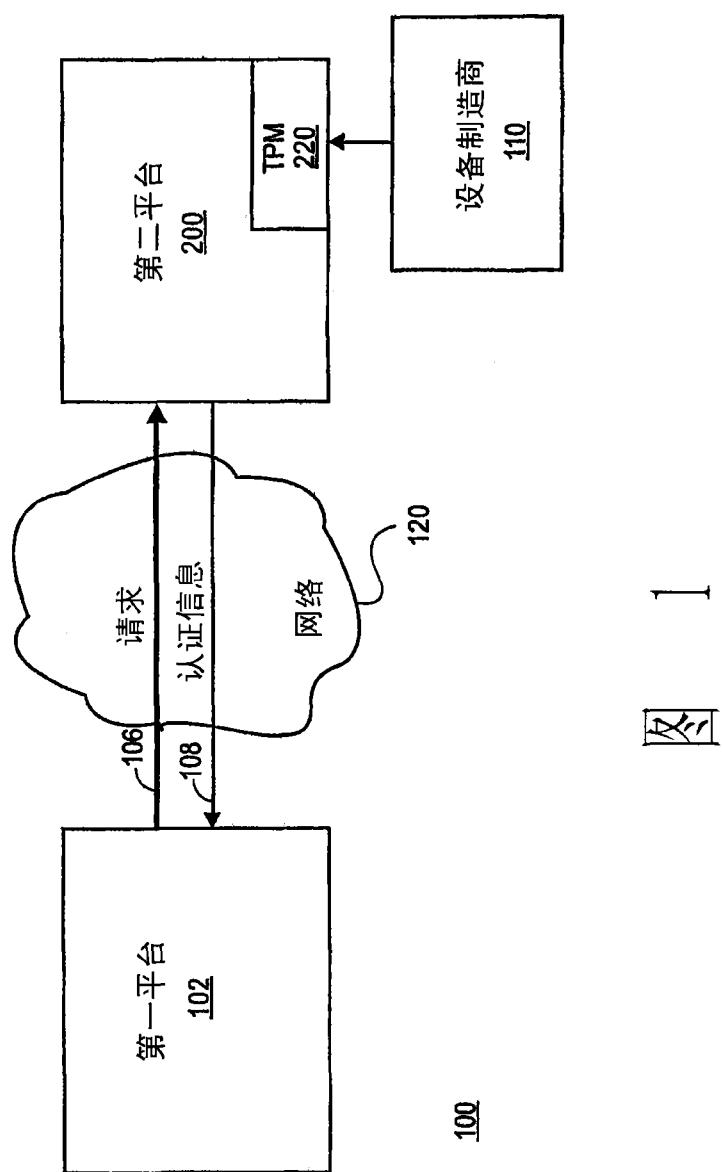
在一个实施例中，证实者平台配备限制验证者可提出供否认的签名的数目的内嵌的能力。这是合理的方法，因为非常小比例的设备将被泄密并使其密钥被移除。然而，如果多于该限制的设备被泄密，则在一个实施例中，设备可被重新配置密钥。仅当设备证实它不是被泄密的设备时，才可被重新配置密钥。另一种方法是在设备内置入取消权威机构的一个或多个公共密钥（公共密钥的散列）。从而，如果否认请求由这些取消权威机构之一批准，则验证平台可给出对签名的否认。该批准可通过使取消权威机构签署否认请求，尤其是签署 (B_0, K_0) 对来指示。

在替换方法中，当验证者请求签名时，他给出取消标识符。在一个实施例中，当向一成员给出取消标识符时，证实者平台将限制对包括相同的取消标识符在内的请求的签名否认。取消标识符可由B值的低位指示，例如低40位。验证者可指示B的这些低位，证实者可使用B的这些低位，并随机选择B其余的位。证实者然后可仅提供对其中 B_0 匹配这些低位的签名的否认。以此方式，验证者平台可被置于群中，其中如果两个验证者使用相同的取消标识符则它们位于同一群中。在一群内，验证者可告诉其它验证者拒绝一成员密钥，但它们不能告诉该群以外的验证者来拒绝该成员密钥。在一个实施例中，该方法也可包括对发出的否认签名请求的数

目的限制。

之前的应用也可包括直接证明的非交互式方法。此外，已发现用于执行直接证明的其它方法。这些方法之一由 Brickell、Boneh、Chen 和 Shacham 提供，它被称为组签名（set signatures）。另一方法由 Brickell、Camenisch 和 Chen 提供，它被称为直接匿名证据。所有这些方法共享了存在随机基数选择使得在签名的创建或交互式证明中，成员在某一有限群，诸如对某个整数 Q 的以 Q 为模的整数内创建假名 $k=B^f$ 的特性。因此，本发明中所述的用于证实否认签名的方法也可应用于这些签名或交互式方法中的任何一个。

公开了示例性实施例和最佳模式，可在保持处于如以下权利要求书定义的本发明的实施例的范围内的同时对所公开的实施例进行修改和变化。



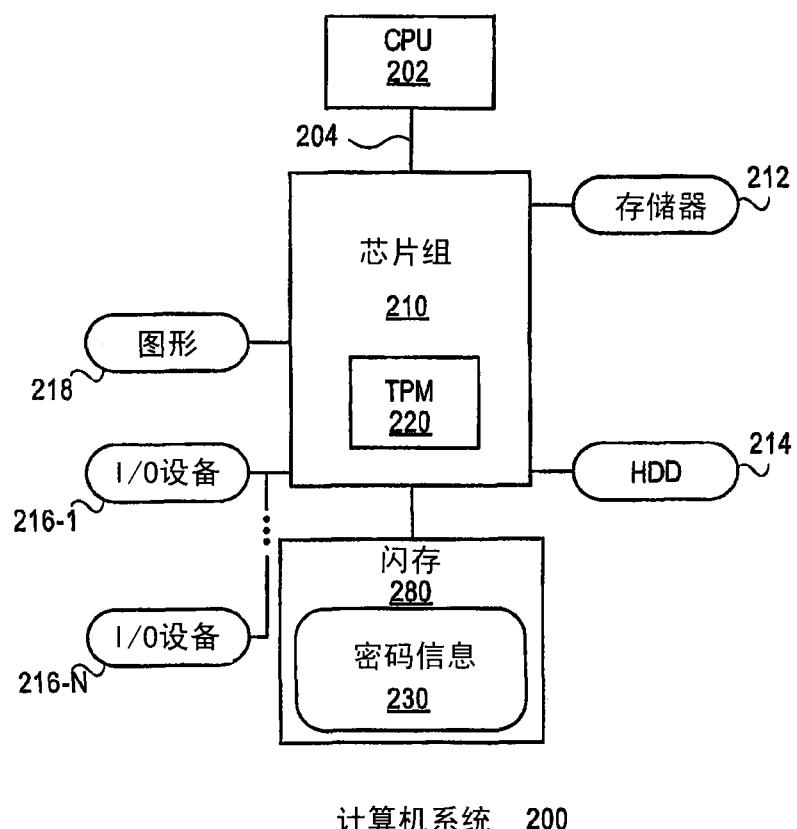


图 2

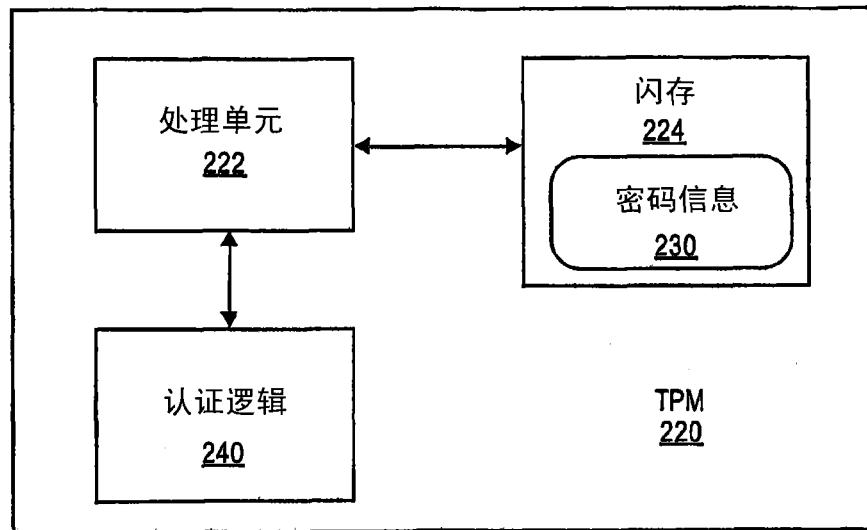


图 3

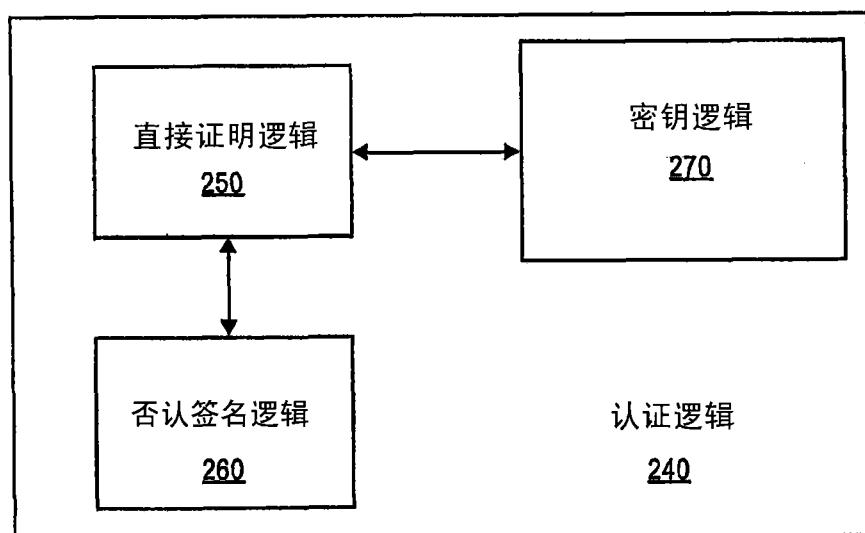


图 4

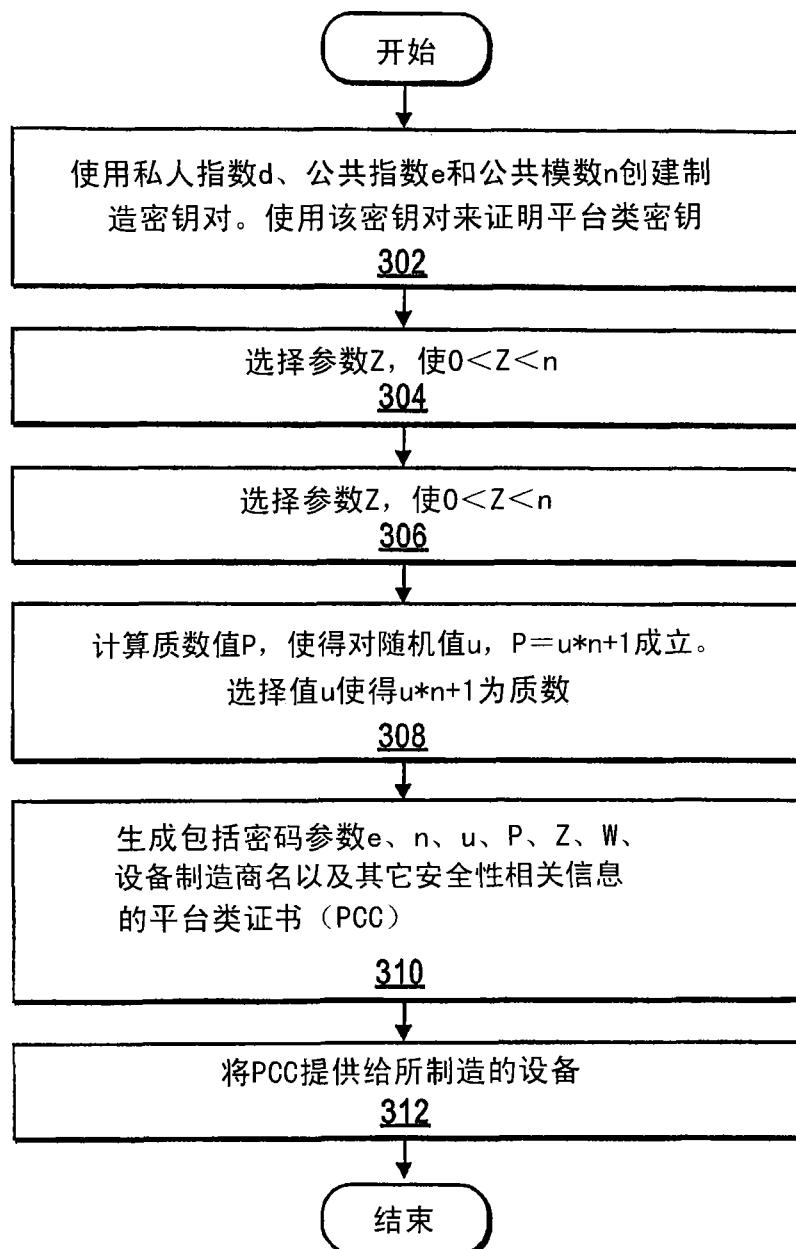


图 5

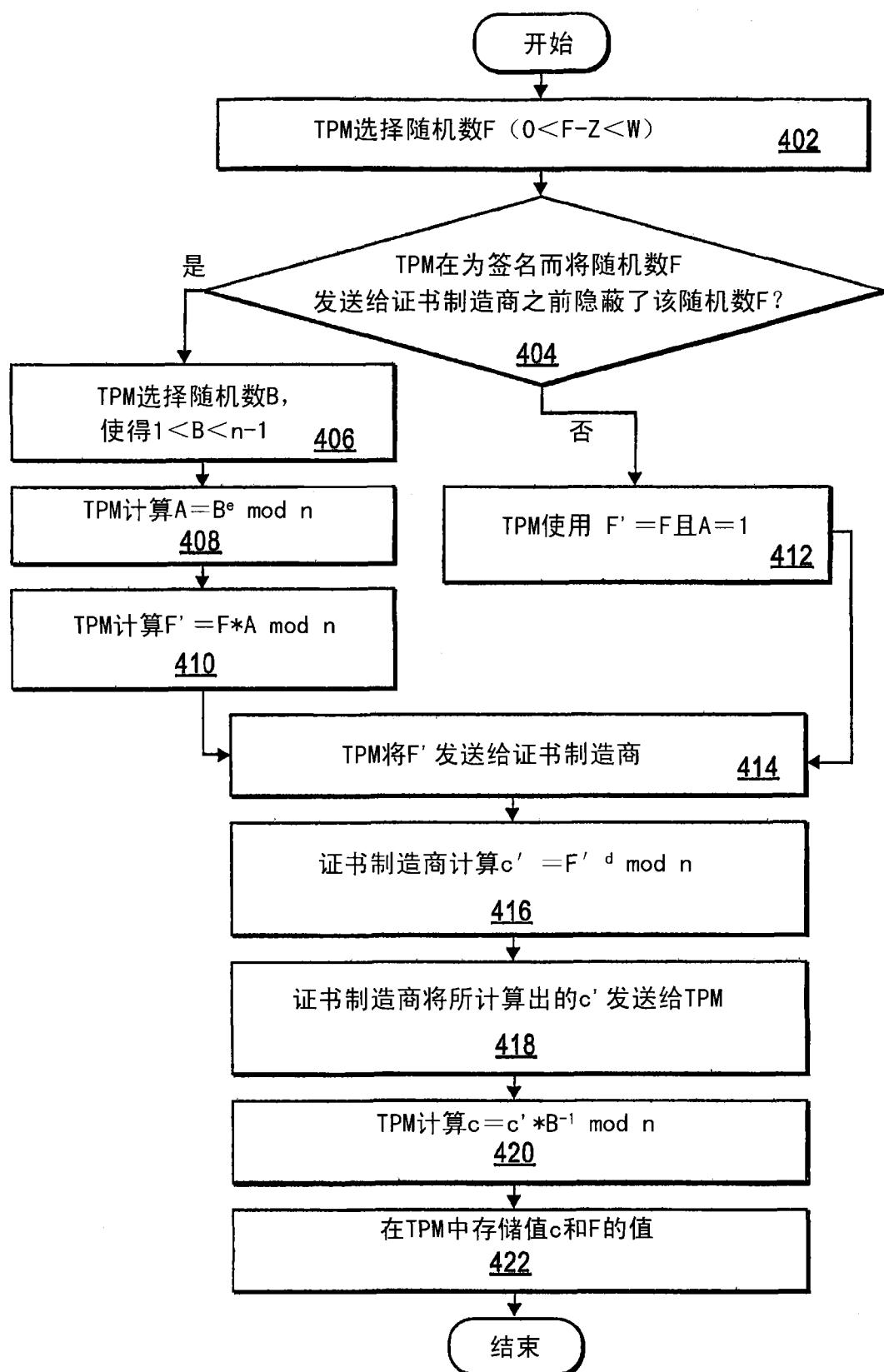


图 6

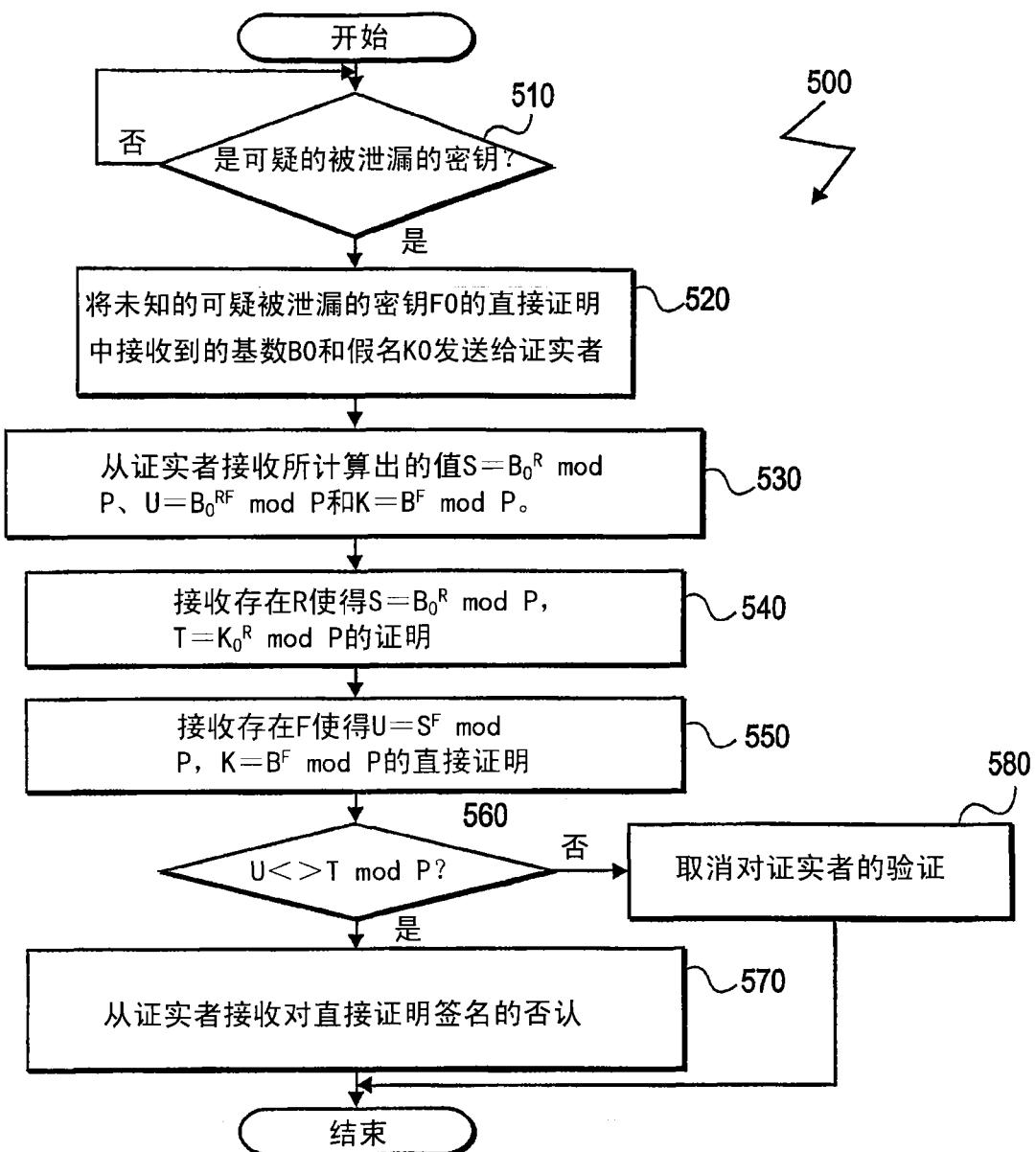


图 7

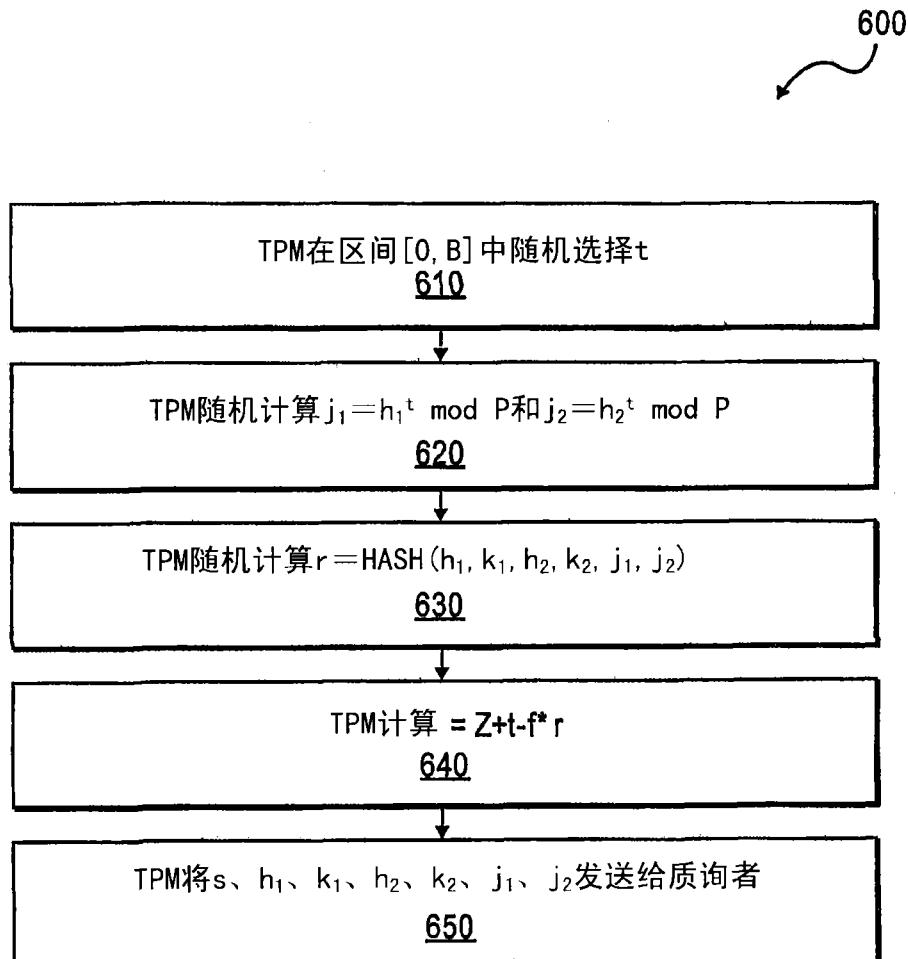


图 8

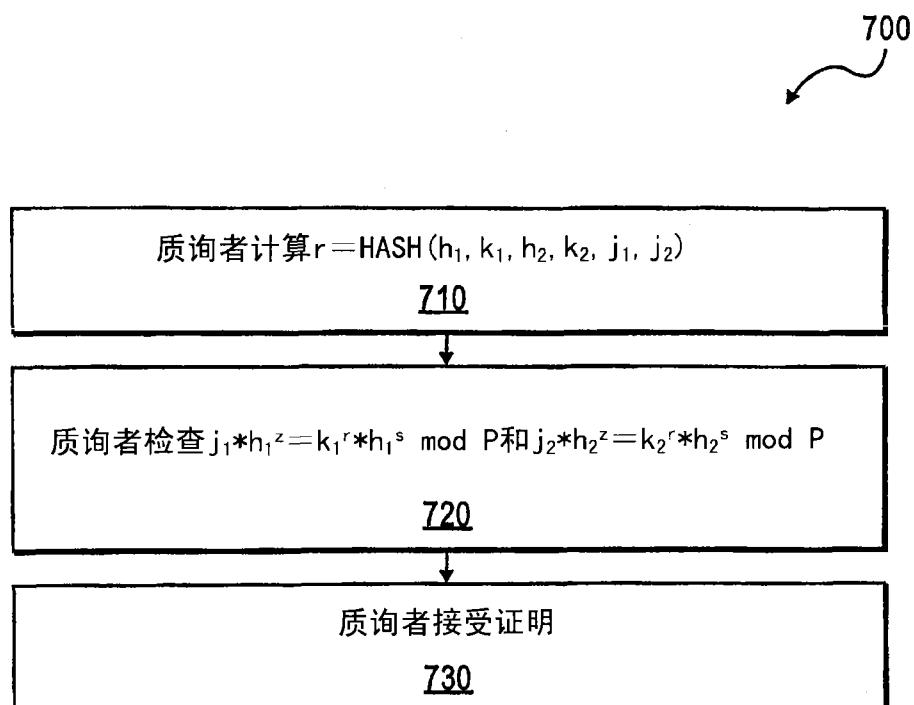


图 9

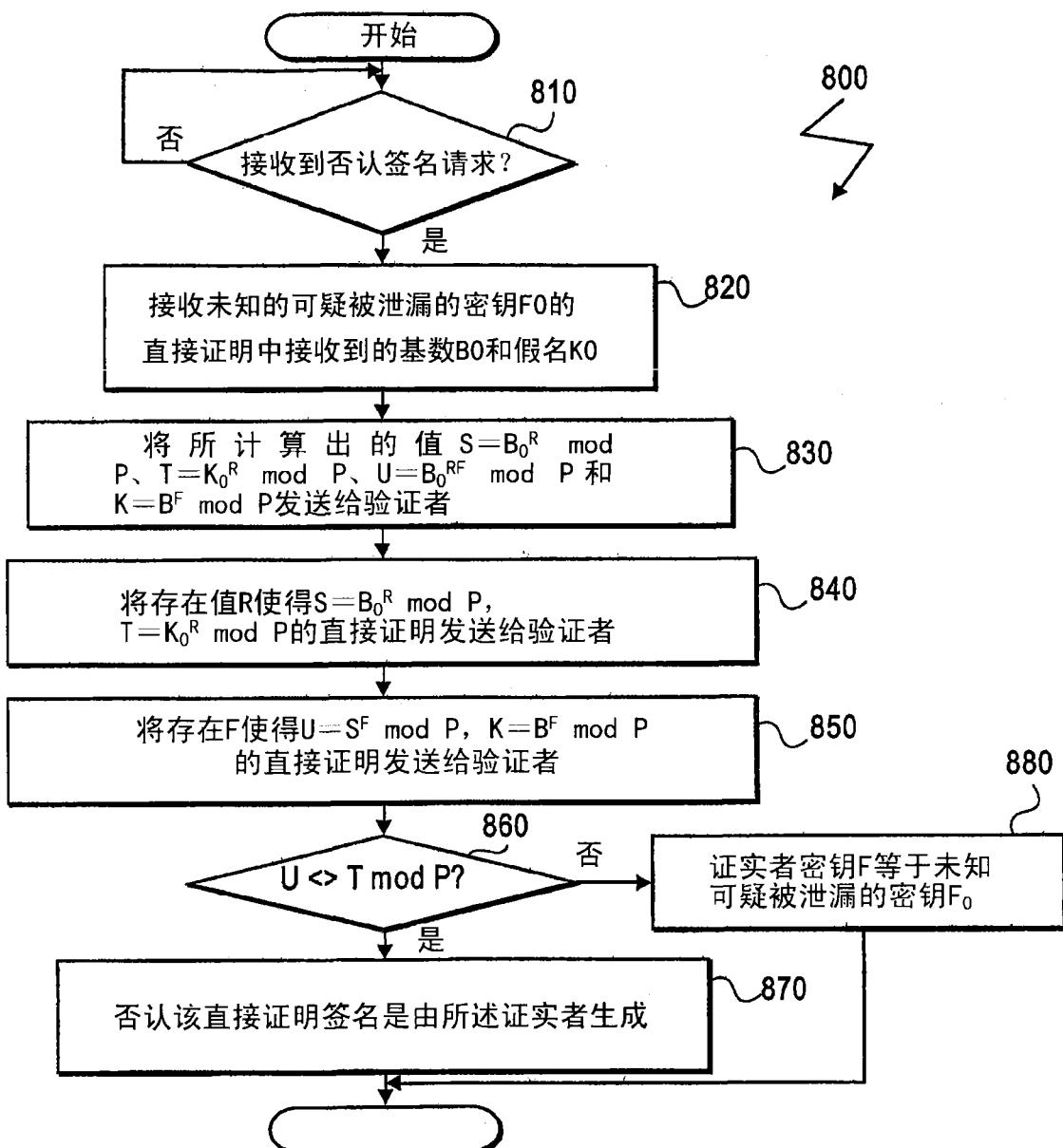


图 10