(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 103733564 B
(45)授权公告日 2018.05.15

(21)申请号 201280039063.7

(22)申请日 2012.05.04

(65)同一申请的已公布的文献号
申请公布号 CN 103733564 A

(43)申请公布日 2014.04.16

(30)优先权数据
61/495,790 2011.06.10 US

(85)PCT国际申请进入国家阶段日
2014.02.10

(86)PCT国际申请的申请数据
PCT/US2012/036541 2012.05.04

(87)PCT国际申请的公布数据
WO2012/170131 EN 2012.12.13

(73)专利权人 塞尔蒂卡姆公司
地址 加拿大安大略

(72)发明人 大卫·威廉·卡拉维兹
格雷戈里·马克·扎韦鲁哈
丹尼尔·理查德·L·布朗

(74)专利代理机构 中科专利商标代理有限责任公司 11021
代理人 赵伟

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

(56)对比文件
CN 101535845 A,2009.09.16,
CN 101815289 A,2010.08.25,
WO 99/49612 A1,1999.09.30,
N.P. Smart,Henk L. Muller,."A wearable public key infrastructure".《Wearable Computers,The Fourth International Symposium on IEEE》.2000,127-133.
Nader M.Rabadi,."Revised Self-Certified Implicit Certificate Scheme for Anonymous Communications in Vehicular Networks".《Vehicular Networking Conference》.2010,第III部分A部分第1段第8－10行,第14行,第2段第6－9行,第5段第3行,B部分第1段第1－2行,第11-12行,第25行－28行,C部分第1-3行.
Zuhua Shao,."Self-certified signature scheme from pairings".《The Journal of Systems and Software》.2007,388-395.

审查员 吕晓华

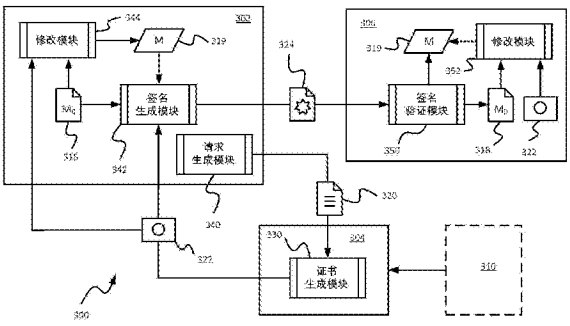
权利要求书4页 说明书21页 附图5页

(54)发明名称

利用隐式证书链的数字签名

(57)摘要

公开了使用隐式证书的方法、系统和计算机程序。在一些方面,访问消息和隐式证书。所述隐式证书与实体相关联。通过将所述消息与基于所述隐式证书的值进行组合来生成修改后的消息。基于所述修改后的消息生成数字签名,并且将所述数字签名发送给接收者。在一些方面,访问来自实体的数字签名和要使用所述数字签名验证的消息。访问与所述实体关联的隐式证书。通过将所述消息与基于所述隐式证书的值进行组合来生成修改后的消息。基于所述数字签名和所述修改后的消息验证所述消息。



CN 103733564 B

1.一种在密码系统(300)中使用隐式证书的方法,所述方法包括:

访问与实体(302)相关联的隐式证书(322);

访问用于由所述实体(302)进行数字签名的消息(318);

基于所述隐式证书生成散列值;

通过将所述用于进行数字签名的消息(318)与所述散列值进行组合来生成修改后的消息(319);

基于所述修改后的消息(319)生成数字签名;以及

通过数据通信网络向接收方发送所述用于进行数字签名的消息(318)和所述数字签名(324),

其中,所述将所述用于进行数字签名的消息(318)与所述散列值进行组合包括以下至少之一:

将所述散列值作为前缀、后缀或其与一个或更多个其他类型的附加物的组合附加到所述用于进行数字签名的消息(318);以及

对所述散列值和所述用于进行数字签名的消息(318)进行字符编码或数据压缩。

2.根据权利要求1所述的方法,其中,所述数字签名是基于所述修改后的消息(319)和与所述隐式证书相关联的密钥值生成的。

3.根据权利要求1所述的方法,其中,所述隐式证书(322)包括所述实体(302)的公钥重构值,以及所述修改后的消息(319)是通过将所述用于进行数字签名的消息(318)与所述实体(302)的公钥重构值进行组合来生成的。

4.根据权利要求1所述的方法,其中,所述隐式证书(322)包括所述实体(302)的公钥重构值,以及所述修改后的消息(319)是通过将所述用于进行数字签名的消息(318)与基于下述项的值进行组合来生成的:

所述实体(302)的公钥重构值,以及

所述隐式证书(322)中包含的附加信息。

5.根据权利要求1所述的方法,其中,访问所述隐式证书(322)包括访问证书机构(304)所颁发的隐式证书(322),以及所述修改后的消息(319)是通过将所述用于进行数字签名的消息(318)与基于下述项的值进行组合来生成的:

所述隐式证书(322);以及

所述证书机构(304)的公钥值。

6.根据权利要求1所述的方法,其中,所述隐式证书(322)包括所述实体(302)的公钥重构值,访问所述隐式证书(322)包括访问由从属于第二证书机构(310)的第一证书机构(304)所颁发的隐式证书(322),以及所述修改后的消息(319)是通过将所述用于进行数字签名的消息(318)与基于所述实体(302)的公钥重构值和以下至少一项的值进行组合来生成的:

所述第一证书机构(304)的公钥;

所述第二证书机构(310)的公钥;

所述第一证书机构(304)的隐式证书(322);或者

所述第二证书机构(310)的隐式证书。

7.一种在密码系统(300)中使用隐式证书(322)的方法,所述方法包括:

访问由实体(302)生成的数字签名；

访问要基于所述数字签名验证的消息(318)；

访问与所述实体(302)相关联的隐式证书(322)；

基于所述隐式证书(322)生成散列值；

通过将所述消息(318)与所述散列值进行组合来生成修改后的消息(319)；以及

基于所述数字签名和所述修改后的消息(319)来验证所述消息(318)，

其中，所述将所述消息(318)与所述散列值进行组合包括以下至少之一：

将所述散列值作为前缀、后缀或其与一个或更多个其他类型的附加物的组合附加到所述消息(318)；以及

对所述散列值和所述消息(318)进行字符编码或数据压缩。

8.根据权利要求7所述的方法，其中，所述消息(318)是基于所述数字签名、所述修改后的消息(319)和与所述隐式证书(322)相关联的公钥值来验证的。

9.根据权利要求7或权利要求8所述的方法，还包括：通过数据通信网络从所述实体接收所述消息(318)和所述数字签名。

10.根据权利要求7所述的方法，还包括：通过数据通信网络从所述实体(302)接收第一修改后的消息(319)，其中，通过将所述消息(318)与所述散列值进行组合来生成的修改后的消息(319)包括第二修改后的消息。

11.根据权利要求10所述的方法，其中，验证所述消息(318)包括：

根据验证算法，使用所述数字签名和与所述隐式证书(322)相关联的公钥来验证所述第一修改后的消息(319)；以及

比较所述第一修改后的消息和所述第二修改后的消息。

12.根据权利要求10所述的方法，其中，访问所述消息(318)包括：根据所述第一修改后的消息(319)导出所述消息(318)。

13.根据权利要求10所述的方法，其中，所述隐式证书(322)包括所述实体(302)的公钥重构值，以及所述第二修改后的消息是通过将所述消息(318)与所述实体(302)的公钥重构值进行组合来生成的。

14.根据权利要求10所述的方法，其中，所述隐式证书(322)包括所述实体(302)的公钥重构值，以及所述第二修改后的消息是通过将所述消息(318)与基于下述项的值进行组合来生成的：

所述实体(302)的公钥重构值，以及

所述隐式证书(322)中包含的附加信息。

15.根据权利要求10所述的方法，其中，访问所述隐式证书(322)包括访问证书机构所颁发的隐式证书(322)，以及所述第二修改后的消息是通过将所述消息(318)与基于下述项的值进行组合来生成的：

所述隐式证书(322)；以及

所述证书机构(304)的公钥值。

16.根据权利要求10所述的方法，其中，所述隐式证书(322)包括所述实体(302)的公钥重构值，访问所述隐式证书(322)包括访问由从属于第二证书机构(310)的第一证书机构(304)所颁发的隐式证书(322)，以及所述第二修改后的消息是通过将所述消息(318)与基

于所述实体(302)的公钥重构值和以下至少一项的值进行组合来生成的：

所述第一证书机构(304)的公钥；

所述第二证书机构(310)的公钥；

所述第一证书机构(304)的隐式证书(322)；或者

所述第二证书机构(310)的隐式证书。

17.一种包括密码模块的计算系统，所述密码模块能够操作用于执行操作，所述操作包括：

访问与实体(302)相关联的隐式证书(322)；

访问用于由所述实体(302)进行数字签名的消息(318)；

基于所述隐式证书(322)生成散列值；

通过将所述用于进行数字签名的消息(318)与所述散列值进行组合来生成第一修改后的消息；

基于所述第一修改后的消息生成数字签名；以及

通过数据通信网络向接收方发送所述用于进行数字签名的消息(318)和所述数字签名，

其中，所述将所述用于进行数字签名的消息(318)与所述散列值进行组合包括以下至少之一：

将所述散列值作为前缀、后缀或其与一个或更多个其他类型的附加物的组合附加到所述用于进行数字签名的消息(318)；以及

对所述散列值和所述用于进行数字签名的消息(318)进行字符编码或数据压缩。

18.根据权利要求17所述的计算系统，其中，所述密码模块包括第一密码模块，以及所述计算系统还包括第二密码模块，所述第二密码模块能够操作用于执行附加操作，所述附加操作包括：

访问所述数字签名；

访问所述用于进行数字签名的消息(318)；

访问所述隐式证书(322)；

通过将所述用于进行数字签名的消息(318)与基于所述隐式证书(322)的第二值进行组合来生成第二修改后的消息；以及

基于所述数字签名和所述第二修改后的消息来验证所述用于进行数字签名的消息(318)。

19.根据权利要求18所述的计算系统，其中，所述计算系统包括所述第一密码模块与所述第二密码模块之间的通信链路。

20.根据权利要求19所述的计算系统，其中，所述第二密码模块能够操作用于从所述第一密码模块接收所述第一修改后的消息(319)、所述数字签名以及所述隐式证书(322)。

21.根据权利要求20所述的计算系统，其中，所述第二密码模块能够操作用于通过下述方式来验证所述用于进行数字签名的消息(318)：

根据验证算法，使用所述数字签名来验证所述第一修改后的消息(319)；以及

比较所述第一修改后的消息(319)和所述第二修改后的消息。

22.根据权利要求20所述的计算系统，其中，所述第二密码模块还能够操作用于根据所

述第一修改后的消息(319)导出所述用于进行数字签名的消息(318)。

23.一种由接收方(306)执行的验证签名消息(324)的方法,所述方法包括:

接收签名消息(324);

访问与实体(302)相关联的隐式证书(322);

从所述签名消息(324)中提取原始消息(318);

基于所述隐式证书生成散列值;

通过将所述原始消息(318)与所述散列值进行组合来生成修改后的消息(319);

基于所述修改后的消息(319)生成数字签名;以及

使用所生成的数字签名来验证所述签名消息,

其中,所述将所述原始消息(318)与所述散列值进行组合包括以下至少之一:

将所述散列值作为前缀、后缀或其与一个或更多个其他类型的附加物的组合附加到所述原始消息(318);以及

对所述散列值和所述原始消息(318)进行字符编码或数据压缩。

利用隐式证书链的数字签名

[0001] 优先权要求

[0002] 本申请要求在2011年6月10日提交的序列号为61/495,790的美国临时申请的优先权,在此通过引用将其全部内容并入本文。

背景技术

[0003] 本说明书涉及在密码系统中使用隐式证书。密码系统可以在公共信道上提供安全通信。例如,在公钥密码系统中可以实现数字签名方案。在一些密码系统中,用户基于可信的第三方颁发的证书来验证其他用户的数字签名的真实性。

附图说明

[0004] 图1是示例数据通信系统的示意图。

[0005] 图2是另一示例数据通信系统的示意图。

[0006] 图3是示例密码系统的示意图。

[0007] 图4是示出用于在密码系统中执行操作的示例技术的流程图。

[0008] 图5是示出用于使用数字签名的示例技术的流程图。

[0009] 在各个图中,类似的参考标号和标记指示类似的要素。

具体实施方式

[0010] 可以按照以下技术来生成和/或使用公钥、数字签名或这两者:基于隐式证书来降低特定的攻击将战胜密码机制的可能性的技术。在一些实施例中,一种或多种技术可被实现为针对连锁攻击或其他类型的攻击的对策。这些对策可以代表这样一类解决方案,其中每个解决方案可被用于有效地阻挠敌手伪造隐式证书或与隐式认证的公钥相关联的签名的能力。例如在信赖方是公钥基础设施内的端实体的情况下,在信赖方是从属于另一证书机构的证书机构的情况下,或者在其他情况下,可以有效地实现这种技术。

[0011] 如此,隐式证书方案可以包括一个或更多个对策组件。在一些实例中,对策组件被应用在用于根据其隐式证书来重构使用者(subject)公钥的算法中。下文关于图2和图4描述了在公钥构建方案中可以应用的一些示例对策技术。在一些实例中,对策组件被应用在用于对消息上的数字签名进行基于隐式证书的验证的算法中。下文关于图3和图5描述了可被应用到数字签名生成和验证方案的一些示例对策技术。在一些示例中,可以使用这些对策组件与附加的或不同的对策组件的组合。

[0012] 图1是示例数据通信系统100的示意图,其示出了在其中可以实现基于隐式证书的密码方案和关联的对策的示例上下文。可以在其他上下文中实现基于隐式证书的密码方案和关联的对策。数据通信系统100包括:证书机构服务器104,两个终端102、106,以及数据网络108。数据通信系统100可以包括附加的、更少的、或者不同的组件。例如,数据通信系统100可以包括附加的存储设备、附加的服务器(包括附加的证书机构服务器)、附加的终端、以及图中未示出的其他特征。

[0013] 证书机构服务器104和终端102、106可以通过数据网络108相互通信以及与数据通信系统100中的其他组件通信。在图1示出的示例中，终端102可以向证书机构服务器104发送证书请求，以及证书机构服务器104可以通过向终端102发送隐式证书122来进行响应。终端102可以向终端106发送签名消息124，以及终端106可以使用证书机构服务器104颁发的隐式证书122来验证签名消息124的真实性。数据通信系统100可以支持附加的或不同类型的通信。在一些实现中，终端102、106还可以在相互之间、与证书机构服务器104、以及与数据通信系统100的其他组件交换加密的消息和其他类型的信息。

[0014] 在一些实现中，签名消息124包括隐式认证的签名。隐式认证的签名可以是消息上的数字签名，或者隐式认证的签名可以是消息的修改版本上的数字签名。可以利用隐式认证的密钥对来对消息进行签名和验证。隐式证书方案以及使用隐式证书的签名方案可被基于所期望的安全级别进行参数化，其中该安全级别可被例如以比特为单位表示为k。隐式证书方案的示例包括椭圆曲线Qu-Vanstone(ECQV)隐式证书方案以及最优邮寄证书(OMC)隐式证书方案。可以使用附加的或不同的隐式证书方案。可以使用隐式证书的数字签名方案的示例包括椭圆曲线Pintsov-Vanstone(ECPV)签名方案，基于密钥的ECPV签名方案，以及Schnorr签名方案。可以使用附加的或不同的数字签名方案。

[0015] ECPV签名方案是具有部分消息恢复的签名方案。标准ANSI X9.62、IEEE P1363a和ISO9796-3规定了ECPV签名方案的示例实现(使用2k比特输出散列函数)。套件E规定了具有2k比特输出的ECPV签名的示例(具体地，AES128-MMO)。ECPV签名方案的基于密钥的变形允许签名者对签名消息的可恢复部分进行加密，使得仅目标接收方可以恢复该可恢复部分。其他各方仍可以验证消息的公共部分上的签名。

[0016] ECQV隐式证书方案是隐式证书方案的示例。在高效加密标准组(SECG)于2009年5月公布的第二版“Standards for Effic ient Cryptography4(SEC4)Standard”中描述了ECQV机制的实现。该SEC4标准规定使用具有2k比特输出的散列函数。套件E也规定了ECQV，但是具有短的(k比特)散列函数，AES-128-MMO。

[0017] 在一些方面，隐式证书可以使得信赖方能够利用公钥基础设施，而不需要向信赖方显式地传输公钥。公钥可被用在密码协议中，诸如用于验证据称已经由公钥的拥有者签名的消息的完整性和来源真实性。与在证书主体内包含使用者公钥、使用者标识符、以及证书机构在至少使用者公钥和使用者标识符上生成的数字签名的显式证书相比，隐式证书可以更加简洁。在一些实现中，隐式证书不显式包含使用者公钥，而是使得能够根据隐式证书重构使用者公钥。在一些实现中，隐式证书可以显式包含使用者公钥。信赖方可以使用证书机构的公钥来重构使用者公钥。

[0018] 在图1示出的示例中，隐式证书方案被下述三方使用：证书机构、证书请求者、以及证书处理者。在示出的示例中，请求者实体从证书机构实体获取隐式证书。隐式证书证明请求者的身份，并且允许处理者实体获取请求者的公钥。更普遍地，在一些上下文中，附加的或不同的实体可以使用隐式证书方案。

[0019] 作为隐式证书方案的示例，ECQV隐式证书方案的一些实现可以按照六个操作方面进行描述。这六个方面可以以任何合适的顺序或组合来执行。而且，可以以更少的、附加的、或者不同的操作方面来实现隐式证书方案。此处作为示例提供六个操作方面的描述。

[0020] ECQV隐式证书方案的第一方面是ECQV设立步骤。在该阶段，证书机构建立椭圆曲

线域参数、散列函数、证书加密格式，并且实体具有随机数生成器。证书机构生成密钥对。实体接收证书机构的公钥和域参数的真实副本。可以使用任何合适的技术来实现ECQV设立。

[0021] ECQV隐式证书方案的第二方面是证书请求操作。证书请求者生成针对证书的请求。将该请求发送给证书机构。该请求的密码成分是使用与证书机构在ECQV设立期间使用的相同过程生成的公钥。可以使用任何合适的技术来实现证书请求。

[0022] ECQV隐式证书方案的第三方面是证书生成操作。当接收到证书请求时，证书机构确认请求者的身份，并且创建隐式证书。证书机构实体向请求者实体发送响应。可以使用任何合适的技术来实现证书生成。

[0023] ECQV隐式证书方案的第四方面是已认证公钥提取操作。给定请求者实体的隐式证书、域参数、以及证书机构的公钥，公钥提取算法计算请求者的公钥。可以使用任何合适的技术来实现已认证公钥提取。

[0024] ECQV隐式证书方案的第五方面是证书接收操作。在接收到对证书请求的响应之后，请求者计算其隐式认证的密钥对，并且确保该密钥对是有效的。可以使用任何合适的技术来实现证书接收。

[0025] ECQV隐式证书方案的第六方面是ECQV签名验证操作。在一些实现中，可以使用形成请求者的证书上的显式签名的附加信息来增强ECQV隐式证书。可以使用任何合适的技术来实现签名验证。

[0026] 在一些情形中，隐式证书颁发可被实现为请求者与证书机构之间的双行程协议，其中第一流程是来自请求者的证书请求，而第二流程是来自证书机构的响应，该响应包含证书。

[0027] 在一个示例操作方面，请求者实体、证书机构以及验证者(或者处理者)实体有权访问椭圆曲线域参数(包括群的生成器G)、随机数生成器、散列函数H、证书编码方案、有效数据类型、以及用于执行该方案的任何其他参数或函数。可以基于密码系统中的指定安全级别来选择所述参数和函数中的一些或全部。请求者已经被分配唯一的标识符I。请求者通过选择值$k_U \in_R [1, n-1]$并且计算$R_U := k_U G$来生成请求(I, R_U)。此处，k_U，可以是整数，G可以是椭圆曲线群的生成器，以及R_U可以是该群中的椭圆曲线点。请求者向证书机构发送该请求。证书机构基于该请求生成隐式证书$Cert_U$。为了生成该请求，证书机构选择随机值$k \in_R [-, n-1]$，并且通过计算$P = R_U + kG$生成公钥重建数据P。此处，k可以是整数，以及P可以是其生成器是G的椭圆曲线群中的椭圆曲线点。证书机构然后通过证书编码例程$Cert_U := Encode(P, I, *)$来生成隐式证书$Cert_U$。证书机构然后通过计算$e := H_n(Cert_U)$生成散列值e，并且通过计算$r := ek + d_{CA} \bmod n$生成私钥分发值r。此处，r表示整数，函数$H_n$表示散列函数，以及$H_n$的输出可以是整数$\bmod n$。Encode()函数中的自变量“*”可以表示通配符，以允许证书机构在证书中包含附加的可选的数据，下文将进行举例说明。

[0028] 隐式证书编码方案的示例包括固定长度字段方案、最小ASN.1编码方案、兼容X.509的ASN.1编码方案等等。固定长度字段方案和ASN.1编码方案可被用于在一些情况下获得更大带宽效率。兼容X.509的ASN.1编码方案生成可被重新编码为标准X.509证书(如，具有或不具有显式签名值)的隐式证书。通过固定长度字段方案编码的证书可以包括一系列字段，每个字段具有固定长度。例如，实体可以都对证书中的字段f_n的数目、每个字段的八位字节长度、指示哪个字段将包含公钥重构数据的索引值i、以及针对每个字段元素的有

效性规则达成一致意见。在一些实现中，证书中的字段之一是公钥重构数据，而其他字段可以具有开放格式。例如，其他字段可以包括诸如请求者的电子邮件地址或者隐式证书的期满日期之类的值。

[0029] 在一个示例操作方面，证书机构向请求者发送私钥分发数据r以及隐式证书$Cert_U$。请求者使用该证书数据来生成请求者的椭圆曲线密钥对(b,B)。请求者可以通过下述方式生成椭圆曲线密钥对(b,B)：计算散列值$e:=H_n(Cert_U)$，计算私钥值$b=ek_U+r \pmod n$，以及计算公钥值B=eP+C。对于附加的或不同类型的隐式证书方案，该示例操作可被适配或修改。

[0030] 在图1示出的示例中，证书机构服务器104是能够执行密码系统中的证书机构的操作的计算系统。证书机构服务器104通常可操作用于接收、发送、处理和存储与密码系统关联的信息。尽管图1示出单个证书机构服务器104，但是可以使用多个证书机构服务器104(包括服务器簇)以及使用不同于服务器的附加的或不同类型的计算设备来实现证书机构。

[0031] 证书机构服务器104通常包括数据处理装置、数据存储介质和数据通信接口。例如，证书机构服务器104可以包括处理器、存储器、输入/输出控制器、和/或其他特征。存储器例如可以包括随机访问存储器(RAM)、存储设备(如，可写只读存储器(ROM)等)、硬盘、缓冲存储器、或者其他类型的存储介质。存储器可以存储与计算机应用关联的指令(如计算机代码)、程序和计算机程序模块、以及其他资源。处理器可以包括任何类型的数据处理装置，如通用微处理器、专用处理器、数字控制器、或者其他类型的设备。输入/输出控制器可以耦合到输入/输出设备(如显示器、键盘等)以及数据网络108。输入/输出设备可以通过通信链路接收和发送模拟或数字形式的数据，所述通信链路例如是串行链路、无线链路(如红外、射频等)、并行链路、或者其他类型的链路。

[0032] 数据网络108可以包括任何合适类型的数据通信网络。例如，数据网络108可以包括无线或有线网络、蜂窝网络、电信网络、企业网、专用公共网络、局域网(LAN)、广域网(WAN)、私有网络、公共网络(如互联网)、WiFI网络、包括卫星链路的网络、或者其他类型的数据通信网络。数据网络108可以包括通过防火墙或者实现各种安全级别的类似特征来定义的分层结构。

[0033] 终端102、106是能够基于数据通信系统100规定的通信方案进行通信的计算设备。终端102、106通常可操作用于接收、发送、处理和存储信息。尽管图1示出两个终端102、106，但是数据通信系统100可以包括任何数目的终端。数据通信系统100可以包括终端的组或子组，子组或组中的终端能够相互通信，但是不一定能够与其他组或子组中的终端通信。数据通信系统100可以包括不同类型的终端，具有不同类型的硬件和软件配置的终端，并且位于各种不同位置的终端。在一些实例中，可以将多个设备或子系统一起识别为单个终端。数据通信系统100中的终端均可以利用证书机构服务器104颁发的隐式证书。

[0034] 终端102通常包括数据处理装置、数据存储介质和数据通信接口。例如，终端102可以包括存储器、处理器和输入/输出控制器。终端可以包括用户接口设备，如显示器、触摸屏、鼠标、或键盘。终端的存储器可以存储与计算机应用关联的指令(如计算机代码)、程序和计算机程序模块、以及其他资源。

[0035] 终端102可被实现为手持设备，如智能电话、个人数字助理(PDA)、便携式媒体播放器、膝上型计算机、笔记本计算机、平板计算机等等。终端可以包括工作站、大型机、非便携

式计算机系统，在建筑物、交通工具或者其他类型的设施中安装的设备。终端可以包括嵌入式通信设备。例如，终端可以包括消息收发设备，其被嵌入在智能能量系统的智能能量表中。也可以使用其他类型的终端。

[0036] 终端可以与具体的用户实体、具体的用户身份或者其任意组合相关联。一个或更多个终端可以与人类用户相关联。在一些实现中，终端不与任何具体的人类用户相关联。一个或更多个终端可以与具体设备、具体位置、具体设施、或者其他标识信息相关联。

[0037] 在一个操作方面，终端102向证书机构服务器104发送证书请求120，以及证书机构服务器104生成针对终端102的隐式证书122。隐式证书122将特定的公钥值与特定的用户实体(如，终端102、与终端102关联的用户、在终端102中实现的模块等)相关联。终端102从证书机构服务器104接收隐式证书122。当终端102有消息要发送给终端106时，终端102使用隐式证书122生成针对消息的数字签名。该数字签名与消息组合在一起，以形成签名消息124，终端102将该签名消息124发送给终端106。在一些实现中，数字签名和消息是分开发送的。终端106接收签名消息124，获取隐式证书122，并且基于隐式证书122验证数字签名。隐式证书还可用于其他类型的方案中，例如用于加密方案中。

[0038] 数据通信系统100实现的隐式证书方案允许终端102、106即使当数据网络108上的通信被恶意用户观察时，或者当恶意用户(如，通过篡改诚实终端的通信)干预通信系统100时，也以安全的方式相互通信。隐式证书122将与终端102关联的用户实体和能够用于验证终端102生成的数字签名的特定公钥值捆绑在一起。终端106能够获取隐式证书122，以验证数字签名是由与终端102关联的用户实体生成的，而不是由冒充者生成的。终端106还可以验证隐式证书122是由可信的第三方在证书机构服务器104处生成的。以这种方式，隐式证书122可以提供可信的第三方做出的确认：签名消息124是由与终端102关联的用户实体签名的，而不是由冒充者签名的。

[0039] 示例隐式证书122包括与终端102关联的用户实体的标识。示例隐式证书122包括能被用于构建用户实体的公钥的信息。在一些实例中，使用隐式证书122验证数字签名还确认：用户实体拥有对应的私钥。图1示出的示例隐式证书122既不包括公钥的显式表示，也不包括证书机构的数字签名的显式表示。因此，在一些实现中，隐式证书122比一些其他类型的数字证书更加简洁。在一些实例中，隐式证书122包括证书机构的数字签名，其允许用户实体(如与终端106关联的用户实体)验证隐式证书122是由可信的证书机构生成的。在一些实例中，证书机构要求用户实体证实用户实体的私钥的知识。在一些实例中，隐式证书122包括用户的公钥的显式表示。

[0040] 替代显式表示终端102的公钥，图1中的示例隐式证书122包括公钥重构数据，该公钥重构数据能够与其他信息(例如，证书机构的公钥等)组合以生成与终端102关联的用户实体的公钥。示例隐式证书122被构建为使得对终端102生成的数字签名的成功验证用作终端102拥有该私钥的确认。因此，根据一些隐式证书方案，可以在密钥使用期间共同验证用户实体与其公钥的捆绑以及用户实体关于其私钥的知识。

[0041] 因为示例隐式证书122不包括终端102的公钥的显式表示，在一些情况下，证书机构有可能在不曾生成公钥值的显式表示的情况下颁发隐式证书122，以及终端102、106有可能在不曾生成公钥值的显式表示的情况下使用隐式证书122。例如，在一些椭圆曲线密码系统中，公钥的值可被表达为：$B=eP+C$，并且替代显式计算公钥B的值，终端102、106在它们例

如使用公钥来生成或验证数字签名时将值e、P和C并入更大的等式(如,签名等式或验证等式)。如此,有可能能够在不显式计算公钥的情况下实际上使用或生成公钥。

[0042] 图2是另一示例数据通信系统200的示意图。数据通信系统200包括:证书机构服务器204a、204b和204x;终端202和206;数据网络208;以及敌手212。数据通信系统200可以包括附加的、更少的、或者不同的组件。例如,数据通信系统200可以包括附加的存储设备、附加的服务器(包括附加的证书机构服务器)、附加的终端、附加的敌手以及图中未示出的其他特征。在一些示例实现中,终端202可以实现为图1中的终端102,并且终端206可以实现为图1中的终端106。在一些示例实现中,证书机构服务器204a、204b、204x中的每一个可以实现为图1中的证书机构服务器104。敌手212可以实现为终端、服务器或者任意其他合适的计算设备或系统。

[0043] 终端202、206可以基于隐式证书方案交换消息。例如,隐式证书方案可被用于数据认证、数据加密或者这些和其他功能的组合。在一些实例中,终端202向终端206发送消息,以及终端202可以基于证书机构服务器204a、204b、204x之一颁发的隐式证书对消息加密、对消息签名、或者执行这两者。敌手212可以观察网络208上的通信,并且发起攻击,从而尝试损害隐式证书方案的安全。证书机构服务器204a、204b、204x和终端202、206实现的隐式证书方案包括能够挫败敌手212的某些类型的攻击的对策。

[0044] 在一些实例中,基于证书机构服务器204a、204b、204x生成的隐式证书链来颁发与终端202关联的隐式证书。例如,证书机构服务器204a、204b、204x可以包括根证书机构和多个从属证书机构。隐式证书链可以包括针对根证书机构的隐式证书和针对每个从属证书机构的隐式证书。

[0045] 在一些示例实现中,通信系统200中实现的隐式证书方案使用基于ECQV隐式证书链导出的公钥。一般而言,根证书机构或者任意从属证书机构可以颁发隐式证书。ECQV隐式证书链可以由根证书机构和一个或更多个从属证书机构的组合来生成,其中每个从属证书机构具有来自上级证书机构的隐式证书。链中的最后一个证书机构可以向用户实体(如,终端)颁发隐式证书。

[0046] 可以使用针对如椭圆曲线群之类的群的附加标记(additive notation)来描述通信系统200实现的示例ECQV隐式证书方案,在所述群中离散对数问题被认为是困难的。群具有阶数(order)n。在一些实现中,群具有基本阶数。系统参数包括群的生成器G,其是已知的并且可用于使用通信系统200的所有实体。

[0047] 在一些实例中,ECQV隐式证书被颁发给终端202所代表的用户实体或者与终端202关联的用户实体。用户实体的ECQV隐式证书可以由参数对(P,I)表示,或者基于参数对(P,I)。值P是针对用户实体的公钥重构数据,以及值I是用户实体的标识信息。可以根据隐式证书来重构用户实体的公钥B。用户实体与证书机构交互,以获取ECQV隐式证书(P,I)和私钥b,使得B=bG。在一些实现中,用户实体的ECQV隐式证书(P,I)基于证书机构形成的ECQV隐式证书链。

[0048] 在一些实例中,每个从属证书机构的重构的公钥充当用于验证该从属证书机构颁发的证书的公钥。例如,根证书机构可以具有私钥c,该私钥c可以是整数,并且公钥C=cG。链中的每个隐式证书由参数对(P_j,I_j)表示,其中j从1到m+1,其中m+1是链的长度。对应的公钥表示为C_j。除了$B=C_{m+1}$,每个公钥C_j是从属证书机构的公钥。第1个公钥可以基于函数F,根据

下述公式来生成：

[0049] $C_1=C_{1-1}+F(C,C_1,...,C_{1-1},P_1,...,P_1,I_1,...,I_1,*_1,...,*_1)P_1.$ (1a)

这m+1个等式可以被组合成如下单个等式：

[0050] $B=C_{m+1}=C+F(C,P_1,I_1,*_1)P_1+\cdots+F(C,C_1,...,C_m,P_1,...,P_{m+1},I_1,...,I_{m+1},*_1,...,*_{m+1})P_{m+1}$ (1b)此处，已经包括$*_i$(其中i=1,...,m+1)，以赢取在如$(P_j,I_j,*_j)$之类的隐式证书结构中包括附加信息的可能性。

[0051] 在一些实例中，等式1a和1b中的函数F的输出是基于对散列函数或另一类型的函数求值而生成的。例如，函数F可以是散列函数，函数F可以包括一个或更多个散列函数，函数F可以调用一个或更多个散列函数，或者函数F可以以其他方式利用散列函数或其他类型的函数。在一些实例中，散列函数是将任意输入映射到在0与n之间的整数的随机函数，或者接近该随机函数。在一些实例中，散列函数是将任意输入映射到在0与$\sqrt{n}$之间的整数的随机函数，或者接近该随机函数。散列函数的示例包括：SHA散列函数族(SHA-1，SHA-256，等等)，通过截断它们的输入创建的这些函数的变形，以及其他散列函数。另一示例散列函数是MMO散列函数，其是利用块密码创建的，通常是利用AES块密码创建的(所得函数称为AES-MMO)。其他基于块密码的散列函数也是合适的。由具有固定密钥(其在域参数中公布)的HMAC构造来创建的函数是另一示例函数。在一些实现中，可以使用例示为具有固定密钥的其他MAC函数，如CBC-MAC。

[0052] 等式1a和1b是在图2中实现的示例隐式证书方案中使用的公钥生成公式的通用表示。在各种实现中，函数F可以采取各种形式。下面描述若干特定的示例。可以选择函数F，使得挫败敌手的攻击。换言之，在一些实例中，函数F可以降低敌手攻击成功的可能性。例如，在一些实例中，可以选择函数F，使得提供与某些传统方案相比提高的安全性。

[0053] 根据一些传统方案，可以如下重构每个公钥：

[0054] $C_j=C_{j-1}+H(P_j,I_j)P_j,$ (2)

[0055] 其中，H是散列函数，。根据传统方案，这m+1个等式可被组合成如下单个等式：

[0056] $B=C_{m+1}=C+H(P_1,I_1)P_1+...+H(P_{m+1},I_{m+1})P_{m+1}$ (3)

[0057] 在一些实例中，该传统方案允许敌手伪造将会被未觉察的信赖方接受的隐式证书。如此，敌手有可能模仿实体(如从属于另一证书机构的证书机构实体)的合法动作，从而向上级证书机构请求隐式证书，该隐式证书将使得该从属证书机构继而能够生成对于从属于它的证书机构而言可接受的证书，或者能够生成对于将使用与已认证公钥对应的私钥来例如对消息进行数字签名(可使用已认证公钥验证该消息)的任何实体而言可接受的证书，或者能够对使用已认证公钥加密的加密消息进行解密。在一些实例中，敌手的恶意模仿仅需要关于公共可用信息的被动知识，例如敌手冒充要求其产生模仿的隐式证书的证书机构的隐式证书系统参数和公钥或隐式证书。在一些实例中，上述等式1a和1b中表示的方案可被实现为对抗这种攻击的成功对策。

[0058] 在对上述等式2和3表示的传统方案的一些示例攻击中，敌手能够使用关于根证书机构的公钥的知识或者关于从属于根证书机构的证书机构的公钥的知识来向证书链添加四个附加链接，导致敌手知道与添加的第四链接的公钥对应的私钥。在对传统方案的另一示例攻击中，敌手添加三个链接并且对选定的任意单个消息进行数字签名，并且该数字签名使用与第三添加链接关联的公钥正确验证。在一些实例中，上述等式1a和1b中表示的方

案可被实现为对抗这种攻击的成功对策。

[0059] 在一些示例实现中，上述等式1a和1b中表示的方案可被用于战胜链式攻击，而等式2和3中表示的方案可能易受链式攻击的伤害。在链式攻击中，敌手有权访问椭圆曲线域参数，包括G(或者更一般地，离散对数群的描述和生成器)、根证书机构的公钥C、以及m+1个标识字符串$I_1,\ldots,I_{m+1}$。成功的链式攻击的输出是m+1个公钥重构数据值$P_1,\ldots,P_{m+1}$和与重构的公钥$B=C_{m+1}$对应的私钥b，即bG=B。

[0060] 为了实现针对示例的长度为4的链的链式攻击，敌手访问输入，包括根证书机构的公钥C和四个标识符I_1,I_2,I_3,I_4。该链式攻击可以做出关于上述等式2和3中的散列函数H的假设，以简化对何时攻击会成功的分析，但是这些假设不是实现攻击所必需的。例如，链式攻击可以假设上述等式2和3中的散列函数H生成在间隔1到n之间均匀分布的值。该链式攻击有可能可以假设上述等式2和3中的散列函数H生成不那样分布的值，如在0与$\sqrt{n}$之间的值，或者以某种方式偏差的值。

[0061] 链式攻击的成功实现可以生成输出，包括四个公钥重构值P_1,P_2,P_3,P_4以及使得下式成立的私钥b：

[0062] $bG=C+H(P_1,I_1)P_1+H(P_2,I_2)P_2+H(P_3,I_3)P_3+H(P_4,I_4)P_4.$ (4)

[0063] 为了实现针对示例的长度为4的链的链式攻击，敌手基于输入执行下述动作。令j的范围为从1到2。计算$H_{j,k}=H(P_{j,k},I_j)$，其中$P_{j,k}=C+kG$，并且k的范围为从1到$n^{1/3}$。将值$H_{j,k}$组装到列表L_j中。总的计算(针对j=1和j=2)可能花费$2n^{1/3}$次标量乘法和散列求值的时间。

[0064] 示例的链式攻击可以如下继续进行。生成值$(r,s,1+H_{1,r}+H_{2,s} \bmod n,(H_{1,r})r+(H_{2,s})s \bmod n)$的列表$L_{1,2}$，使得$1+H_{1,r}+H_{2,r} \bmod n<n^{2/3}$。该列表(其现在可以替代列表$L_1$和列表$L_2$)将具有约$n^{1/3}$的长度，因为每个列表$L_j$具有尺寸$n^{1/3}$，以及概率$H_{1,r}+H_{2,s} \bmod n<n^{2/3}$约是$n^{-1/3}$。不是全部的成对比较都进行。相反，可以使用散列表(高存储)或排序列表(低存储)。注意(非负)$1+H_{1,r}+H_{2,s}$最大可以是2n-1。因此，$1+H_{1,r}+H_{2,s} \bmod n$或者是$1+H_{1,r}+H_{2,s}$，或者是$1+H_{1,r}+H_{2,s}-n$。对于$H_{1,r}<n^{2/3}-1$，满足$0\leqslant H_{2,s}<n^{2/3}-1-H_{1,r}$的值是合适的。而且，满足$n-1-H_{1,r}\leqslant H_{2,s}<\min(n,n+nn^{2/3}-1-H1,r)$的$H_{1,r}$值是合适的。

[0065] 示例链式攻击可以如下继续进行。令j的范围为从3到4。计算$H'_{j,k}=H(P_{j,k},I_j)$，其中$P_{j,k}=C+kG$，并且k的范围为从1到$nn^{1/3}$。将值$H_{j,k}$组装到列表L_j中。总的计算(针对j=3和j=4)可能花费$2n^{1/3}$次标量乘法和散列求值的时间。产生值$(t,u,-(H_{3,t}+H_{4,u}) \bmod n,(H_{3,t})t+(H_{4,u})u \bmod n)$的列表$L_{3,4}$，使得$-(H_{3,t}+H_{4,u}) \bmod n<n^{2/3}$。该列表现在替代列表$L_3$和列表$L_4$。

[0066] 示例链式攻击可以如下继续进行。现在找到列表$L_{1,2}$和$L_{3,4}$.中的冲突(r^*,s^*,t^*,u^*)。因为$L_{1,2}$和$L_{3,4}$中的第三坐标值范围均是从0到$n^{2/3}$，并且每个列表具有$n^{1/3}$个表项，所以在一些情形下应该存在冲突。在一些实现中，找到冲突的代价可被保持在约$n^{1/3}$。找到冲突则识别出了使得下式成立的值(r^*,s^*,t^*,u^*)：

[0067] $$\left(1+H_{1,r^*}+H_{2,s^*} \bmod n\right)+\left((H_{3,t^*}+H_{4,u^*}) \bmod n\right)=0 \bmod n。$$

可以通过设置下式来完成示例链式攻击：

[0068]

$$b=\left((H_{1,r^*})r^*+(H_{2,s^*})s^* \bmod n\right)+\left((H_{3,t^*})t^*+(H_{4,u^*})u^* \bmod n\right) \bmod n$$

[0069] 在一些实现中，上面描述的示例链式攻击利用了广义生日攻击方法。例如，David

Wagner在Advances in Cryptology——CRYPTO2002上发表的题目为“A Generalized Birthday Problem”的论文提供对广义生日方法的描述。一些传统攻击需要$n^{1/2}$量级的时间(其相当得高),证实了攻击的有效性。例如,在选择n具有比特长度256(实践中的常见选择)的情况下比较$n^{1/2}$和$n^{1/3}$,示出了从128比特级别(如果最佳攻击具有代价$n^{1/2}$)下降到85比特级别(当最佳攻击具有代价$n^{1/3}$)的安全性降低。

[0070] 在一些实例中,链式攻击可被扩展(如下文所示)到后面跟着使用Schnorr算法(其是PVS算法的基础)的消息签名的长度为3的链,其中由(e=H*(U,M),v)构成的消息M上的签名如下:

[0071] $C_1=C+H(P_1,I_1)P_1$

[0072] $C_2=C_1+H(P_2,I_2)P_2$

[0073] $B=C_3=C_2+H(P_3,I_3)P_3U=vG-H^*(U,M)B=vG-H^*(U,M)(C+H(P_1,I_1)P_1+H(P_2,I_2)P_2+H(P_3,I_3)P_3)$。

[0074] 为了实现该示例场景下的链式攻击,选择消息M的期望值。令$P_j=C+p_jG$,其中j=1,2,3,以及U=fC+tG。对下式求值:

[0075] $fC=-H^*(U,M)(1+H(p_1,I_1)P_1+H(P_2,I_2)P_2+H(P_3,I_3)P_3)C$。或者等价于对下式求值:

[0076] $-fH^*(U,M)^{-1}=1+H(P_1,I_1)P_1+H(P_2,I_2)P_2+H(P_3,I_3)P_3$。

[0077] 示例链式攻击可以如下继续进行。令f=1,并且如上文针对长度为4的链所概述地那样继续,但是使用$H^*(U,M)^{-1}\bmod n$作为散列函数值来替代左侧的H,并且对下式求值:

[0078] $0=1+H^*(U,M)^{-1}+H(P_1,I_1)P_1+H(P_2,I_2)P_2+H(P_3,I_3)P_3(\bmod n)$然后相应地设置v。例如,可以根据下式来设置v:

[0079] $t=v-H^*(U,M)(H(P_1,I_1)p_1+H(P_2,I_2)p_2+H(P_3,I_3)p_3)(\bmod n)$。

[0080] 因此,这些示例链式攻击有可能损害隐式证书方案(诸如上述等式2和3表示的方案)的可靠性。然而,可以通过对策来避免或者降低这种链式攻击的成功。例如,在一些实现中,下述技术中的一些或全部可被用于战胜上文描述的示例链式攻击。

[0081] 下面的示例公钥生成算法中的每一个可被用作针对上述链式攻击以及其他类型的攻击的对策。下述示例算法是根据上面描述的ECQV隐式证书链来表达的。这些示例也可被修改以适应其他隐式证书方案。而且,所述示例是针对存在多个证书机构(根证书机构和一个或更多个从属证书机构)的情况,一般性地表达的。这些示例可以在存在单个证书机构(如,仅根证书机构)的情况下有效地实现。另外,尽管这些技术被描述为对策,但是这些技术即使在不存在敌手或攻击威胁时也可能是有用的或者提供优点。如此,这些技术可在任何上下文中例如用作针对攻击的对策或者用于其他目的。

[0082] 作为第一示例对策方案,可以使用下述公式来生成公钥,在一些示例方案中该公钥利用ECQV隐式证书链。下述公式可被用作针对链式攻击的对策、用作针对其他类型的攻击的对策、或者用于其他目的。

[0083] $C_1=C+H(P_1,I_1,*_1)P_1$

[0084] $C_2=C_1+H(P_1,I_1,*_1,P_2,I_2,*_2)P_2$

[0085] $C_3=C_2+H(P_1,I_1,*_1,P_2,I_2,*_2,P_3,I_3,*_3)P_3$

[0086] $B=C_{m+1}$

[0087] $=C_m+H(P_1,I_1,*_1,\ldots,P_{m+1},I_{m+1},*_{m+1})P_{m+1}$

[0088] 作为第二示例对策方案，在一些示例方案中可以使用下述公式来生成公钥，该公钥利用ECQV隐式证书链。下述公式可被用作针对链式攻击的对策、用作针对其他类型的攻击的对策、或者用于其他目的。

[0089] $C_1=C+H(P_1,I_1,*_1)P_1=C+H_1P_1$

[0090] 其中$H_1=H(P_1,I_1,*_1)$

[0091] $C_2=C_1+H(H(P_1,I_1,*_1),P_2,I_2,*_2)P_2$

[0092] $=C_1+H_2P_2$

[0093] $C_3=C_2+H(H(H(P_1,I_1,*_1),P_2,I_2,*_2),P_3,I_3,*_3)P_3$

[0094] $=C_2+H_3P_3$

[0095] $B=C_{m+1}$

[0096] $=C_m+H(H_m,P_{m+1},I_{m+1},*_{m+1})P_{m+1}=C_m+H_{m+1}P_{m+1}$

[0097] 作为第三示例对策方案，在一些示例方案中可以使用下述公式来生成公钥，该公钥利用ECQV隐式证书链。下述公式可被用作针对链式攻击的对策、用作针对其他类型的攻击的对策、或者用于其他目的。

[0098] $C_1=C+H(C,P_1,I_1,*_1)P_1$

[0099] $C_2=C_1+H(C_1,P_2,I_2,*_2)P_2$

[0100] $B=C_{m+1}$

[0101] $=C_m+H(C_m,P_{m+1},I_{m+1},*_{m+1})P_{m+1}$

[0102] 作为第四示例对策方案，在一些示例方案中可以使用下述公式来生成公钥，该公钥利用ECQV隐式证书链。下述公式可被用作针对链式攻击的对策、用作针对其他类型的攻击的对策、或者用于其他目的。

[0103] $C_1=C+H(P_1,I_1,*_1)P_1$

[0104] $C_2=C_1+H(C_1-C,P_2,I_2,*_2)P_2$

[0105] $B=C_{m+1}$

[0106] $=C_m+H(C_m-C_{m-1},P_{m+1},I_{m+1},*_{m+1})P_{m+1}$

[0107] 作为第五示例对策方案，在一些示例方案中可以使用下述公式来生成公钥，该公钥利用ECQV隐式证书链。下述公式可被用作针对链式攻击的对策、用作针对其他类型的攻击的对策、或者用于其他目的。如果根据Merkle-Damgard构造来构造散列函数，则其具有使得其变得非随机的某种特定(称为长度扩展特性)。如果散列函数具有Merkle-Damgard(MD)特性，则可以使用下述技术。下述技术在其他上下文和情况下也可以是有用的。令H_i表示用IV_i来替代标准MD特性散列函数的IV(初始化矢量)。初始化矢量(IV)是对加密基元(cryptographic primitive)(有时需要是随机的或伪随机的)的固定尺寸的输入。当在散列函数中使用时，IV通常被规定为函数的一部分，并且不会改变。相应地，

[0108] $IV_1=H(P_1,I_1,*_1)$

[0109] $IV_2=H_1(P_2,I_2,*_2)$

[0110] $IV_3=H_2(P_3,I_3,*_3)$，

[0111] 等等。此外，

[0112] $C_1=C+H(P_1,I_1,*_1)P_1$

[0113] $C_2=C_1+H_1(P_2,I_2,*_2)P_2$

[0114] $C_3=C_2+H_2(P_3,I_3,*_3)P_3$

[0115] $B=C_{m+1}$

[0116] $=C_m+H_m(P_{m+1},I_{m+1},*_{m+1})P_{m+1}$

[0117] 在一些实例中，证书机构(包括根证书机构或者从属证书机构)能够编码隐式证书内的任何额外需要的信息，但是如果一方不隐含信任该证书机构，则其可以向上前进直到到达可信的证书机构或者信赖方。该信任模型可以是“传递性的”，因为一方可以信任这样的实体，该实体据推测检查了链的上级部分，并且该实体继而可能不是已经独立检查到高达直接可信的(根或者中间)证书机构，而是已经检查到可信的某个其他实体，该某个其他实体已经检查(或者信任)链的更前的部分。作为这种额外信息的示例，证书机构可以对与链中上级的隐式证书对应的信息进行编码。如果某个证书机构被某个信赖方信任，则这种额外信息可以节省带宽和通信。作为示例，在上述第二示例对策方案中，其包括下述公式：

[0118] $C_1=C+H(P_1,I_1,*_1)P_1=C+H_1P_1$

[0119] $C_2=C_1+H(H(P_1,I_1,*_1),P_2,I_2,*_2)P_2$

[0120] $=C_1+H(H_1,P_2,I_2,*_2)P_2=C_1+H_2P_2$

[0121] $C_3=C_2+H(H(H(P_1,I_1,*_1),P_2,I_2,*_2),P_3,I_3,*_3)P_3$

[0122] $=C_2+H(H_2,P_3,I_3,*_3)P_3=C_2+H_3P_3$

[0123] $B=C_{m+1}$

[0124] $=C_m+H(H_m,P_{m+1},I_{m+1},*_{m+1})P_{m+1}=C_m+H_{m+1}P_{m+1}$

[0125] 一些子证书机构C_j(其中$j=1\cdots,m$)可以在$*_{j-1}$内编码H_{j-1}。如果信赖方不直接信任子证书机构C_j，则该信赖方可以查找对H_{j-1}的独立确认，如通过与较前的证书机构通信，以其他方式获取教前的隐式证书和/或散列函数输出值。

[0126] 前面概述的五个示例对策以及其他示例对策中的任何一个可被修改或适配。更一般地，可以基于函数F，根据下述等式来生成ECQV隐式证书方案的第1个公钥：

[0127] $C_1=C_{1-1}+F(C,C_1,\ldots,C_{1-1},P_1,\ldots,P_1,I_1,\ldots,I_1,*_1,\ldots,*_1)P_1.$ (1a)

其中F是输出整数的某个函数。例如，函数F可以是散列函数、包括散列函数、调用散列函数、或者以其他方式使用散列函数。类似地，可以基于函数F，根据下述等式来生成OMC隐式证书方案的第1个公钥：

[0128] $C_1=P_1+F(C,C_1,.,C_{1-1},P_1,.,P_1,I_1,.,I_1,*_1,.,*_1)C_{1-1}$。

[0129] 图3是示例密码系统300的示意图，该密码系统300实现基于隐式证书的数字签名方案。该密码系统300包括：终端模块302、306；证书机构模块304；以及可能的附加特征。例如，密码系统300可以包括一个或更多个附加的证书机构模块310。密码系统300可以包括附加的或不同的组件。终端模块302、306均可以是由一个或更多个终端实现的计算机程序模块。例如，终端模块302可以由图1中的终端102或者图2中的终端202来实现；以及终端模块306可以由图1中的终端106或者图2中的终端206来实现。

[0130] 证书机构模块304可以是由一个或更多个证书机构服务器实现的计算机程序模块。例如，证书机构模块304可以由图1的证书机构服务器104或者图2的证书机构服务器204a、204b、204x中的任一个来实现。在一些实例中，证书机构模块304可操作用于执行从属证书机构的操作，以及附加的证书机构模块310可操作用于执行根证书机构和可能的一个或更多个中间证书机构的操作。在一些实例中，证书机构模块304可操作用于执行根证书机

构或者中间证书机构的操作。

[0131] 终端模块302、306和证书机构模块304可以由附加的或不同类型的硬件系统来实现。例如，证书机构模块304(或者在一些实例中证书机构模块304的各个模块、数据或者其他方面)可被卸载到非证书机构设备。在一些实例中，例如在对等计算环境中，服务器功能可以分布在客户端设备上。作为另一示例，终端模块(或者在一些实例中，终端模块的各个模块、数据或其他方面)可配备在服务器设备上，如证书机构服务器或者其他类型的服务器。

[0132] 终端模块302、306和证书机构模块304可以例如通过数据网络或者其他类型的通信链路相互通信。在一些实现中，终端模块302、306和证书机构模块304可以通过在图1的数据网络108或图2的数据网络208上发送的消息而相互通信。在图3示出的示例中，终端模块302可以向证书机构模块304发送证书请求320。证书机构模块304可以从终端模块302接受该证书请求320，以及响应于该证书请求320向终端模块302发送隐式证书322。证书机构模块304还可以向终端模块302发送私钥分发数据。可以将该私钥分发数据与隐式证书322一起或者分开地发送给终端模块302。证书机构模块304还可以例如向证书数据库发布隐式证书322。终端模块302可以从证书机构模块304接收隐式证书322，以及向终端模块306发送签名消息324。终端模块306可以从终端模块302接收签名消息324和隐式证书322。在一些实例中，终端模块306可以从其他源取回隐式证书322。密码系统300可以支持附加的或不同类型的通信。

[0133] 密码系统300使用允许终端模块验证从其他终端模块接收的消息的真实性的隐式证书方案。根据该隐式证书方案，证书机构颁发的隐式证书将每个用户实体的标识与特定的公钥值捆绑在一起。用户实体可以基于用户实体的私钥来生成数字签名，并且其他用户能够基于用户实体的公钥验证该数字签名。隐式证书方案可以基于任何合适类型的群来实现。例如，ECQV隐式证书方案以及其他隐式证书方案可以使用椭圆曲线上的点的群、有限域中的乘法群、或者离散对数问题在其中可能是困难的其他群来实现。基于椭圆曲线的数字签名方案的示例包括ECDSA(椭圆曲线数字签名算法)、ECPV签名以及ECNR(椭圆曲线Nyberg Rueppel)。可以使用附加的或不同的类型的隐式证书方案，如OMC方案。

[0134] 当终端模块302对消息M_0签名时，针对消息M_0的签名可以基于M来生成，该M是消息的M_0的修改版本。可以通过将消息M_0与附加信息组合来形成修改后的消息M。例如，可以通过将消息M_0与后缀、前缀或者其与其他附加物的组合进行级联来形成消息M。与消息M_0组合的信息可以包括用于验证消息的公钥、用于验证消息的公钥的一些部分、用于验证消息的公钥的函数、或者其他信息。在一些实现中，与消息M_0组合的信息包括签名者的隐式证书或者签名者的隐式证书的一些部分或函数。在一些实现中，与M_0组合的信息包括证书机构的公钥、证书机构的公钥重构值、或者与证书机构关联的其他信息。

[0135] 相应地，为了对消息M_0进行签名，终端模块302根据消息M_0生成修改后的消息M。例如，可以根据下式生成修改后的消息M：

[0136] $M=F_1(M_0,F_2(P,I,[C],*))$，

[0137] 其中F_1和F_2是某些函数。函数F_2可以是散列函数或者其他类型的函数。例如，函数F_2可以基于值P，I，[C]，*中的一个或更多个来生成整数值。作为示例，函数F_2可以基于值P，I生成整数值。在一些示例中，函数F_2可以使用一个或更多个SHA散列函数族。作为另一示例，

函数F_2可以将一列输入进行级联(例如,通过搅乱顺序、对输入应用可逆变换、或者以其他方式混合输入),并且输出单个值。函数F_1可以是附加函数或者组合输入值的其他类型的函数。例如,函数F_1可以将函数F_2的输出作为前缀、后缀或者其与一个或更多个其他类型的附加物的组合附加到消息M_0。作为另一示例,作为补充或备选,函数F_1可以应用可逆变换,如字符编码或者数据压缩。修改后的消息M可被用在签名函数中。签名函数可以基于修改后的消息M、签名者的私钥和隐式证书生成数字签名。

[0138] 接收者可以接收签名消息,并且使用签名者的公钥来根据数字签名恢复修改后的消息M。在一些实例中,签名消息包括原始消息M_0和基于M的数字签名。在这种实例中,接收者可以基于消息M_0和发送者用于生成修改后的消息M的公钥信息来生成修改后的消息M。在一些实例中,签名消息包括修改后的消息M和基于修改后的M的数字签名。在这种实例中,接收者可以基于修改后的消息M和发送者用于生成修改后的消息M的公钥信息来生成原始消息M_0。

[0139] 在图3示出的示例中,隐式地认证用于验证签名者的数字签名的公钥。在一些实例中,可以将基于已经根据公钥(或者与公钥有关的信息)修改的修改后的消息M生成数字签名,而不是基于原始消息M_0来生成数字签名当做对策,以降低伪造攻击的成功可能性。例如,在一些实例中,该对策可以降低某些类型的链式攻击或者涉及生日问题的其他类型的攻击的可能性。在一些实例中,该对策可被用作针对不涉及生日问题的攻击的对策。例如,该技术可以防止对ECDSA与ECQV的组合以及ECDSA与OMC的组合的一些类型的攻击。

[0140] 终端模块302包括修改模块344、签名生成模块342、请求生成模块340、以及可能的其他模块。请求生成模块340可以生成证书请求320。证书请求320可以包括特定用户实体的标识I。证书请求320可以包括椭圆曲线点R_U。证书请求320可以包括附加的或不同的信息。标识值I可以是特定用户实体、特定设备、或者这二者的唯一标识符。请求生成模块340可以通过选择随机数k_U以及计算$R_U=k_UG$来生成椭圆曲线点R_U。例如,终端模块302可以具有生成随机数的随机数生成器模块。

[0141] 修改模块344可以使用来自隐式证书322和消息318的数据或者与隐式证书322和消息318有关的数据,以生成修改后的消息319。消息318可以包括任何类型的电子文档、数据文件、数据对象、或者其他格式的信息。在一些实例中,消息318是电子邮件消息、电子文档、或者可以由合适的软件应用编辑和生成的电子数据文件。在一些实例中,消息318是在硬件组件之间的信令应用中使用的数据消息或者数据消息的组合。例如,在智能能量基础架构中,消息318可以包括来自智能能量表的状态信息。

[0142] 修改模块344可以基于消息318和附加信息生成修改后的消息319。附加信息可以包括隐式证书322或者从隐式证书322中提取的或者以其他方式导出的数据(例如,公钥重构值P、标识值I、或者这些和其他数据的组合)。附加信息可以包括证书机构公钥信息。例如,附加信息可以包括证书机构的公钥C、任何根证书机构的公钥、任何从属证书机构的公钥、或者它们的任意组合。附加信息可以包括证书机构的隐式证书或者从任何证书机构的隐式证书导出的信息。例如,附加信息可以包括链中的任何从属证书机构或它们的组合的隐式证书。可以由修改模块344通过组合附加信息与消息318来生成修改后的消息319。例如,附加信息可被附着到消息318、与消息318混合、或者以其他方式与消息318组合在一起。

[0143] 签名生成模块342可以使用隐式证书322来基于修改后的消息319生成数字签名。

用于生成数字签名的示例技术包括ECPV签名方案、基于密钥的ECPV签名方案、Schnorr签名方案、ECDSA等等。签名生成模块342可以使用终端模块302的私钥和隐式证书322来生成数字签名。签名生成模块342可以基于私钥分发数据r、隐式证书322和用于生成证书请求320的随机值k_U来生成终端模块302的私钥。签名生成模块342生成的数字签名可被附着到消息318或修改后的消息319、与消息318或修改后的消息319混合、或者以其他方式与消息318或修改后的消息319组合在一起，以创建签名消息324。数字签名可以与消息318分开发送。终端模块302可以向终端模块306发送隐式证书322。

[0144] 终端模块306包括修改模块352、签名验证模块350、以及可能的其他模块。签名验证模块350可以验证与签名消息324关联的数字签名。用于基于公钥来解码数字签名的示例技术包括ECPV签名方案、基于密钥的ECPV签名方案、Schnorr签名方案、ECDSA等等。签名消息324包括据称由与标识值I关联的用户实体生成的数字签名。签名验证模块350可以从终端模块306接收隐式证书322，或者从其他源取回与标识值I关联的隐式证书322。签名验证模块350可以基于任何适合的信息(如根据隐式证书322中的公钥重构数据重构的公钥)来生成修改后的消息319。例如，签名验证模块350可以基于公钥重构数据P、隐式证书322和证书机构的公钥C来计算公钥B。

[0145] 在图3的示例中，签名验证模块350接收作为签名消息324的一部分的消息318。签名验证模块350可以从签名消息324中提取消息318，并且将消息318提供给修改模块352。修改模块352可以基于消息318和被修改模块344用于生成修改后的消息319的附加信息，生成修改后的消息319。终端模块306可以将修改模块352生成的修改后的消息319与使用数字签名验证的修改后的消息319进行比较。终端模块可以验证签名消息324的真实性，例如，两个修改后的消息319是否匹配。可以通过附加的或者不同的技术来验证签名消息。例如，在一些实例中，签名消息324包含修改后的消息319而不是原始消息318。在该实例中，可以部分地基于例如使用签名者的公钥信息从修改后的消息319生成原始消息318来验证签名消息。

[0146] 证书机构模块304包括证书生成模块330以及可能的其他模块。证书机构模块304可以执行用于颁发供在密码系统300中使用的隐式证书322的一个或更多个操作。证书生成模块330可以例如响应于接收到证书请求320，生成隐式证书322。

[0147] 证书生成模块330基于证书请求320中的信息生成隐式证书。例如，证书生成模块330可以选择随机值k，并且通过计算$P=R_U+kG$生成公钥重构数据P，其中R_U是请求生成模块340生成的椭圆曲线点，且被包含在证书请求320中。证书机构模块304可以具有生成随机数的随机数生成器模块。证书生成模块330可以将公钥重构数据P编码到隐式证书$Cert_U$中，以及有时还将其他信息编码到隐式证书$Cert_U$中。隐式证书$Cert_U$可以通过证书编码方案来生成，如固定长度字段方案、最小ASN.1编码方案、兼容X.509的ASN.1编码方案，或者其他方案。

[0148] 在一些实例中，证书机构模块304中的证书验证模块可以接收证书生成模块330生成的信息，并且验证隐式证书$Cert_U$服从安全规则和设置。如果隐式证书$Cert_U$被认可，则隐式证书$Cert_U$可被发布为隐式证书322。如果隐式证书$Cert_U$没被认可，则可以由证书生成模块330生成和验证新的隐式证书$Cert'_U$。

[0149] 图4是示出用于执行密码系统中的操作的实例处理400的流程图。处理400可以由证书机构、对应机构(correspondent)、或者密码系统的这些实体和其他实体的任何合适的

组合来实现。在一些实例中，处理400可以由图3中示出的终端模块302、306或者证书机构模块304来实现。处理400可以包括由计算系统执行的操作。例如，操作可以由图1和图2中示出的终端或者证书机构服务器执行。图4中示出的实例400可以使用附加的、更少的、或者不同的操作来实现，其可以按照示出的顺序或者按照不同的顺序来执行。在一些实现中，操作中的一个或更多个操作可以重复或迭代，例如直到达到终止条件为止。

[0150] 在步骤410，访问隐式证书。例如可以通过下述方式来访问隐式证书：从存储器读取隐式证书，从远程源接收隐式证书，根据其他数据生成隐式证书，或者以其他方式来访问隐式证书。隐式证书可以是证书机构生成的隐式证书。该证书机构可以是任何合适的证书机构，如根证书机构、中间证书机构、或者任意从属证书机构。

[0151] 隐式证书与实体相关联。例如，隐式证书可以与用户、终端、位置、软件模块等相关联。实体可以是证书机构服务器、对应终端、或者任何合适的设备或系统组件。在一些实例中，生成隐式证书的证书机构是根证书机构或者中间证书机构，以及实体是对应机构或者从属于根证书机构的另一证书机构。隐式证书可以基于隐式证书链。例如，当生成隐式证书的证书机构是中间证书机构或其他从属证书机构时，隐式证书可以基于上级证书机构颁发的一个或更多个其他隐式证书。实体的隐式证书可以包括实体的标识符、实体的公钥重构值、或者这些和其他信息的任意合适组合。

[0152] 在步骤420，访问证书机构公钥信息。例如可以通过下述方式访问证书机构公钥信息：从存储器读取该信息，从远程对应机构接收该信息，根据其他数据生成该信息，或者以其他方式来访问该信息。在一些实例中，证书机构公钥信息包括：颁发在步骤410处访问的隐式证书的证书机构的公钥值、颁发在步骤410处访问的隐式证书的证书机构的公钥重构值、另一证书机构公钥信息、或者这些信息和其他信息的组合。

[0153] 在步骤430，对散列函数求值。可以使用任意合适的散列函数。散列函数的示例包括SHA散列函数族(SHA-1，SHA-256，等等)以及其他散列函数。可以由任意合适的数据处理装置来对散列函数求值。例如，可以由通用处理器、主处理器、专用处理器、或者一个或更多个处理器的任意合适组合来对散列函数求值。对散列函数求值可以产生散列值。

[0154] 可以基于证书机构公钥信息和实体的公钥重构值对散列函数求值。在一些实例中，可以基于证书机构的公钥、证书机构的公钥重构值、或者这些和任意其他证书机构公钥信息的组合来对散列函数求值。散列函数可以采用任意合适的输入组合。在一些示例中，散列函数可以表达为$H(P_1,I_1,P_2,I_2)$，其中P_1表示证书机构的公钥重构值，I_1表示证书机构的标识符，P_2表示实体的公钥重构值，以及I_2表示实体的标识符。作为另一示例，散列函数可被表达为散列链$H(H(P_1,I_1),P_2,I_2)$。作为另一示例，散列函数可被表达为$H(C_1,P_2,I_2)$，其中C_1表示证书机构的公钥值。

[0155] 在一些实现中，散列函数的求值基于多个证书机构公钥信息。例如，在实体的隐式证书是由从属证书机构生成的实例中，可以基于从属证书机构公钥信息以及上级证书机构(如根证书机构或者中间证书机构)的公钥信息对散列函数求值。在一些实例中，散列函数可以表达为$H(P_1,I_1,P_2,I_2,P_3,I_3)$，其中$P_2$表示从属证书机构的公钥重构值，$I_2$表示从属证书机构的标识符，$P_1$表示上级证书机构的公钥重构值，$I_1$表示上级证书机构的标识符，$P_3$表示实体的公钥重构值，以及$I_3$表示实体的标识符。在一些实例中，散列函数可以表达为散列链$H(H(H(p_1,I_1),P_2,I_2),P_3,I_3)$。

[0156] 在步骤440，执行加密操作。可以基于在步骤430处散列函数产生的散列值来执行加密操作。例如，加密操作可以使用散列值、根据散列值导出的或计算出的值、或者这些和其他输入的任意合适组合。根据需要，可以基于附加的或不同的信息执行加密操作。

[0157] 加密操作可以包括在密码系统中执行的任意合适的操作。例如，加密操作可以是下述协议的一部分或者可以与下述协议关联地执行：数据认证协议、数据安全协议、证书生成协议、或者其他类型的协议。在一些实例中，加密操作可以是下述算法的一部分或者可以产生下述算法使用的信息：加密算法、解密算法、数字签名生成算法、数字签名验证算法、或者其他类型的算法。加密操作可以产生任意合适的输出。一些加密操作可以产生实体的公钥、数字签名、对数字签名的验证、加密消息、解密消息、或者其他类型的输出。

[0158] 作为示例，加密操作可以包括生成实体的公钥值。可以基于步骤430中散列函数产生的散列值来生成该公钥值，或者可以基于根据散列值计算的或导出的其他值来生成该公钥值。在一些实例中，可以作为下述操作的一部分来生成实体的公钥值：使公钥值生效、验证据称由实体产生的数字签名、解密来自实体的消息、或者其他加密操作。在一些实例中，生成公钥值产生公钥值来作为输出值，该输出值可被存储、删除、发送、在其他计算中使用等等。

[0159] 在一些实例中，可以例如通过对使用或以其他方式依赖公钥值的密码函数求值来生成公钥值。密码函数可以接收公钥值作为输入。在一些实例中，密码函数接收可被用于计算公钥值的值作为输入，并且密码函数可以使用这些输入值来例如以数学上等价的方式替代实际的公钥值。如此，密码函数可以使用公钥值，而不需要显式地接收公钥值作为输入。相应地，在一些实例中，对使用或以其他方式依赖公钥值的密码函数求值时不显式计算公钥值。

[0160] 图5是示出用于使用数字签名的示例处理500的流程图。处理500可以由证书机构、对应机构、或者密码系统的这些实体和其他实体的任何合适的组合来实现。在一些实例中，处理500的方面可以由图3中示出的终端模块302、306或者证书机构模块304、或者它们的组合来实现。处理500可以包括由通信系统中的多个实体执行的操作。例如，操作可以由图1和图2中示出的一个或更多个终端或者证书机构服务器或者它们的组合来执行。图5中示出的实例500可以使用附加的、更少的、或者不同的操作来实现，其可以按照示出的顺序或者按照不同的顺序来执行。在一些实现中，操作中的一个或更多个操作可以重复或迭代，例如直到达到终止条件为止。

[0161] 图5示出了证书机构502、发送者504和验证者506执行的操作。作为示例，证书机构502的操作可以由证书机构服务器执行，发送者504的操作可以由第一终端执行，以及验证者506的操作可以由第二终端执行。在一些实例中，附加的或不同的组件或者计算装置可以执行示例处理500的一个或更多个操作。

[0162] 在步骤510，证书机构502生成数字证书。证书机构502可以是任意合适的证书机构(例如，根证书机构、从属证书机构等等)。数字证书可以是隐式证书、显式证书、或者任意其他类型的数字证书。数字证书可以包括实体的公钥重构值、实体的标识符、或者这些或其他信息的任意合适组合。在图5示出的示例处理500中，证书机构502生成的数字证书包括发送者504的公钥重构值。

[0163] 在步骤512，数字证书被传送给发送者504。可以以任意合适的方式传送数字证书。

例如，数字证书可以通过数据通信网络传送、通过无线或有线通信链路发送、在盘上或者其他计算机可读介质上运送、或者以任意合适组合来传送。在图5示出的示例中，发送者504从证书机构502接收数字证书。

[0164] 在步骤514，发送者504修改要被签名的消息。该消息可以基于数字证书进行修改。发送者504可以例如通过下述方式访问数字证书和消息：从存储器读取它们中的一个或更多个，从远程设备接收它们中的一个或更多个，本地生成它们中的一个或更多个，或者通过用于访问数据的这些和其他技术的任意合适组合。

[0165] 可以通过任意合适技术生成第一修改后的消息。发送者504可以通过下述方式生成该第一修改后的消息：基于发送者的数字证书生成散列值，以及将散列值与消息进行组合。发送者504可以通过将消息与发送者的公钥重构值进行组合来生成第一修改后的消息。发送者504可以通过将消息与其他值组合来生成该第一修改后的消息。所述其他值可以基于签名者的数字证书中的信息以及可能的其他信息。例如，所述其他值可以根据签名者的公钥重构值、签名者的公钥值、签名者的标识符、数字证书中包括的其他信息或者任意合适组合而产生。

[0166] 在一些实例中，第一修改后的消息是通过将消息与证书机构的公钥信息进行组合来生成的。例如，第一修改后的消息可以基于签名者的数字证书和证书机构的公钥二者来生成。当证书机构502从属于另一证书机构(如，根证书机构、中间证书机构等)时，第一修改后的消息可以通过将消息与根据签名者的公钥重构值和一个或更多个其他值产生的值进行组合来生成。所述其他值可以例如包括：证书机构502的公钥、上级证书机构的公钥、证书机构502的数字证书、上级证书机构的数字证书，等等。

[0167] 在步骤516，发送者504生成数字签名。可以基于修改后的消息生成数字签名。在一些实例中，可以基于附加的或不同的信息来生成数字签名。可以根据任意合适的签名算法或其他合适的技术来生成数字签名。

[0168] 在步骤518，数字签名和其他信息被传送给验证者506。在一些实例中，传送给验证者506的信息包括消息(例如，未修改的消息)。在一些实例中，传送给验证者506的信息包括第一修改后的消息。在任意情况中，数字签名可以与其他信息一起传送，或者数字签名可以单独传送。在一些实例中，发送者504还向验证者506发送发送者的数字证书，或者验证者506可以从其他源获取发送者的数字证书。从发送者504向验证者506传送的信息可以以任意合适的方式传送。例如，该信息可以通过数据通信网络传送、通过无线或有线通信链路发送、在盘上或者其他计算机可读介质上运送、或者以任意合适组合来传送。在图5示出的示例中，验证者506从发送者504接收该信息。

[0169] 验证者506可以直接从发送者504获取消息(例如，未修改的消息)，或者验证者506可以根据发送者504提供的其他信息导出该消息。在一些实现中，在步骤518，发送者向验证者506传送第一修改后的消息，并且验证者506从第一修改后的消息中提取原始的未修改的消息。验证者506可以以任意合适的方式获取原始的未修改的消息。

[0170] 在步骤520，验证者506访问该原始的未修改的消息，并且修改该消息。可以基于发送者的数字证书中包含的信息来修改该消息。验证者506可以例如通过下述方式访问数字证书和消息：从存储器读取它们中的一个或更多个，从远程设备接收它们中的一个或更多个，本地生成它们中的一个或更多个，或者通过用于访问数据的这些和其他技术的任意合

适组合。当验证者506修改该消息时，验证者506产生第二修改后的消息。

[0171] 可以通过任意合适技术生成第二修改后的消息。在图5示出的示例处理500中，在步骤520中，验证者506以与在步骤514处发送者504修改消息的相同方式来修改消息。例如，发送者504和验证者506均能够根据预定的或者预先布置的算法来修改消息。如此，步骤520中由验证者506产生的第二修改后的消息可以与步骤514中发送者504产生的第一修改后的消息相同。

[0172] 在一些实现中，验证者506通过下述方式生成该第二修改后的消息：基于发送者的数字证书生成散列值，以及将散列值与消息进行组合。验证者506可以通过将消息与发送者的公钥重构值进行组合来生成第二修改后的消息。验证者506可以通过将消息与其他值组合来生成该第二修改后的消息。所述其他值可以基于签名者的数字证书中的信息以及可能的其他信息。例如，可以根据签名者的公钥重构值、签名者的公钥值、签名者的标识符、数字证书中包括的其他信息或者任意合适组合来产生所述其他值。

[0173] 在一些实现中，第二修改后的消息是通过将消息与证书机构公钥信息进行组合来生成的。例如，可以基于签名者的数字证书和证书机构的公钥二者来生成第二修改后的消息。当证书机构502从属于另一证书机构时，第二修改后的消息可以通过将消息与根据签名者的公钥重构值和一个或更多个其他值产生的值进行组合来生成。所述其他值可以例如包括：证书机构502的公钥、上级证书机构的公钥、证书机构502的数字证书、上级证书机构的数字证书，等等。

[0174] 在步骤522，验证者506验证消息。该消息是基于发送者504在步骤516中生成的数字签名以及验证者506在步骤520中生成的第二修改后的消息来验证的。在一些实例中，可以基于附加的或不同的信息来验证消息。可以部分地基于任意合适的签名验证算法或者其他合适的技术来验证消息。对消息进行验证可以向验证者506提供对消息真实性的保证。例如，成功地验证消息可以指示消息是来自发送者504的真实通信，并且没有被篡改或伪造。

[0175] 在一些方面，验证者506使用数字签名来验证发送者504产生的第一修改后的消息，然后验证者506将第一修改后的消息与第二修改后的消息进行比较。在一些实例中，基于数字证书，根据与发送者在步骤516中生成数字签名所使用的数字签名算法对应的验证算法，来验证第一修改后的消息。如果基于数字签名可以验证第一修改后的消息，以及如果第一修改后的消息与第二修改后的消息匹配，则验证者506可以接受该消息(即，未修改的消息)是真实的。如果基于数字签名不能验证第一修改后的消息，或者如果第一修改后的消息与第二修改后的消息不匹配，则验证者506可以因为不可信而拒绝该消息。

[0176] 本说明书中描述的主题和操作中的一些可被实现在数字电子电路中，或者实现在计算机软件、固件或硬件中，其包括本说明书中公开的结构及其等价结构或者它们中的一个或更多个的组合。本说明书中描述的主题和操作中的一些可以实现为嵌入在非瞬时计算机存储介质上的一个或更多个计算机程序(即，一个或更多个计算机程序指令模块)，用于由数据处理装置执行或者控制数据处理装置的操作。作为备选或补充，程序指令可被编码以传输给合适的接收机装置，用于由数据处理装置执行。计算机存储介质可以是下述设备中，或者可以包含在下述设备中：计算机可读存储设备、计算机可读存储、随机或串行存取存储器阵列或器件、或者它们中的一个或更多个的组合。而且，尽管计算机存储介质不是传播信息，但是计算机存储介质可以是编码在人工生成的传播信号中的计算机程序指令的源

或目的地。计算机存储介质还可以是一个或更多个单独的物理组件或介质(例如,多个卡、盘或者其他存储器件),或者可被包括在一个或更多个单独的物理组件或介质(例如,多个卡、盘或者其他存储器件)中。

[0177] 本说明书中描述的操作可被实现为由数据处理装置对一个或更多个计算机可读存储设备上存储的数据或者从其他源接收的数据执行的操作。属于"数据处理装置"包括用于处理数据的所有种类的装置、设备和机器,作为示例,其包括可编程处理器、计算机、片上系统、或者前述装置中的多个或其组合。该装置可以包括专用逻辑电路,如FPGA(现场可编程门阵列)或者ASIC(专用集成电路)。除了硬件之外,该装置还可以包括创建所关注的计算机程序的执行环境的代码,所述代码例如是构建处理器固件、协议栈、数据库关联系统、操作系统、跨平台运行时环境、虚拟机、或者它们中的一个或更多个的组合的代码。该装置和执行环境可以实现各种不同的计算模型基础设施,如网站、分布式计算和网格计算基础设施。

[0178] 计算机程序(也称为程序、软件、软件应用、脚本、或者代码)可以以任何形式的编程语言来编写,包括汇编或解释语言、声明或过程语言,并且其可以以任何形式进行部署,包括部署为独立程序、或者部署为模块、组件、子例程、对象或适合于在计算环境中使用的其他单元。计算机程序可以与文件系统中的文件对应,但这不是必须的。程序可被存储在保存其他程序或数据(如,在标记语言文档中存储的一个或更多个脚本)的文件的一部分中,存储在专用于所讨论的程序的单个文件中,或者存储在多个协作文件(如,存储一个或更多个模块、子程序或者代码部分)中。计算机程序可被部署,以在一个计算设备上,或者在位于一个地点的或分布在多个地点且通过通信网络互联的多个计算机上执行。

[0179] 在本说明书中描述的处理和逻辑流程可以由一个或多个可编程处理器来执行,该一个或多个可编程处理器执行一个或多个计算机程序以通过操作输入数据和生成输出来执行动作。该处理和逻辑流程还可以通过执行专用逻辑电路,如FPGA(现场可编程门阵列)或ASIC(专用集成电路)来执行,并且装置可被实现为所述专用逻辑电路。作为示例,适合于计算机程序的执行的处理器包括通用和专用微处理器以及任何类型的数字计算设备中的任何一个或多个处理器。一般而言,处理器将从只读存储器或随机存取存储器或两者接收指令和数据。计算设备的基本元件是用于根据指令执行动作的处理器以及一个或多个用于存储指令和数据的存储器设备。通常,计算设备还包括用于存储数据的一个或多个存储设备,或者可操作地耦合以从用于存储数据的一个或多个存储设备接收数据和/或将数据传送到给用于存储数据的一个或多个存储设备。然而,计算设备不是必须具有这样的设备。此外,计算机可被嵌入到另一个设备,如移动电话、个人数字助理(PDA)、移动音频或视频播放器、游戏控制台、全球定位系统(GPS)接收器、或便携式存储设备(如通用串行总线(USB)闪存驱动器),这仅是举出几例。适于存储计算机程序指令和数据的设备包括所有形式的非易失性存储器、介质和存储器设备,例如包括:半导体存储器设备,如EPROM、EEPROM和闪存设备;磁盘,如内部硬盘或可移动磁盘;磁光盘;以及CD-ROM和DVD-ROM盘。处理器和存储器可被补充专用逻辑电路或者集成在专用逻辑电路中。为了提供与用户的交互,在本说明书中描述的主题可被实现在具有显示设备以及键盘和指示设备的计算机上,该显式设备用于向用户显示信息,例如是LCD(液晶显示器)屏幕,该键盘和指示设备例如是触摸屏、触笔、鼠标等,通过其用户可以向计算机提供输入。其他种类的设备也可被用于提供与用户的交互,例

如，提供给用户的反馈可以是任何形式的感官反馈，如视觉反馈、听觉反馈或触觉反馈；以及，来自用户的输入可以以任何形式接收，包括声音、语音或触觉输入。另外，计算设备可以通过向用户使用的设备发送文档以及从其接收文档来与用户进行交互；例如，通过响应于接收自Web浏览器的请求向用户的客户端设备上的Web浏览器发送网页。

[0180] 在本说明书中描述的主题中的一些主题可被实现在包括下述计算系统中，所述计算系统包括后端组件(如，作为数据服务器)，或者包括中间件组件(如应用服务器)，或者包括前端组件(如，具有通过其用户可以与本说明书中描述的主题的实现进行交互的图形用户界面或Web浏览器的客户端计算设备)，或者一个或多个这种后端、中间件或前端组件的任意组合。该系统的组件可以通过任何形式或介质的数字数据通信(如，数据网络)进行互连。该计算系统可以包括客户端和服务器。客户端和服务器通常彼此远离，并且典型地通过数据网络进行交互。客户端和服务器的关系是凭借在各自计算机上运行的并且彼此具有客户端-服务器关系的计算机程序而产生。在一些实现中，服务器向客户端设备发送数据。可以在服务器处从客户端设备接收在客户端设备上生成的数据。

[0181] 尽管本说明书包含众多具体的实现细节，但是这些不应被解释为对所要求保护的范围的限制，而是作为对特定实施方式的具体特征的描述。在本说明书中在不同实施方案的上下文中描述的某些特征也可以在单个实施方案中组合实现。反之，在单个实施方案的上下文中描述的各种特征也可以在多个实施方案中单独地或以任何合适的子组合进行实现。而且，尽管可能在上文将特征描述为以特定组合行动，甚至最初也是如此要求的，但是来自所要求保护的组合的一个或多个特征在一些情况下可以从组合中删去，并且所要求保护的组合可以针对子组合或子组合的变形。类似地，尽管在附图中以特定的顺序示出操作，但是这不应当被解释为：为了实现期望的结果，需要以所示的特定顺序或以连续顺序来执行这些操作，或者需要完成所有图示的操作。在某些情况下，多任务和并行处理可能是有利的。此外，在上述的实施方式中的各种系统组件的分离不应被理解为在所有实施方式中都要求这样的分离，而是应该理解为，所描述的程序组件和系统通常可以集成在单个软件产品中或者可以封装成多个软件产品。在一些方面，访问隐式证书。所述隐式证书与实体相关联，并且由证书机构生成。所述隐式证书包括所述实体的公钥重构值。访问与证书机构关联的证书机构公钥信息。基于对散列函数求值来生成第一值。所述散列函数的求值基于所述证书机构公钥信息和所述实体的公钥重构值。可以基于所述第一值生成所述实体的公钥值。这些和其它方面的实现可以包括以下特征中的一个或多个。所述证书机构是根证书机构，并且所述实体是从属于所述根证书机构的第二证书机构。所述证书机构是从属于根证书机构的中间证书机构，以及所述实体是从属于所述中间证书机构的第二证书机构。所述隐式证书基于隐式证书链。所述证书机构是根证书机构，以及所述实体是用户实体。

[0182] 作为补充或备选，这些和其他方面的实现可以包括以下特征中的一个或多个。生成所述公钥值包括：使所述公钥值生效，使用所述公钥值来验证来自所述实体的数字签名，或者这二者。生成所述公钥值包括：作为对使用公钥值的密码函数求值的一部分，隐式生成所述公钥值。生成所述公钥值或者对所述密码函数求值可以显式计算所述公钥值，也可以不显式计算所述公钥值。

[0183] 作为补充或备选，这些和其他方面的实现可以包括以下特征中的一个或多个。所述第一值和所述公钥值是由所述实体生成的。所述第一值和所述公钥值是由所述证书机构

生成的。所述第一值和所述公钥值是由依赖所述公钥值的不同的第二实体生成的。所述证书机构公钥信息包括所述证书机构的公钥值、所述证书机构的公钥重构值，或者这两者。

[0184] 作为补充或备选，这些和其他方面的实现可以包括以下特征中的一个或多个。所述证书机构是从属证书机构。访问附加的与根证书机构关联的证书机构公钥信息。所述第一值是基于根据下述信息对散列值求值而生成的：从属证书机构的证书机构公钥信息、根证书机构的附加证书机构公钥信息、以及实体的公钥重构值。

[0185] 在一些方面，访问与实体关联的隐式证书。所述隐式证书包括所述实体的公钥重构值。访问用于由所述实体进行数字签名的消息。通过将所述消息与基于所述隐式证书的值进行组合来生成修改后的消息。数字签名是基于所述修改后的消息生成的。

[0186] 在一些方面，访问实体生成的数字签名。访问要基于所述数字签名验证的消息。访问与所述实体关联的隐式证书。通过将所述消息与基于所述隐式证书的值进行组合来生成修改后的消息。基于所述数字签名和所述修改后的消息来验证所述消息。

[0187] 这些和其他方面的实现可以包括以下特征中的一个或多个。所述修改后的消息是通过下述方式生成的：基于所述实体的隐式证书生成散列值，以及将所述散列值与所述消息进行组合。通过数据通信网络将所述消息和所述数字签名发送给接收者。所述修改后的消息是通过将所述消息与所述实体的公钥重构值进行组合来生成的。所述修改后的消息是通过将所述消息与基于所述实体的公钥重构值和所述隐式证书中的附加信息的值进行组合生成的。

[0188] 作为补充或备选，这些和其他方面的实现可以包括以下特征中的一个或多个。访问所述隐式证书包括：访问证书机构颁发的隐式证书。所述修改后的消息是通过将所述消息与基于所述证书机构的隐式证书和公钥值的值进行组合而生成的。访问所述隐式证书包括：访问从属于第二证书机构的第一证书机构颁发的隐式证书，所述修改后的消息是通过将所述消息与基于所述实体的公钥重构值和一个或更多个其他值的值进行组合而生成的。所述其他值包括所述第一证书机构的公钥、所述第二证书机构的公钥、所述第一证书机构的隐式证书、所述第二证书机构的隐式证书、或其组合。

[0189] 作为补充或备选，这些和其他方面的实现可以包括以下特征中的一个或多个。验证者通过数据通信网络从所述实体接收第一修改后的消息。通过将所述消息与基于所述隐式证书的值进行组合而生成的修改后的消息是第二修改后的消息。验证所述消息包括：使用所述数字签名，根据验证算法验证所述第一修改后的消息。验证所述消息包括：将所述第一修改后的消息与所述第二修改后的消息进行比较。访问所述消息包括根据所述第一修改后的消息导出所述消息。

[0190] 因此，已经描述了所述主题的实施方式。其他实施方式在所附权利要求的范围内。在一些实例中，权利要求中记载的动作是以不同顺序执行的，并且仍然获得期望的结果。另外，附图中描述的处理不是必须按照示出的特定顺序或者按照连续顺序才能获得期望结果。在一些实现中，多任务和并行处理可能是有利的。

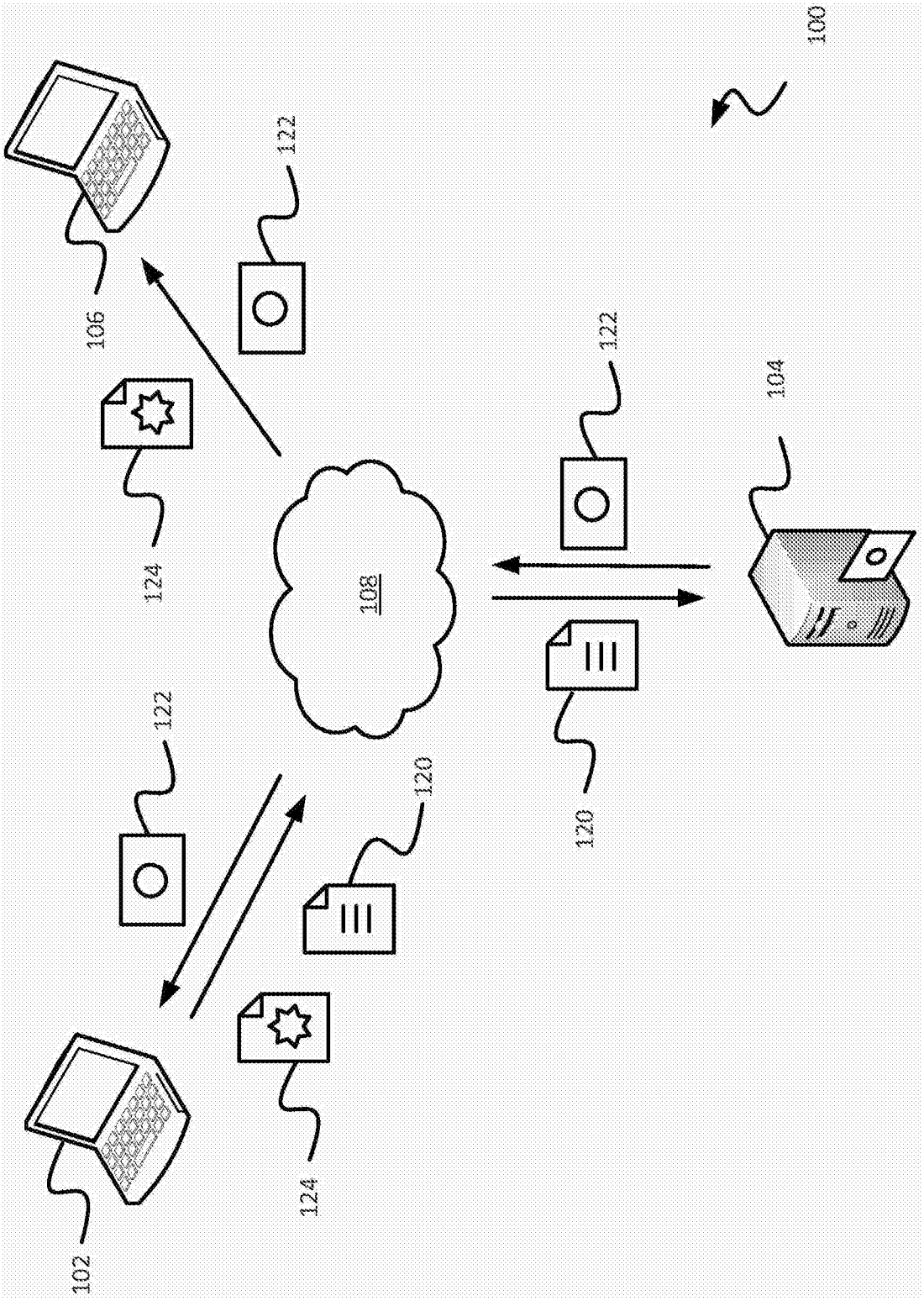


图1

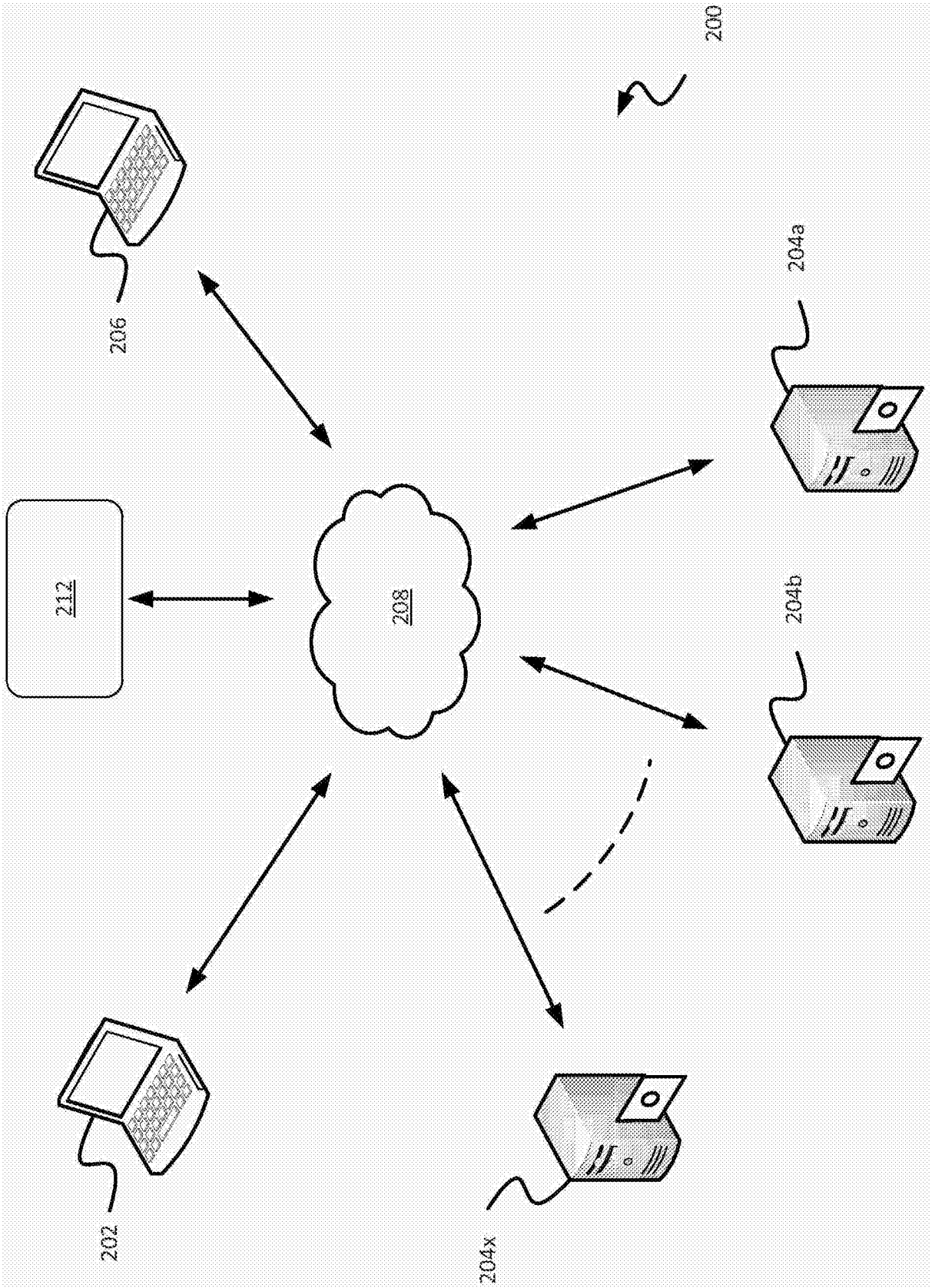


图2

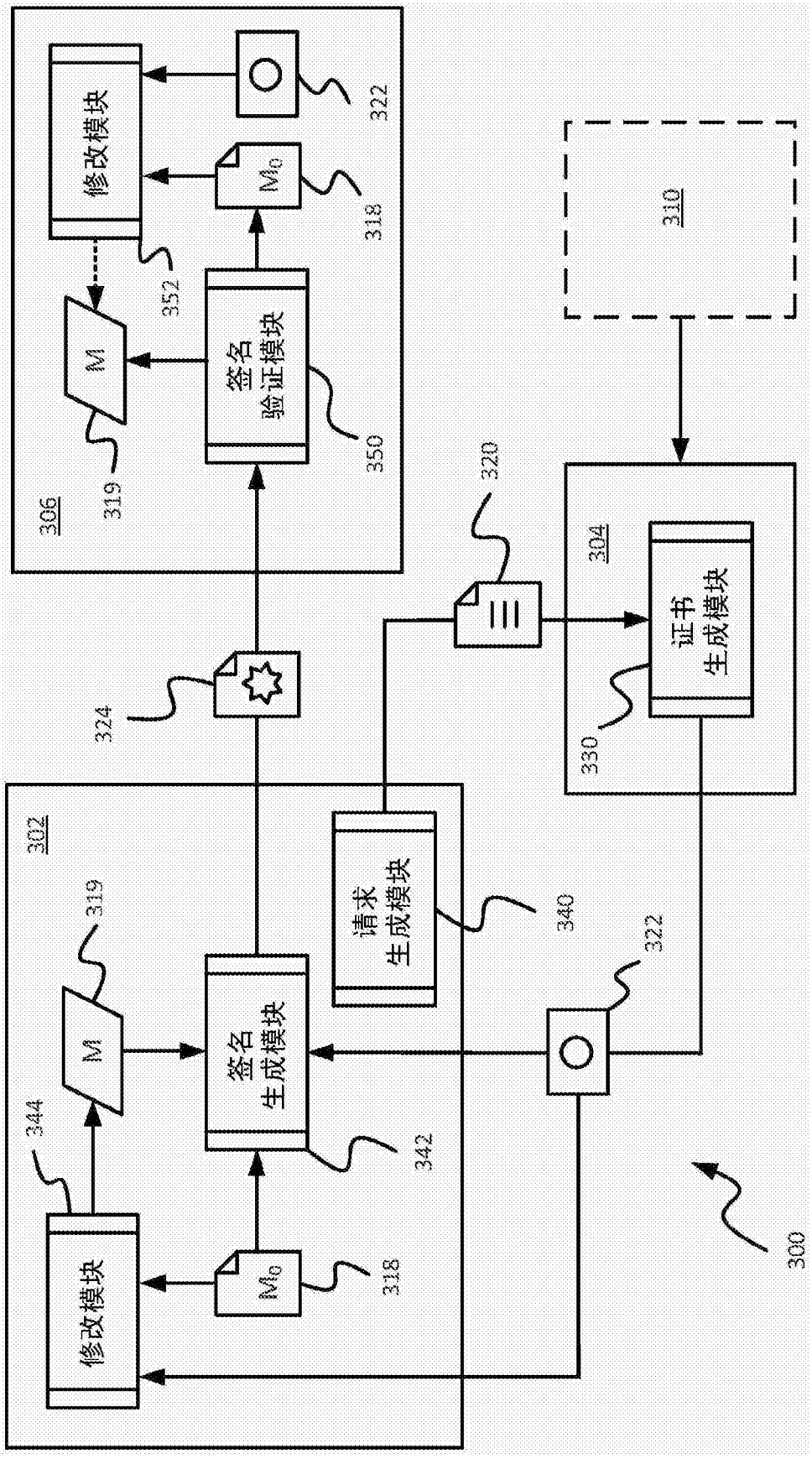

修改模块
322
M_0
318
352
M
319
签名
验证模块
350
306
310
320
304
证书
生成模块
330
324
302
319
M
344
签名
生成模块
342
请求
生成模块
340
322
修改模块
M_0
318
300

图3

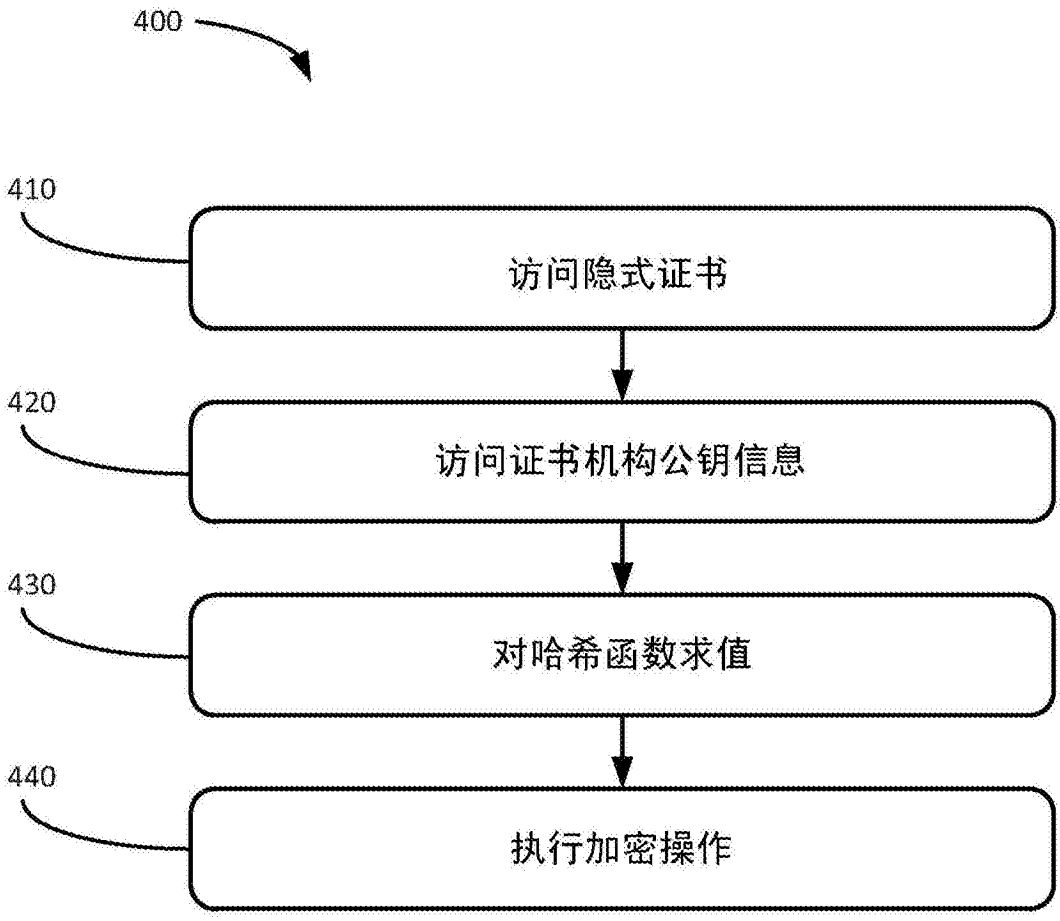


图4

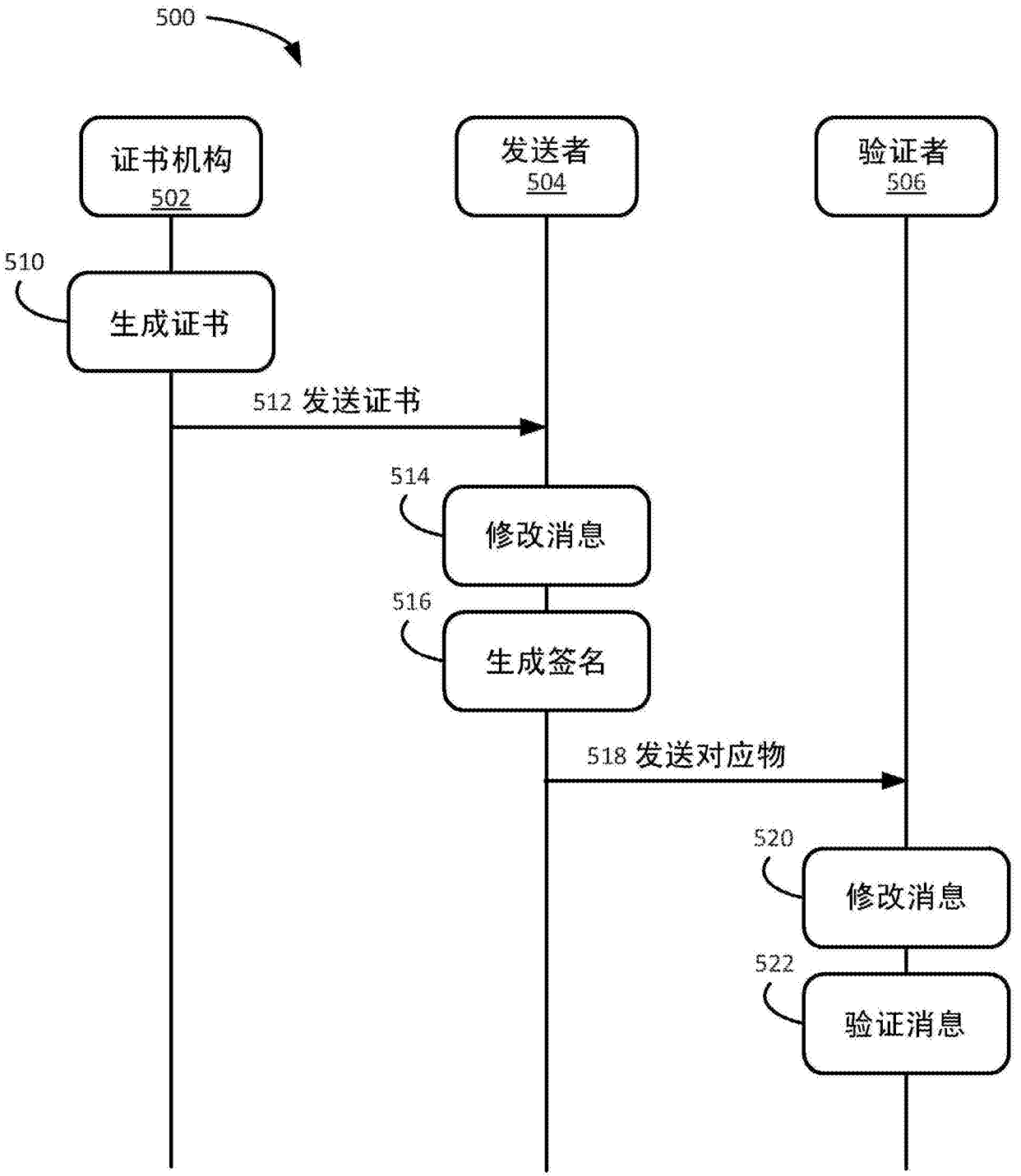

500
证书机构
502
发送者
504
验证者
506
510
生成证书
512 发送证书
514
修改消息
516
生成签名
518 发送对应物
520
修改消息
522
验证消息

图5