[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 1/00 (2006.01)

[12] 发明专利说明书

专利号 ZL 200480029960.5

[45] 授权公告日 2008 年 5 月 14 日

[11] 授权公告号 CN 100388154C

[22] 申请日 2004.8.20
[21] 申请号 200480029960.5
[30] 优先权
[32] 2003.10.17 [33] EP [31] 03405749.7
[32] 2004. 3.24 [33] EP [31] 04405181.1
[86] 国际申请 PCT/IB2004/002716 2004.8.20
[87] 国际公布 WO2005/038635 英 2005.4.28
[85] 进入国家阶段日期 2006.4.12
[73] 专利权人 国际商业机器公司
地址 美国纽约
[72] 发明人 J·卡梅尼施
[56] 参考文献
CN1399490A 2003.2.26
US5633929A 1997.5.27
WO0201794A2 2002.1.3
US5604805A 1997.2.18
WO0242935A2 2002.5.30
审查员 李 楠
[74] 专利代理机构 北京市中咨律师事务所
代理人 于 静 张亚非

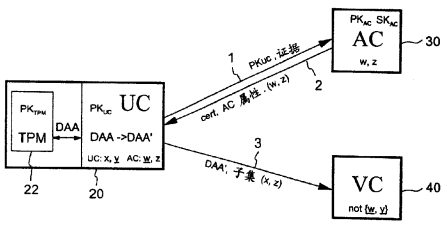
权利要求书 3 页 说明书 13 页 附图 2 页

[54] 发明名称

用于具有属性的用户证明签名的方法和系统

[57] 摘要

本发明公开了一种用于生成和验证用户证明签名值(DAA')并颁发用于生成该用户证明签名值(DAA')的证明值(cert)的方法。 此外，本发明涉及一种用于使用用户证明签名值(DAA')的系统，该用户证明签名值(DAA')对应于至少一个属性(A，B，C，D)，每个该属性具有属性值(w，x，y，z)，零个、一个或多个属性值(x，y)对于事务保持匿名，该系统包括：具有安全模块(22)的用户设备(20)，该安全模块提供模块公钥(PK_{TPM})和安全模块证明值(DAA)，该用户设备(20)提供用户公钥(PK_{UC})和证据值，该用户公钥(PK_{UC})内在地包括零个、一个或多个用户确定的属性值(x，y)，该证据值表明用户公钥(PK_{UC})有效地得自安全模块(22)的模块公钥(PK_{TPM})；证明者计算机(30)，其提供零个、一个或多个证明者确定的属性值(w，z)和证明值(cert)，该证明值基于证明者秘密密钥(SK_{AC})、用户公钥(PK_{UC})和匿名属性值(w，z)；以及验证计算机(40)，用于验证(i)用户证明签名值(DAA')是否有效地得自安全模块(22)提供的安全模块证明值(DAA)和证明值(cert)，以及(ii)证明值(cert)是否与至少一个属性的子集(B，D)相关联，该子集(B，D)内的每个属性具有显露的属性值(x，z)。



1. 一种用于生成与验证计算机（40）一起使用的用户证明签名值的方法，该用户证明签名值对应于至少一个属性，每个该属性具有属性值，一个或多个验证者隐藏属性值在可被具有安全模块（22）的用户设备（20）与该验证计算机（40）执行的事务中保持匿名，该方法包括以下步骤：

提供用户公钥和表明该用户公钥有效地得自该安全模块的模块公钥的证据值；

从证明者计算机（30）接收到

（I）具有至少一个具有其属性值的属性的证明值，一个或多个用户确定的属性值对于该证明者计算机（30）保持未知，

该证明值得自证明者秘密密钥、用户公钥和一个或多个证明者确定的属性值，

该用户公钥内在地包括一个或多个用户确定的属性值，以及

（II）至少一个证明者确定的属性值；以及

从该证明值和安全模块（22）提供的安全模块证明值得到该用户证明签名值的一部分，

其中可验证（i）该用户证明签名值的一部分是否有效地得自该安全模块证明值和该证明值，以及（ii）该证明值是否与至少一个属性的子集相关联，该子集内的每个属性具有显露的属性值。

2. 根据权利要求 1 的方法，还包括以下步骤：

从所述安全模块（22）接收第一安全模块证明值；

从该第一安全模块证明值得到中间用户证明签名值；

使用该中间用户证明签名值、证明值、证明者公钥和验证者隐藏属性值利用散列函数生成第二签名值；

将该第二签名值提供给该安全模块（22）；

从该安全模块（22）接收用户证明签名值的一部分；以及

由所述用户设备使用一个或多个所述验证者隐藏属性值，被接收到的所述用户证明签名值的一部分，用户公钥和证明者公钥，来计算该用户证明签名值的另外的部分。

3. 根据权利要求 1 或 2 的方法，其中，通过使用所述证明者公钥和所述一个或多个用户确定的属性值从所述模块公钥得到所述用户公钥。

4. 一种用于颁发证明值以便生成对应于至少一个属性的用户证明签名值的方法，每个该属性具有属性值，一个或多个验证者隐藏属性值对于可被具有安全模块（22）的用户设备（20）与验证计算机执行的事务保持匿名，该方法包括以下步骤：

从该用户设备（20）接收到用户公钥和证据值，该用户公钥内在地包括对证明者计算机（30）不可见的一个或多个用户确定的属性值，该证据值表明该用户公钥有效地得自该安全模块（22）的模块公钥；

基于证明者秘密密钥、该接收到的用户公钥和一个或多个证明者确定的属性值颁发该证明值；以及

将该证明值提供给该用户设备（20），

其中该用户证明签名值的一部分可由该用户设备（20）从该证明值和该安全模块（22）提供的安全模块证明值得到，并且可由验证计算机验证（i）该用户证明签名值的一部分是否有效地得自该安全模块证明值和该证明值，以及（ii）该证明值是否与至少一个属性的子集相关联，该子集内的每个属性具有显露的属性值。

5. 一种用于验证从证明值生成的用户证明签名值的方法，该用户证明签名值对应于至少一个属性，每个该属性具有属性值，一个或多个验证者隐藏属性值对于可被具有安全模块（22）的用户设备（20）执行的事务保持匿名，该方法包括以下步骤：

从用户设备（20）接收到该用户证明签名值；以及

验证（i）该用户证明签名值的一部分是否有效地得自该安全模块（22）提供的安全模块证明值和一证明值，以及（ii）该证明值是否与至少一个属性的子集相关联，该子集内的每个属性具有显露的属性值，

其中该证明值得自证明者秘密密钥、用户公钥和保持匿名的至少一个证明者确定的属性值，

该用户公钥内在地包括用户确定的属性值。

6. 根据权利要求5的方法，其中，所述验证步骤还包括：

通过使用所述用户证明签名值、证明者公钥和显露的属性值计算第一用户证明签名验证值；以及

检查该第一用户证明签名验证值是否等于该用户证明签名值内包含的值。

7. 一种用于使用用户证明签名值的系统，该用户证明签名值对应于至少一个属性，每个该属性具有属性值，一个或多个用户确定的属性值对于事务保持匿名，该系统包括：

具有安全模块（22）的用户设备（20），该安全模块提供模块公钥和安全模块证明值，该用户设备（20）提供用户公钥和证据值，该用户公钥内在地包括一个或多个用户确定的属性值，该证据值表明该用户公钥有效地得自该安全模块（22）的模块公钥；

证明者计算机（30），该证明者计算机提供一个或多个证明者确定的属性值和证明值，该证明值基于证明者秘密密钥、该用户公钥和一个或多个证明者确定的属性值；以及

验证计算机（40），该验证计算机用于验证（i）该用户证明签名值的一部分是否有效地得自该安全模块（22）提供的安全模块证明值和该证明值，以及（ii）该证明值是否与至少一个属性的子集相关联，该子集内的每个属性具有显露的属性值。

用于具有属性的用户证明签名的方法和系统

技术领域

本发明涉及一种用于生成和验证用户证明签名（attestation-signature）值并颁发用于生成用户证明签名值的证明值的方法。另外，本发明涉及用于使用用户证明签名值的系统。此外，本发明还涉及用于执行该方法的计算机程序单元以及用于使计算机执行该方法的存储在计算机可用介质上的计算机程序产品。

背景技术

计算机已发展成用于许多应用和服务的工具。在当今世界里，越来越需要可信赖的计算环境。需要综合的信任、安全和私密功能以在内容提供者、应用和服务提供者、消费者、企业和金融机构尤其是用户可依赖的设备之间建立多方信任。

为此，已建立可信平台模块（TPM）。该模块的作用是提供受保护的存储、平台认证、受保护的加密过程和可证明状态能力以为计算平台提供一信任等级。此信任的基础是公认的管理机构作出的平台对于预期用途可信的认证。所谓的可信计算机组（TCG）为在多个平台包括个人计算机、服务器、PDA 和数字电话之间的可信计算硬件构件块和软件接口开发和促进开放工业标准规范。这将使能进行更安全的数据存储、在线业务实践和在线商业交易，同时保护私密和个人权利。用户将具有更安全的本地数据存储和更低的来自外部软件攻击和物理盗窃两者的身份盗窃的风险。

为了实现可证明状态的功能，发布者向下文也被简称为 TPM 的可信平台模块发布证书以便允许 TPM 以后远程证明其是真正的 TPM，并因此验证方可具有由 TPM 声明和证明的置信度。为了允许 TPM 证明其是真正

的而无需验证方能够识别 TPM，可信计算机组已规定了所谓的直接匿名证明（direct anonymous attestation）（DAA）协议。该协议允许 TPM 使验证方确信其已获得发布者的证明而无需显露其身份。

此外，TCG 规定了 DAA 颁发协议以向平台的 TPM 提供证明（具有证书），以便平台可以后向任何当事方证明其保存有证明，而验证方不会识别该平台或将此证明证据与该平台提供的其他证明证据相联系。

但是，直接匿名证明过程不允许包括平台可在证实其得到证明时以匿名方式使用或示出给验证者的谓词或属性。

从上文可见，本领域中仍需要改进的允许具有在事务内保持匿名的被认证/证明的属性或属性值的证明的协议和系统。

词汇表

下文给出一些非正式的定义以帮助理解说明书。

属性－具有各自属性值 w、x、y、z 的 A、B、C、D

x，y－证明者（attester）隐藏属性值，或用户确定的属性值

w，z－证明者显露属性值、证明者确定的属性值，或匿名属性值

w，y－验证者隐藏属性值

x，z－验证者显露属性值、显露的属性值或非匿名属性值

TPM－可信平台模块

PK_{UC}－用户公钥

PK_{AC}－具有值 n，g，g'，h，S，Z，R_0，R_1，Γ，γ，ρ 的证明者公钥

PK'_{AC}－修改的证明者公钥

SK_{AC}－证明者秘密密钥

cert－证明值

cert'－用户值

DAA'－用户证明签名值

DAA－安全模块证明值，或用户证明签名值的一部分

f_0，f_1，v'－TPM 秘密值

a－证明值 *cert* 的第一部分，或第一证明值

c，$sf0$，$sf1$，sv，sx，sy－证据值，其中 sx，sy 是扩充的证据值

c－证据值的一部分

c'－第二证据验证值

C'－第二签名值，或中间用户证明签名值

c_h－中间证据值

e－证明值 *cert* 的第二部分，是随机素数

G'－第一用户证明签名验证值

G，$sf0'$，$sf1'$，sv'－安全模块证明值 DAA 的一部分

sy'，sw'，se'，seu'－用户证明签名值 DAA'的一部分

T_1－用户证明签名值 DAA'的一部分

T'_1－第一签名值，或第一安全模块证明值

T''_1－中间用户证明签名值

T'''_1－中间用户证明签名验证值

U－安全模块的公钥 PK_{TPM} 的一部分

U'－中间证据值

U''－第一证据验证值

U'''－中间证书值

v－秘密签名值，其中 $v=v'+v''$

v''－证明值 *cert* 的第三部分，是随机整数

W－第一中间用户证据值

W'－第二中间用户证据值

发明内容

下文提出了一种允许具有在事务内保持匿名的被认证/证明的属性或属性值的证明的系统和方法。通常，证明可包括可以后匿名示出的谓词。就是说，证明可包括平台或其用户的一些特性或属性。在用户的具有可信

平台模块的用户计算机、证明者或证明者计算机例如私密认证管理机构、和通常是验证计算机的验证者或验证方之间执行事务。如所指出的，用户设备具有在此也被称为可信平台模块（TPM）的安全模块，并且它们被共同称为平台，其允许平台认证、被保护的加密过程以及可证明状态能力。当 TPM 匿名证实其得到证明时，每个特性或属性可被示出或隐藏。例如，平台具有证明可表示它是某公司的有效平台例如膝上型电脑、PDA、移动设备等。然后，可使用属性来编码该公司的特定分支或站点。当证实其具有得到的证明时，可准许该平台访问某些资源例如该公司的 LAN（经由无线接入点或公共因特网）。然后，可使用特性/属性来例如告知它是本地用户或来自其他部门的客人。

证明内包含的属性或特性可由用户、证明者或他们一起确定。

另一种选择是将平台的一些特性/属性存储在 TPM 内，并然后使 TPM 将以临时秘密密钥签名的它们发送的验证者，TPM 用匿名证明协议对该秘密密钥的公钥签名。这些特性/属性可在制造期间被写入 TPM 并此后不会再改变。很明显，这允许仅处理 TPM 支持的特性/属性且不允许改变它们，这相当不灵活。但是，在提出的系统和方法中，特性/属性的数量和种类没有被 TPM 约束，特性/属性可被改变，并且特性/属性可被任何人即也被与制造者不同的实体认证。

每个特性或属性具有特性或属性值。下文为了简单起见，仅使用属性和属性值。

根据本发明，提供了一种用于使用用户证明签名值 DAA'的系统，该用户证明签名值对应于至少一个具有属性值（w，x，y，z）的属性（A，B，C，D），零个、一个或多个属性值（x，y）对于事务和在事务内保持匿名。该系统包括具有提供模块公钥 PK_{TPM} 和安全模块证明值 DAA 的安全模块的用户设备。该用户设备提供用户公钥 PK_{UC}，该用户公钥内在地包含用户确定的属性值（x，y）和表明用户公钥 PK_{UC} 有效地得自安全模块的模块公钥 PK_{TPM} 的证据值。系统还包括提供证明者确定的属性值（w，z）和证明值 *cert* 的证明者计算机，该证明值基于证明者秘密密钥 SK_{AC}、用户

公钥 PK_{UC} 和通常证明者确定的属性值（w，z）。系统还包括用于验证以下各项的验证计算机：（i）用户证明签名值 DAA'是否有效地得自安全模块 22 提供的安全模块证明值 DAA 和证明值 *cert*，以及（ii）证明值 *cert* 是否与至少一个属性的子集（B，D）相关联，该子集（B，D）内的每个属性具有显露的属性值（x，z）。

根据本发明的另一个方面，提供了一种用于生成与验证计算机一起使用的用户证明签名值 DAA'的方法，该用户证明签名值 DAA'对应于至少一个属性（A，B，C，D），每个该属性具有属性值（w，x，y，z），零个、一个或多个属性值（w，y）在可被具有安全模块的用户设备与验证计算机执行的事务内保持匿名。该方法包括以下步骤：

提供用户公钥 PK_{UC} 和表明用户公钥 PK_{UC} 有效地得自安全模块的模块公钥 PK_{TPM} 的证据值；

从证明者计算机接收

（I）具有至少一个具有其属性值（w，x，y，z）的属性（A，B，C，D）的证明值 *cert*，零个、一个或多个属性值（x，y）对于该证明者计算机保持未知，

该证明值 *cert* 得自证明者秘密密钥 SK_{AC}、用户公钥 PK_{UC} 和零个、一个或多个证明者确定的属性值（w，z），

用户公钥 PK_{UC} 内在地包括零个、一个或多个用户确定的属性值 x，y，以及

（II）至少一个证明者确定的属性值（w，z）；以及

从证明值 *cert* 和该安全模块提供的安全模块证明值 DAA 得到用户证明签名值 DAA'，

其中可验证（i）用户证明签名值 DAA'是否有效地得自安全模块证明值 DAA 和证明值 *cert*，以及（ii）证明值 *cert* 是否与至少一个属性的子集（B，D）相关联，该子集（B，D）内的每个属性具有显露的属性值（x，z）。

所述得到用户证明签名值 DAA'的步骤还可包括以下步骤：从安全模

块接收第一安全模块证明值 T'_1；使用证明者公钥 PK_{AC} 和散列函数从第一安全模块证明值 T'_1 得到中间用户证明签名值 C'；将中间用户证明签名值 C'提供给安全模块；从安全模块接收用户证明签名值 DAA'的一部分；以及由用户设备使用零个、一个或多个属性值（w，y），被接收到的用户证明签名值 DAA'的部分，用户公钥 PK_{UC} 和证明者公钥 PK_{AC}，来计算用户证明签名值 DAA'的另外的部分，所述属性值（w，y）被编码在证明值 *cert* 内而没有显露给验证者，并因此还被称为验证者隐藏属性值（w，y）的。这确保了这些属性对于验证计算机保持是未知的。

可通过使用证明者公钥 PK_{AC} 和一个或多个属性值（x，y）从模块公钥 PK_{TPM} 得到用户公钥 PK_{UC}。通过这样做，确认了这些证明者隐藏属性值（x，y）保持对于证明者即证明者计算机是未知的。

用户设备可利用可信第三方的公钥提供对于验证计算机保持是未知的一个或多个验证者隐藏属性值（w，y）即用户确定的属性值 w，y 的加密。这允许可信第三方以后恢复验证者隐藏属性值（w，y）。

根据本发明的另一个方面，提供了一种用于颁发证明值 *cert* 以便生成对应于至少一个属性（A，B，C，D）的用户证明签名值 DAA'的方法，每个该属性具有属性值（w，x，y，z），零个、一个或多个属性值（w，y）对于可被具有安全模块的用户设备与验证计算机执行的事务保持匿名。该方法包括以下步骤：从用户设备接收用户公钥 PK_{UC} 和证据值，该用户公钥 PK_{UC} 内在地包括对证明者计算机不可见的零个、一个或多个用户确定的属性值 x，y，该证据值表明用户公钥 PK_{UC} 有效地得自安全模块的模块公钥 PK_{TPM}；基于证明者秘密密钥 SK_{AC}、接收到的用户公钥 PK_{UC} 和零个、一个或多个证明者确定的属性值（w，z）颁发该证明值 *cert*；以及将该证明值 *cert* 提供给用户设备，其中用户证明签名值 DAA'可被用户设备从证明值 *cert* 和安全模块提供的安全模块证明值 DAA 得到，并且可验证（i）用户证明签名值 DAA'是否有效地得自安全模块证明值 DAA 和证明值 *cert*，以及（ii）证明值 *cert* 是否与至少一个属性的子集（B，D）相关联，该子集（B，D）内的每个属性具有显露的属性值（x，z）。

根据本发明的另一个方面，提供了一种用于验证从证明值 *cert* 生成的用户证明签名值 DAA'的方法，该用户证明签名值 DAA'对应于至少一个属性（A，B，C，D），每个该属性具有属性值（w，x，y，z），零个、一个或多个属性值（w，y）对于可被具有安全模块的用户设备与验证计算机执行的事务保持匿名。该方法包括以下步骤：从用户设备接收到用户证明签名值 DAA'；并验证（i）用户证明签名值 DAA'是否有效地得自安全模块提供的安全模块证明值 DAA 和证明值 *cert*，以及（ii）证明值 *cert* 是否与至少一个属性的子集（B，D）相关联，该子集（B，D）内的每个属性具有显露的属性值（x，z），证明值 *cert* 得自证明者秘密密钥 SK_{AC}、用户公钥 PK_{UC} 和保持匿名的证明者确定的属性值（w，z），该用户公钥 PK_{UC} 内在地包括用户确定的属性值（x，y）即证明者隐藏属性值。

所述验证步骤还可包括通过使用用户证明签名值 DAA'、证明者公钥 PK_{AC} 和显露的属性值（x，z）计算第一用户证明签名验证值 G'；以及检查该第一用户证明签名验证值 G'是否被包含在用户证明签名值 DAA'内。

附图说明

下面参照以下附图，并仅作为示例，详细说明本发明的优选实施例。

图 1 示出具有证明者计算机（AC）、具有可信平台模块（TPM）的用户计算机（UC）、和验证计算机（VC）的情景的示意图。

图 2 示出在可信平台模块（TPM）、用户计算机（UC）和证明者计算机（AC）之间的示意流。

图 3 示出在可信平台模块（TPM）、用户计算机（UC）和验证者即验证计算机（AC）之间的用于生成和验证用户证明签名值 DAA'的示意流。

附图仅是为说明目的提供的。

具体实施方式

在参照附图说明本发明的实施例之前，讨论证明方案的一些一般问题。

直接匿名证明协议涉及颁发者或证明者、可信平台模块（TPM）、具

有 TPM 的主机平台（主机），和一些验证者。TPM 的所有通信经由其主机执行。颁发者或证明者以这样的方式向主机和 TPM 一起颁发证明，即

- 在证实已获得证明时，主机仅能在涉及 TPM 时这样做

- 证实对证明的占有可匿名（或用假名）进行，即从而验证者不能将两个不同的证据相联系（或者不能将对不同验证者的证据相联系）。

因此，证明方案包括四个过程:

“密钥生成”，其允许颁发者生成证明方案的公钥和秘密密钥;

“连接协议”，其在主机/TPM 和颁发者之间运行，并且允许主机/TPM 得到证明;

“签名过程”，其在主机和 TPM 之间运行，允许它们匿名地证实他们得到了证明，同时认证一消息，此证实过程的结果是可发送给验证者的签名；以及

“验证过程”，其允许验证者检查平台是否得到证明以及此平台是否认证了给定的消息。

证明可包括一些属性，由此每个属性可被示出或被隐藏。属性可由用户、由证明者或由它们共同确定。当证实已得到包括属性的证明之后，用户可选择可将哪些属性显露给用户而哪些属性不应显露。

下面的附图和说明示出可如何应用用户证明签名值。

图 1 示出具有还被标记为 AC 的证明者计算机 30、分别被标记为 UC 和 TPM 的包括安全模块 22 的用户设备 20、和被标记为 VC 的验证计算机 40。代表主机平台（主机）或简称平台的用户设备 20 连接到证明者计算机 30 和验证计算机 40 即验证者，该证明者计算机在此还被称为颁发者或证明者。该系统允许使用用户证明签名值 DAA’，该签名值对应于具有属性值 w，x，y，z 的属性 A，B，C，D。系统被设计成使得在与验证计算机 40 的事务中验证者隐藏属性值 w，y 保持匿名。

除了也被称为匿名属性值的验证者隐藏属性值 w，y 之外，属性值被命名如下:

x，y－证明者隐藏属性值，或用户确定属性值，因为它们是由用户确

定的；w，z－证明者显露的属性值，或证明者确定属性值，因为它们是由证明者确定的；x，z－验证者显露的属性值，显露的属性值，或非匿名属性值。

TPM 即安全模块 22 提供了模块公钥 PK_{TPM}，而用户设备 20 还提供用户公钥 PK_{UC}，该用户公钥内在地包括用户确定属性值 x，y，和显示用户公钥 PK_{UC} 有效地得自安全模块 22 的模块公钥 PK_{TPM} 的证据值。安全模块 22 还提供安全模块证明值 DAA，该值是用户证明签名值 DAA'的一部分。

证明者计算机 30 提供证明者公钥 PK_{AC}，并具有证明者秘密密钥 SK_{AC}。此外，证明者计算机 30 提供证明者确定的属性值 w，z 和证明值 *cert*，该证明值基于证明者秘密密钥 SK_{AC}、用户公钥 PK_{UC} 和证明者确定的属性值 w，z。

验证计算机 40 可验证（i）用户证明签名值 DAA'是否有效地得自安全模块 22 提供的安全模块证明值 DAA 和证明值 *cert*，以及（ii）证明值 *cert* 是否与具有显露的属性值 x，z 的属性 B，D 的子集相关联。

在操作中，如附图中的箭头 1 指示并被标记为“PK_{UC}，证据”，用户设备 20 将内在地包括用户确定属性值 x，y 和证据值的用户公钥 PK_{UC} 发送给证明者计算机 30。反过来，如箭头 2 指示并被标记为“*cert*，AC 属性（w，z）”，证明者计算机 30 发送回证明值 *cert* 和证明者确定属性值 w，z。然后如箭头 3 指示并被标记为“DAA'，子集（x，y）”，用户设备 20 可将用户证明签名值 DAA'和这里包含显露的或非匿名的属性值 x，z 的属性的子集发送给验证计算机 40，该验证计算机然后可启动验证过程。

图 2 示出可信平台或安全模块 22、用户计算机 20 和证明者计算机 30 之间的示意流，其分别由标记为“PK_{UC}，证据”和“*cert*，AC 属性（w，z）”的箭头 1 和 2 指示。首先，在步骤 101，安全模块 22 由修改的证明者公钥 PK'_{AC} 生成模块公钥 PK_{TPM} 和 TPM 秘密值 f_0，f_1，v'。在步骤 102，用户设备 102 将模块公钥 PK_{TPM} 与证明者公钥 PK_{AC} 和属性 B，C 的用户确定属性值 x，y 一起使用，以便生成内在地包含用户确定属性值 x，y 的用户公钥 $PK^{\bullet}_{UC}$ 和由“证据”指示的证据值，所述证据值表明用户公钥 PK_{UC}

有效地得自安全模块 22 的模块公钥 PK_{TPM}。如下文将详细说明的，证据包括证据值 *c*，*sf0*，*sf1*，*sv*，*sx*，*sy*。然后在步骤 103，证明者计算机 30 利用“PK_{UC}，证据”、证明者秘密密钥 SK_{AC} 和证明者确定属性值 w，z 生成证明值 *cert*。然后，如图 1 中的箭头 2 指示，将属性值 *cert* 和证明者确定属性值 w，z 一起提供给用户计算机 20，在步骤 104 内，用户计算机 20 生成用户值 *cert'*。然后在步骤 105 内，安全模块 22 使用此用户值 *cert'* 生成秘密签名值 *v*。

图 3 示出如图 1 中的被标记为“DAA'，子集（x，y）”的箭头 3 指示的用于在安全模块 22 即 TPM、也被称为平台 20 的用户计算机 20 和证明者计算机 30 之间生成和验证用户证明签名值 DAA'的示意流。在步骤 201，安全模块 22 从修改的证明者公钥 PK'_{AC}、一些 TPM 秘密值 f_0，f_1 和秘密签名值 *v* 生成第一签名值 T'_1，该第一签名值也被称为第一安全模块证明值。当平台 20 接收到该第一签名值 T'_1 时，从该第一签名值 T'_1 计算或得到中间用户证明签名值 T''_1。然后在步骤 202，平台 20 使用该中间用户证明签名值 T''_1 以及证明值 *cert*、证明者公钥 PK_{AC} 和验证者隐藏属性值 w，y，以利用散列函数生成第二签名值 *C'*，该第二签名值也被称为中间用户证明签名值。在步骤 203，安全模块 22 使用此第二签名值 *C'* 和 TPM 秘密值 f_0，f_1，*v'*，以生成安全模块证明值 DAA。然后在步骤 204，平台 20 能够从该安全模块证明值 DAA 以及证明值 *cert*、证明者公钥 PK_{AC}、用户公钥 PK_{UC} 和验证者隐藏属性值 w，y 得到用户证明签名值 DAA'。

当用户计算机 20 将用户证明签名值 DAA'提供给验证计算机 40 时，该验证者然后可使用证明者公钥 PK_{AC} 和显露的属性值 x，z，来验证用户证明签名值 DAA'是否有效地得自安全模块证明值 DAA 和一证明值 *cert*，以及该证明值 *cert* 是否与具有显露的属性值 x，z 的属性的子集 B，D 相关联。如验证步骤 205 的输出箭头所示，其输出“成功”或“不成功”，即验证有效或无效。

更具体的，下文被称为证明者的证明者计算机 30 的通常包括值（*n*，*g*，*g'*，*h*，*S*，*Z*，R_0，R_1，Γ，γ，ρ）的公钥扩增基值 R_2，…，R_k。这些

基值 R_2，...，R_k 中的每一个对应于一特定的属性 A，B，C，D，例如 A 对应于 R_2，B 对应于 R_3，C 对应于 R_4，以及 D 对应于 R_5。在下文中仅使用了 R_2，...，R_k，但是，将该描述一般化以使用任何数量的这样的基值是直接了当的。

为了从证明者得到证明值 *cert*，下文被称为平台的用户计算机 20 从下文被称为 TPM 的安全模块 22 接收值 *U*，并计算

$$U' = U \cdot R_2^{x} \cdot R_3^{y} \bmod n$$

并将此值发送给证明者。值 *U* 也被称为安全模块的公钥 PK_{TPM} 的部分，而计算出的 *U'*也被称为和用作中间证据值。

在此假设平台使前两个属性对证明者隐藏，但是应指出，可使用属性的任何子集。此外，平台从 TPM 接收到至少第一中间用户证据值 *W*，平台从该值计算出第二中间用户证据值

$$W' = W \cdot R_2^{r2} \cdot R_3^{r3}$$

其中 *r2* 和 *r3* 是随机选择的整数。应指出，*W'*的计算应对应于 *U'*的计算，就是说，在 *U'*的计算中出现的每个基值 R_i 应在 *W'*的计算中出现并带有随机指数 *ri*。然后，平台在中间证据值 c_h 的计算中使用 *W'*而不是 *W* 作为散列函数的输入，并将 c_h 发送给 TPM。TPM 将以另外的证据值 *c*、*sf0*、*sf1* 和 *sv* 作为响应。平台用值 $sx = r2 + c \cdot x$ 以及 $sy = r3 + c \cdot y$ 来扩增这些另外的证据值，并将这些扩增的证据值发送给证明者。证明者通过计算第一证据验证值

$$U'' = U'^{c} \cdot S^{sv} \cdot R_0^{sf0} \cdot R_1^{f2y} \cdot R_2^{sx} \cdot R_3^{sy} \bmod n,$$

使用 *U''*作为散列函数的输入以得到第二证据验证值 *c'*，并验证 *c'*是否等于扩增的证据值内包含的值 *c*，来验证这些证据值。如果这些验证成功，则证明者计算中间证书值

$$U''' = U' \cdot R_4^{w} \cdot R_5^{z} \bmod n$$

其中 *w* 和 *z* 是证明者确定的属性值，选择合适大小的随机素数 *e* 和随机整数 *v''*，并计算第一证明值

$$a = (Z/(U''' \cdot S^{v''}))^{1/e} \bmod n。$$

类似于平台确定的属性值，证明者可以选择不同的属性值。如果证明者使用一个也被平台使用的基值 R_i，则将由平台和证明者共同确定对应的属性。在此不对该问题进行进一步讨论。证明者将证明值部分 a，e，v'' 与证明者确定的属性值 w，z 一起发送给平台。

当平台希望向知道属性值 x 和 z 的验证者即验证计算机 40 证实证明时，它以如下方式进行：它首先选择随机整数 u，并计算

$$T_1 = a \cdot h^u \bmod n$$

并将 T_1 作为用户证明签名值 DAA'的一部分发送给下文被称为验证者的验证计算机 40。然后，它从 TPM 接收到第一签名值 T'_1，并计算中间用户证明签名值

$$T''_1 = T'_1 \cdot a^{re} \cdot H^{reu} \cdot R_3^{t3} \cdot R_4^{t4} \bmod n$$

其中，re、reu、$t3$ 和 $t4$ 是随机整数，而 R_3 和 R_4 是对应于保持匿名即对验证者隐藏的属性的基值。如果平台希望隐藏其他属性值，则它应在计算 T''_1 时使用对应的基而不是 R_3 和 R_4（以及对应的随机整数指数而不是 $t3$ 和 $t4$）。然后，如图 3 内的步骤 202 所示，平台使用 T''_1 和一些其他的值作为散列函数的输入以得到第二签名值 C'。平台将 C' 发送给 TPM，并接收包括值 G，$sf0'$，$sf1'$，sv' 的安全模块证明值 DAA。平台利用至少值 $sy' = t3 + G \cdot y$，$sw' = t4 + G \cdot w$，$se' = re + G \cdot e$ 和 $seu' = reu + G \cdot e \cdot u$ 扩增这些安全模块证明，并将得到的值列表作为用户证明签名值 DAA'发送给验证者。

验证这样的被接收的用户证明签名值 DAA'包括由验证者计算中间用户证明签名验证值

$$T'''_1 = (T'_1/(R_2^x \cdot R_5^z))^G \cdot S^{sv'} \cdot R_0^{sf0'} \cdot R_1^{sf1'} \cdot T_1^{se'+GL} \cdot h^{-seu'} \cdot R_3^{sy'} \cdot R_4^{sw'} \bmod n$$

其中 L 是安全参数，并使用 T'''_1 作为散列函数的输入来得到第一用户证明签名验证值 G'，并验证 G' 是否等于用户证明签名值 DAA'内包含的值 G。由于 G 是安全模块证明值 DAA 的一部分，而该安全模块证明值 DAA 是用户证明签名值 DAA'的一部分，所以它也是用户证明签名值 DAA'的一部分。

任何公开的实施例可与所示和/或所述的其他实施例中的一个或几个组合。实施例的一个或多个特征也可能组合。

本发明可在硬件、软件或硬件和软件的组合内实现。任何类型的计算机系统或适于执行文中公开的方法的其他装置都适用。硬件和软件的典型组合可以是具有这样的计算机程序的通用计算机，该计算机程序在被加载和执行时控制该计算机系统使得该计算机系统执行文中公开的方法。本发明还可包含在这样的计算机程序产品内，该计算机程序产品包含使能够实现文中公开的方法的所有特征，并且在加载到计算机内时能够执行这些方法。

计算机程序装置或计算机程序在本上下文内是指这样的一组指令的以任何语言、代码或符号表示的任何表达，该组指令旨在使具有信息处理能力的系统直接地或者在 a）转换成另一种语言、代码或符号；b）以不同的物质形式再现这两种操作中的任何一个或全部之后执行特定功能。

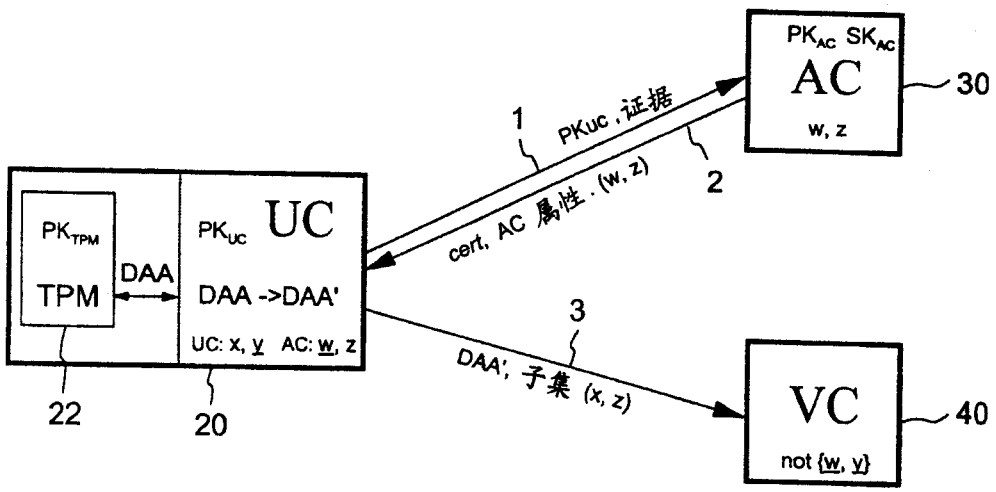

PK_AC SK_AC
AC
w, z
30
1
PKUC，证据
cert, AC 属性：(w, z)
2
PK_TPM
TPM
DAA
PK_UC UC
DAA ->DAA'
UC: x, y AC: w, z
3
DAA', 子集 (x, z)
VC
not {w, y}
40
22
20

图 1

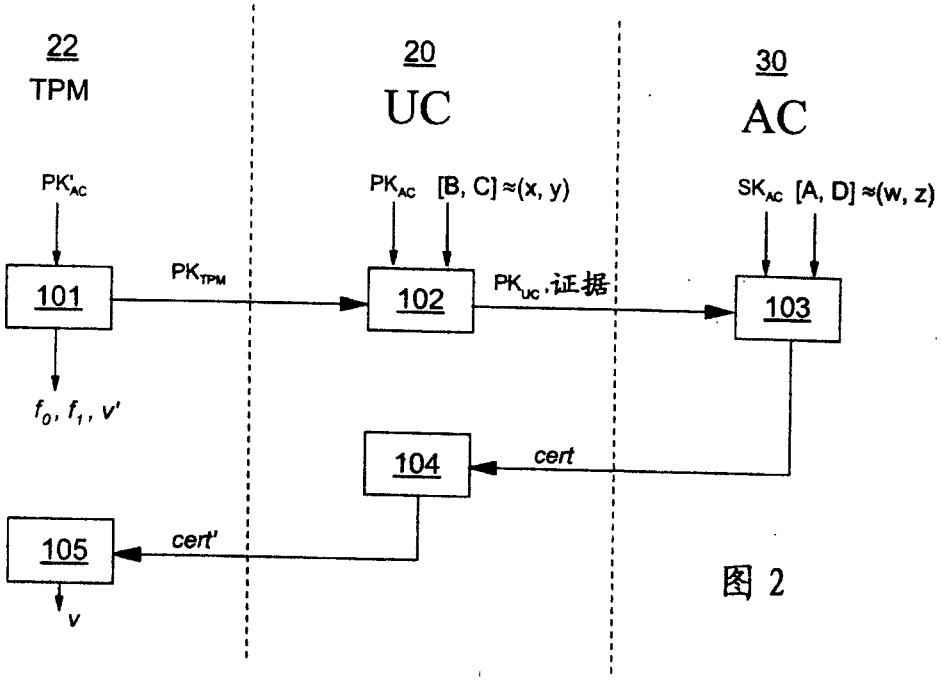

22
TPM
20
UC
30
AC
PK'AC
PKAC [B, C] ≈(x, y)
SKAC [A, D] ≈(w, z)
101
PKTPM
102
PKUC,证据
103
f0, f1, v'
104
cert
105
cert'
v

图 2

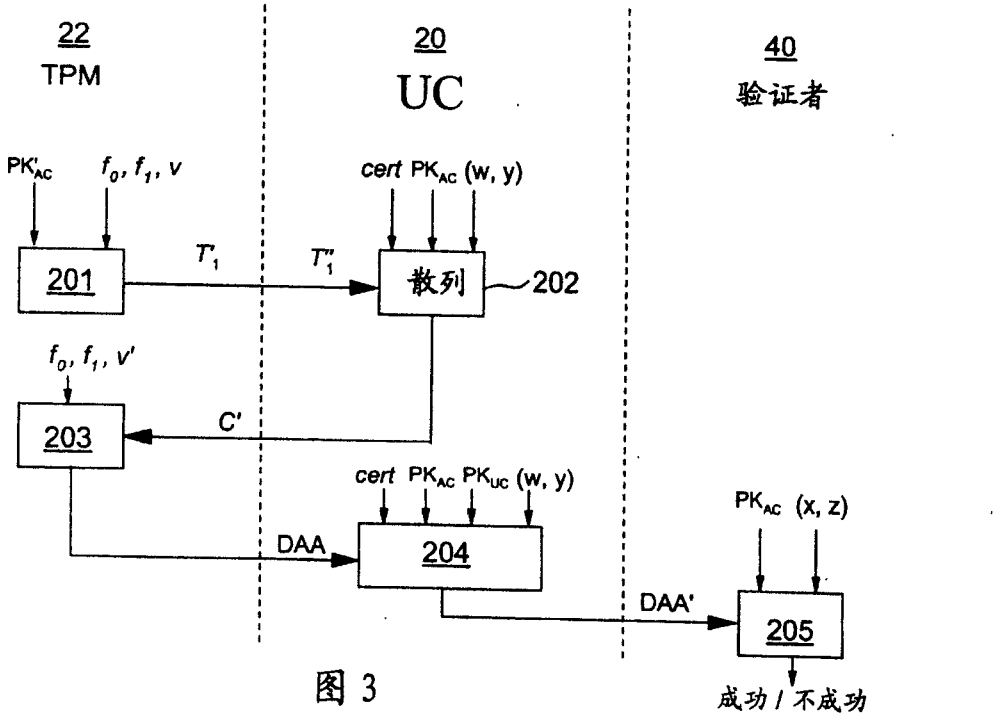

22
TPM
20
UC
40
验证者
PK'AC
f0, f1, v
cert PKAC (w, y)
201
T'1
T''1
散列
202
f0, f1, v'
203
C'
cert PKAC PKUC (w, y)
DAA
204
PKAC (x, z)
DAA'
205
成功 / 不成功

图 3