(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 101427234 B
(45)授权公告日 2011.02.23

(21)申请号 200780014261.7

(22)申请日 2007.04.23

(30)优先权数据
11/408,894 2006.04.21 US

(85)PCT申请进入国家阶段日
2008.10.21

(86)PCT申请的申请数据
PCT/US2007/010092 2007.04.23

(87)PCT申请的公布数据
WO2007/124180 EN 2007.11.01

(73)专利权人 微软公司
地址 美国华盛顿州

(72)发明人 G·S·西德胡 N·霍顿
S·K·辛格豪尔

(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 陈斌

(51)Int.Cl.
G06F 15/16(2006.01)
G06F 17/00(2006.01)
H04L 9/30(2006.01)

(56)对比文件
US 6671804 B1,2003.12.30, 说明书第1栏第45行-第7栏第8行.
US 2004/0064693 A1,2004.04.01, 说明书第14段栏第10行-第694段第5行, 附图1B,7.
US 2005/0010794 A1,2005.01.13, 说明书第60段第6行-第8行.

审查员 武晓冬

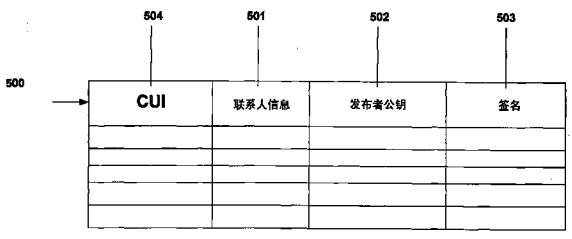
权利要求书 3 页 说明书 7 页 附图 12 页

(54)发明名称

用于对等联系人交换的方法和系统

(57)摘要

一系统可在公众可用的索引存储器中发布经认证的联系人信息、检索联系人信息并确认它。所要求保护的方法和系统可提供基于客户机的、服务器可任选的方法来进行发布。公众可用的索引存储可以是在对等网络中使用的分布式散列表。系统可在其中服务器不可用或者其中服务器信任最小的其它安全目录服务应用程序中使用。



CN 101427234 B

1. 一种使用公众可用的索引存储用于安全发布系统的方法，所述方法包括：

提供在统计上对于发布者公钥是唯一的加密唯一标识符；

通过使用对应于所述发布者公钥的发布者私钥签署发布者的联系人信息来创建签名；

将记录插入公众可用的索引存储，其中所述记录包括所述发布者公钥、所述签名以及所述发布者的联系人信息，并且所述记录由所述加密唯一标识符索引；

基于所述加密唯一标识符检索所述记录；

确定所述加密唯一标识符是否与被包括在所述记录中的所述发布者公钥有关；以及

确定所述发布者的联系人信息是否由对应于被包括在所述记录中的所述发布者公钥的私钥签署；

确定所述发布者的联系人信息是否具有期望的格式和句法；

在确定所述加密唯一标识符与被包括在所述记录中的所述发布者公钥有关、所述发布者的联系人信息由对应于被包括在所述记录中的所述发布者公钥的私钥签署、以及所述发布者的联系人信息具有期望的格式和句法后，建立与所述发布者的安全连接；

在确定所述加密唯一标识符没有与被包括在所述记录中的所述发布者公钥有关、所述发布者的联系人信息没有由对应于被包括在所述记录中的所述发布者公钥的私钥签署、或所述发布者的联系人信息不具有期望的格式和句法后，拒绝建立与所述发布者的安全连接。

2. 如权利要求 1 所述的方法，其特征在于，所述索引存储是分布式散列表和目录服务器之一。

3. 如权利要求 1 所述的方法，其特征在于，所述加密唯一标识符是使用散列函数从所述发布者公钥得到的。

4. 如权利要求 1 所述的方法，其特征在于，所述记录还包括与加密强度成比例的持续时间参数。

5. 如权利要求 4 所述的方法，其特征在于，建立安全连接还包括在确定所述加密唯一标识符与被包括在所述记录中的所述发布者公钥有关、所述发布者的联系人信息由对应于被包括在所述记录中的所述发布者公钥的私钥签署、所述发布者的联系人信息具有期望的格式和句法后、以及由所述持续时间参数指示的持续时间尚未期满后，建立与所述发布者的安全连接。

6. 如权利要求 1 所述的方法，其特征在于，所述加密唯一标识符包括由对等实体组拥有的组公钥。

7. 如权利要求 1 所述的方法，其特征在于，所述加密唯一标识符是至少根据第一用户加密唯一标识符和第二用户加密唯一标识符形成的。

8. 一计算机系统包括：

形成对等网络的多个对等节点；

所述对等网络的分布式散列表；

第一对等节点，创建在统计上对于所述第一对等节点的公钥唯一的加密唯一标识符，通过使用对应于所述公钥的所述第一对等节点的私钥签署对应于所述第一对等节点的联系人信息来创建签名，以及将包含所述第一对等节点的公钥、所述签名以及对应于所述第

一对等节点的联系人信息的记录插入到所述分布式散列表中，其中所述记录由所述加密唯一标识符索引；

第二节点，基于所述加密唯一标识符检索所述记录、确定所述加密唯一标识符是否与被包括在所述记录内的所述第一对等节点的公钥有关、确定对应于所述第一对等节点的所述联系人信息是否由对应于被包括在所述记录内的所述第一对等节点的公钥的所述私钥签署以及确定对应于所述第一对等节点的所述联系人信息是否具有期望的格式和句法；以及

所述第二节点进一步包括在确定所述加密唯一标识符与被包括在所述记录内的所述第一对等节点的公钥有关、对应于所述第一对等节点的所述联系人信息由对应于被包括在所述记录内的所述第一对等节点的公钥的所述私钥签署、以及对应于所述第一对等节点的所述联系人信息具有期望的格式和句法后，建立与所述第一对等节点的安全连接；

所述第二节点进一步包括在确定所述加密唯一标识符不与被包括在所述记录内的所述第一对等节点的公钥有关、对应于所述第一对等节点的所述联系人信息没有由对应于被包括在所述记录内的所述第一对等节点的公钥的所述私钥签署、或对应于所述第一对等节点的所述联系人信息不具有期望的格式和句法后，拒绝建立与所述第一对等节点的安全连接。

9. 如权利要求 8 所述的系统，其特征在于，所述加密唯一标识符包括关联于所述第一节点的第一加密唯一标识符与关联于所述第二节点的第二加密唯一标识符的组合。

10. 如权利要求 9 所述的系统，其特征在于，所述联系人信息是使用所述第二节点的公钥加密的。

11. 如权利要求 8 所述的系统，其特征在于，所述记录包括持续时间参数，其中所述持续时间参数与用于生成所述公钥和对应于所述公钥的所述私钥的加密算法的强度成比例。

12. 如权利要求 11 所述的系统，其特征在于，所述第二节点建立与所述第一对等节点的安全连接进一步包括在确定所述加密唯一标识符与被包括在所述记录内的所述第一对等节点的公钥有关、对应于所述第一对等节点的所述联系人信息由对应于被包括在所述记录内的所述第一对等节点的公钥的所述私钥签署、对应于所述第一对等节点的所述联系人信息具有期望的格式和句法、以及由所述持续时间参数指示的持续时间尚未期满后，所述第二节点建立与所述第一对等节点的安全连接。

13. 一种用于检索联系人信息并验证所述联系人信息的方法，包括：

从公钥得到加密唯一标识符；

基于所述加密唯一标识符在索引存储中检索条目，其中所述条目包含联系人信息以及所述公钥，其中所述条目进一步包括所述加密唯一标识符并被所述加密唯一标识符索引，其中，所述联系人信息和所述公钥一起由对应于所述公钥的私钥签署；

确定所述加密唯一标识符是否与所述公钥有关；以及

确定所述联系人信息和公钥是否由对应于所述公钥的所述私钥签署；

确定所述联系人信息是否具有期望的格式和句法；

在确定所述加密唯一标识符与所述公钥有关、所述联系人信息和公钥由对应于所述公钥的所述私钥签署、以及所述联系人信息具有期望的格式和句法后，建立安全连接；以及

在确定所述加密唯一标识符没有与所述公钥有关、所述联系人信息和公钥没有由对应

于所述公钥的所述私钥签署、或所述联系人信息不具有期望的格式和句法后，拒绝建立安全连接。

14. 如权利要求 13 所述的方法，其特征在于，还包括确定所述条目的持续时间参数是否已经期满。

15. 如权利要求 14 所述的方法，其特征在于，所述持续时间参数指示的持续时间与用于生成所述公钥和私钥的加密等级成比例。

16. 如权利要求 13 所述的方法，其特征在于，所述加密唯一标识符是通过组合第一加密唯一标识符与第二加密唯一标识符来形成的，以及其中，所述联系人信息是使用关联于所述第二加密唯一标识符的计算机的公钥来加密的。

用于对等联系人交换的方法和系统

[0001] 技术背景

[0001] 目录服务通常使用网络服务器来提供。为了使用目录服务，要求用户连接至服务器并具有用户帐号以便访问目录服务。另外，用户必须信任服务器提供数据完整性和数据认证。如果目录服务旨在用于较小的连接实体组，例如自组织网络，则创建并设立用于该自组织网络的目录服务器可能是低效率的。例如，自组织网络在本质上一般是瞬时的，并且由于管理员时间、装备资源容量（某一服务器必须被重新分配或添加）以及用户时间（帐号创建与设立可能牵涉到用户），为短持续时间和少量用户设立专用服务器的成本太过高昂。而且，尽管基于服务器的系统是常见的，但新的无服务器的系统诸如对等网络可在创建自组织网络方面提供更多的灵活性，因为它们不要求专用的服务器来促进通信。然而，为了使用现有的加密过程来允许在这些自组织网络上的安全通信，可能需要目录服务来促进不依赖于基于服务器的模型的公钥交换。

[0002] 发明内容

[0003] 一系统在公众可用的索引存储中发布经认证的联系信息。该系统还可提供检索联系人信息并验证它的方法。所要求保护的方法和系统可以是基于客户机的，而服务器是可任选的。公众可用的索引存储可以是在对等网络中使用的分布式散列表。该系统可在其它其中服务器不可用或者其中服务器信任最小的安全目录服务应用程序中使用。

[0004] 在一个实施例中，系统可用作一般的消息发布系统。在另一实施例中，系统可用于提供选择性发布，在其中被投送的记录仅可由预期的接收者来检索和阅读。

[0005] 附图说明

[0006] 图 1 例示可按照权利要求操作的计算系统的框图；

[0007] 图 2 例示一般的对等网络；

[0008] 图 3 例示一般的目录服务器和服务；

[0009] 图 4 例示分布式散列表；

[0010] 图 5 例示在权利要求的实施例中使用的记录；

[0011] 图 6 例示发布过程实施例；

[0012] 图 7 例示检索过程实施例；

[0013] 图 8 例示包含持续时间参数的修改记录；

[0014] 图 9 例示使用持续时间参数的另一个确认过程；

[0015] 图 10 例示用于选择性发布的修改记录；

[0016] 图 11 例示用于选择性发布的发布过程实施例；以及

[0017] 图 12 例示用于选择性发布的检索过程实施例。

[0019] 具体实施方式

[0018] 尽管下面的文本阐述众多不同实施例的详细描述，但应当理解，该描述的法律范围是由本专利所附的权利要求书的语言定义的。详细描述应当仅解释为是示例性的，并不描述每一可能的实施例，因为描述每一可能的实施例即使不是不可能也是不实际的。众多

的替换实施例可使用当前技术或者使用在本专利的申请日之后开发的技术来实现，但仍然落在本发明的范围之内。

[0019] 还应当理解，除非在本专利中使用“如在本文所使用的，术语‘_____’这里定义为表示...”语句或相似语句来明确定义一个术语，否则不旨在其普通或平常的意义之外明确或隐含地限制该术语的意义，并且这样的术语不应解释为限于基于在本专利的任何部分（除了权利要求书的语言之外）中所作的任何陈述的范围。对于在本专利所附权利要求书中所述的任何术语在本专利中以与单数意义一致的方式来引用，这仅是为了清楚而不混淆读者，并且不是要隐含或者以其它方式来将该权利要求术语限制于该单数意义。最后，除非一个权利要求元素是通过陈述词语“装置 (means)”和功能而非陈述任何结构来定义，任何权利要求元素的范围不应基于对 35U.S.C. §112 第六段的应用来解释。

[0020] 图 1 例示合适计算系统环境 100 的一个示例，在其上可实现所要求保护的方法和装置的各块的系统。计算系统环境 100 只是合适计算环境的一个示例并且不旨在对权利要求的方法和装置的使用范围或功能性提出任何限制。也不应当将计算环境 100 解释为对在示例性操作环境 100 中例示的任一组件或组件组合有任何依赖性或需求。

[0021] 要求保护的方法和装置的各块可与众多其它通用或专用计算系统环境或配置一起使用。适于与本发明的方法或装置一起使用的公知的计算系统、环境和 / 或配置包括但不限于，个人计算机、服务器计算机、手持式或膝上型设备、多处理器系统、基于微处理器的系统、机顶盒、可编程消费电子产品、网络 PC、小型计算机、大型计算机、包含任何上述系统或设备的分布式计算环境等等。

[0022] 要求保护的方法和装置的各块可在诸如程序模块等由计算机执行的计算机可执行指令的一般上下文中描述。一般而言，程序模块包括例程、程序、对象、组件、数据结构等，它们执行特定的任务或者实现特定的抽象数据类型。这些方法和装置还可在分布式计算环境中实践，其中任务由通过通信网络链接的远程处理设备来执行。在分布式计算环境中，程序模块可位于包含存储器存储设备在内的本地和远程两者的计算机存储介质中。

[0023] 参考图 1，用于实现要求保护的方法和装置的各块的示例性系统包括计算机 110 形式的通用计算设备。计算机 110 的组件包括但不限于，处理单元 120、系统存储器 130 和系统总线 121，后者将包括系统存储器在内的各种系统组件耦合至处理单元 120。系统总线 121 可以是任意若干类型的总线结构，其中包括存储器总线或存储器控制器、外围总线和使用任何各种总线体系结构的局部总线。作为示例而非限制，这样的体系结构包括工业标准体系结构 (ISA) 总线、微通道体系结构 (MCA) 总线、增强型 ISA(EISA) 总线、视频电子标准协会 (VESA) 局部总线以及还被称为夹层总线的外围组件互连 (PCI) 总线。

[0024] 计算机 110 一般包括各种计算机可读介质。计算机可读介质是可由计算机 110 访问的任何可用介质并且包括易失性与非易失性、可移动与不可移动介质。作为示例而非限制，计算机可读介质可包括计算机存储介质和通信介质。计算机存储介质包括以用于存储诸如计算机可读指令、数据结构、程序模块或其它数据的信息的任何方法或技术实现的易失性与非易失性、可移动与不可移动介质。计算机存储介质包括但不限于，RAM、ROM、EEPROM、闪存或其它存 储器技术，CD-ROM、数字多功能盘 (DVD) 或其它光盘存储，磁带盒、磁带、磁盘存储或其它磁存储设备，或者任何可用于存储所需信息并可由计算机 110 访问的任何其它介质。通信介质一般体现为在诸如载波或其它传输机制中的经调制数据信号中

的计算机可读指令、数据结构、程序模块或其它数据并且包括任何信息传递介质。术语“经调制的数据信号”指具有以将信息编码到信号中的方式设置或改变的一或多个特性的信号。作为示例而非限制，通信介质包括线接介质如线接网络或直接线连接以及无线介质如声音、RF、红外和其它无线介质。上述的任何组合也应当包括在计算机可读介质的范围内。

[0025] 系统存储器 130 包括易失性和 / 或非易失性存储器形式的计算机存储介质，诸如只读存储器 (ROM)131 和随机存取存储器 (RAM)132。基本输入 / 输出系统 133(BIOS) 包含诸如启动时帮助在计算机 110 内的元件之间传送信息的基本例程，通常存储在 ROM131 中。RAM132 一般包含可由处理单元 120 立即访问和 / 或正在操作的数据和 / 或程序模块。作为示例而非限制，图 1 例示操作系统 134、应用程序 135、其它程序模块 136 和程序数据 137。

[0026] 计算机 110 还可包括其它可移动 / 不可移动、易失性 / 非易失性计算机存储介质。仅作为示例，图 1 例示读写不可移动、非易失性磁介质的硬盘驱动器 140，读写可移动、非易失性磁盘 152 的磁盘驱动器 151 以及读写可移动、非易失性光盘 156 诸如 CD ROM 或其它光介质的光盘驱动器 155。可在示例性操作环境中使用的其它可移动 / 不可移动、易失性 / 非易失性计算机存储介质包括但不限于，磁带盒、闪存卡、数字多功能盘、数字录像带、固态 RAM、固态 ROM 等等。硬盘驱动器 141 一般通过不可移动存储器接口诸如接口 140 连接至系统总线 121，而磁盘驱动器 151 和光盘驱动器 155 一般通过可移动存储器接口诸如接口 150 连接至系统总线 121。

[0027] 上面讨论并在图 1 中例示的这些驱动器及其相关联的计算机存储介质为计算机 110 提供计算机可读指令、数据结构、程序模块和其它数据的存储。在图 1 中，例如，硬盘驱动器 141 例示为存储操作系统 144、应用程序 145、其它程序模块 146 和程序数据 147。注意，这些组件可以与操作系统 134、应用程序 135、其它程序模块 136 和程序数据 137 相同或者不同。操作系统 144、应用程序 145、其它程序模块 146 和程序数据 147 在这里给出不同的标号以说 明至少它们是不同的副本。用户可通过输入设备诸如键盘 162 和定点设备 161（通常指鼠标、轨迹球或触摸板）将命令和信息输入到计算机 20 中。其它输入设备（未示出）可包括话筒、操纵杆、游戏手柄、圆盘式卫星天线、扫描仪等等。这些和其它输入设备通常通过耦合至系统总线的用户输入接口 160 连接到处理单元 120，但可通过其它接口和总线结构诸如并行端口、游戏端口或通用串行总线 (USB) 来连接。监视器 191 或其它类型的显示设备也通过诸如视频接口 190 的接口连接到系统总线 121。除了监视器之外，计算机还可包括其它外围输出设备诸如扬声器 197 和打印机 196，它们可通过输出外围接口 190 来连接。

[0028] 计算机 110 可在使用至一或多个远程计算机如远程计算机 180 的逻辑连接的网络化环境中运行。远程计算机 180 可以是个人计算机、服务器、路由器、网络 PC、对等设备或其它普通网络节点，并且一般包括上面相对于计算机 110 所述的许多或全部元素，尽管在图 1 中仅示出一个存储器存储设备 181。图 1 所示的逻辑连接包括局域网 (LAN)171 和广域网 (WAN)173，但还可包括其它网络。这类联网环境在办公室、企业级计算机网络、内联网和因特网中是很常见的。

[0029] 当在 LAN 联网环境中使用时，计算机 110 通过网络接口或适配器 170 连接到 LAN171。当在 WAN 联网环境中使用时，计算机 110 通常包括调制解调器 172 或用于在诸如因特网等 WAN173 上建立通信的其它装置。调制解调器 172 可以是内置或外置的，它可以通

过用户输入接口 160 或其它合适的机制连接至系统总线 121。在网络化环境中，相对于计算机 110 描述的程序模块或其部分可以存储在远程存储器存储设备中。作为示例而非限制，图 1 将远程应用程序 185 例示为驻留在存储器设备 181 上。应了解到，例示的网络连接是示例性的并且可使用在计算机之间建立通信链接的其它手段。

[0030] 对等 (P2P) 系统使用以分散方式例如在没有中央服务器的帮助下相互通信的节点的网络。对等网络中的每一节点（例如应用程序或设备）可通过直接连接与网络上的另一节点通信，或者每一节点可使用一或多个中间节点间接地通信以将通信中继至预期的节点。

[0031] 图 2 例示 P2P 系统 200 的高级示图。系统 200 包括对等实体 (202-212) 的集合。对等实体 (202-212) 可以是通过网络或网络组合耦合在一起的个人计算机设备。图 2 例示了其中每一对等实体 (202-212) 连接至所有其它对等实体 (202-212) 的示例。在其它情形中，一或多个对等实体 (202-212) 可以通过一或多个中间参与者 (202-212) 连接至其它对等实体 (202-212)。然而，为了在对等网络上提供安全通信，首先需要建立对等节点之间的安全连接。

[0032] 连接安全可基于如本领域所公知的对称密钥加密过程。然而，为了实现该加密安全，对等实体需要首先交换允许在最初建立安全连接的证书和 / 或公钥。在一些现有系统中，诸如在图 3 中所示的，该交换可使用中央目录服务器 300 来促进，其中用户 301、302、303 可将它们的证书 304、305、306 和 / 或公钥投送到目录服务器 300 上。目录服务 307 可以是包含按用作密钥 309 的用户名或者其它标识符来索引的证书和 / 或公钥的记录 308 的数据库表。能够连接到目录服务器 300 并被允许访问目录服务 307 的用户可使用目标用户的标识符来查找目标用户，并且获得目标用户对应的公钥。该方法要求到服务器 300 的连通性、与目录服务器 300 的显式注册并且信任目录服务器 300。而且，某方必须负担主宿的成本，诸如服务器。当用户 303 正从远程位置连接时，另外还需要因特网连通性 310。服务器注册过程涉及用于在目录服务器 300 中提升信任的用户帐户。例如，如果任何用户可访问服务器 300，则可认为服务器 300 更容易受到损害，特别是在投送和交换诸如公钥的安全信息的时候。此外，因为自组织的临时网络的瞬时性质以及设立目录服务器的难度，为自组织的临时网络创建目录服务器是不切实际的。用于自组织非对等网络的可能工作区可以是通过电子邮件或通过网络外的过程来交换公钥，诸如向目标成员物理地发送或者邮寄包含证书 / 公钥的磁盘。这可允许对等实体建立服务器无关的安全链接。然而，这很麻烦且容易出错。

[0033] 所要求保护的服务器无关索引过程的实施例可使用无服务器索引存储，诸如图 4 所示的分布式散列表 (DHT)400。该分布式散列表 400 可在一组形成对等网络 405 的对等实体 401-404 上维护。分布式散列表中的条目可例如使用散列函数在逻辑上划分或归组。散列函数可用某种有组织的方式来将记录聚集在一起，从而使检索更有效率。DHT 具有两个基本属性 :1) 表（例如表 400）跨多个节点（例如节点 401-404）的分布 ;以及 2) 提供用于发布和检索记录的 路由机制（未示出）。路由机制和分布可由诸如 Chord、PNRP、Pastry、Tapestry 等覆盖协议管理。尽管 DHT 可用于提供按照权利要求的实施例的索引存储，但要强调的是，可使用可由一组对等实体容易地访问的任何索引存储，包括基于服务器的索引。在基于服务器的索引的情形中，所要求保护的系统可单独减少服务器所要求的信任的

等级，因为所要求保护的系统可为不安全的索引存储提供必需的安全等级。

[0034] 所要求保护的服务器无关索引过程的实施例可使用如图 5 所示的特定记录格式。图 5 例示，发布者可将包含联系人信息 501、发布者的公钥 502 和使用发布者的私钥的联系人信息的签名 503 的记录 500 投送至索引存储。或者，签名可以是联系人信息和公钥的组合。该记录可由记录密钥 504 来索引。在一个实施例中，记录的密钥 504 可以是加密的唯一标识符 (CUI)。CUI 具有两个基本属性。第一，CUI 在统计上是唯一的，以及第二，CUI 可对应于特定的用户公钥，诸如发布者公钥 502。与普通的数据库索引方案相似，记录密钥需要是唯一的，以防止重复的实体条目。因此，CUI 可以是按照其对于特定的情形或应用程序为唯一的可能性很大的方式而得到的。例如，在只有少量成员的对等者组中，如果加密唯一标识符可从相同的成员公钥得到的可能性对于组大小而言是不太可能的，则 CUI 在统计上是唯一的。

[0035] CUI 可使用诸如散列或加密算法的算法从公钥得到。可使用该算法验证 CUI 对应或者匹配其公钥。在一个实施例中，CUI 可用于以较短且用户可管理的形式，诸如在题为“Callsigns”美国专利第 10/882079 号中描述的 P2P 系统中使用的对等者名称来表示较长的用户标识符诸如公钥。

[0036] 图 5 的记录可用于将联系人信息发布至索引存储，诸如图 4 的 DHT400。CUI 密钥 504 可用于定位每一记录 500 并且检索联系人信息 501 和公钥 502。在该实施例中，所发布的信息可以是公开的，即所发布的信息可以不加密，除签名之外。然而，下面描述的其它实施例可加密所发布信息的各部分。而且，尽管该实施例例示使用记录 500 来促进公钥 502 的交换，但要强调的是，该系统可在任何其中可使用唯一消息发布的应用程序中使用。例如，代替联系人信息 501，可针对用户 CUI504 投送任何消息。

[0037] 图 6 例示按照权利要求的实施例的一般发布过程。使用诸如散列函数的算 法，可为给定用户的公钥生成 CUI601。重要的是注意，无论使用什么算法，都可验证 CUI 是否对应于用于生成它的公钥。可构造联系人信息或者其它消息数据以及发布者的公钥的记录 602，并且联系人信息和 / 或发布者的公钥可由发布者的私钥（它对应于公钥）来签署 603。包括联系人信息、公钥和签名的记录可插入到公众可用的索引中 604。记录可由对应于发布者公钥的 CUI 来索引。

[0038] 图 7 例示按照权利要求的实施例的检索过程。希望与第二对等者连接的用户可获得第二对等者的 CUI701。可在带外通过电子邮件或者网络外过程来获得 CUI（例如，传统邮件、语音通信、名片等）。CUI 随后可用于在索引存储中查找映射到该 CUI 的记录 702。如上所述，记录可包括密钥、一些消息信息（联系人信息）和签名。

[0039] 用户随后可基于 CUI 来查询索引存储以检索记录 703。一旦检索到 CUI，即可使用包含在记录内的公钥来验证 CUI 以确保它们彼此对应 704。该过程框可用于验证记录对应于 CUI。可用许多方法来使 CUI 在统计上对于公钥是唯一的。在一个实施例中，对等通信系统可预建立通用映射过程，例如使用公认的散列函数。该初始的验证过程帮助确保记录确实对应于给定的 CUI。

[0040] 如果 CUI 正确地映射，则记录的签名随后可用于确定该签名是否由发布者的对应私钥签名 705。这可通过提供消息源自发布者的证据来认证消息，因为可以假设发布者拥有对应于用于该加密的公钥的私钥。

[0041] 如果记录 / 消息被正确地签名，则随后可对记录的联系人信息执行消息格式和 / 或句法检查 706。这可用于，例如确保消息没有被删改过以匹配签名。尽管提供被删改的消息以匹配加密的签名在统计上是困难的，但并非不可能。然而，删改会导致不符合预期或期望格式的消息。因而，首先检查消息以确定消息格式是否符合期望格式。例如，在传输联系人信息时，联系人信息可要求十个字符的格式。如果记录格式不提供这十个字符的格式，则消息可能已经被某人或某物篡改了 711。

[0042] 或者或者另外，可检查消息的语义。例如，联系人信息可限制为选项列表以及这些选项之间的特定关系。因此，如果格式要求两个条目，第一条目与第二个条目相关（语义）并且它们不匹配该期望格式，则消息可能已经被某人或某物篡改了 711。

[0043] 如果验证过程 704、705、706 均已经成功完成，则记录是真实的并且随后被使用 707，例如，公钥可用于建立通信链接。如果验证步骤 704、705、706 中的任一个失败，则消息可能已经某人或某物被篡改 711。在公钥交换系统的情形中，可拒绝连接。

[0044] 在图 8 所示的另一实施例中，持续时间参数 801 可被包括在记录 800 中。该持续时间参数 801 可对应于在所述的认证过程中使用的加密等级。例如，加密等级可对应于用于生成在所要求保护的系统中使用的公 / 私钥对的加密强度。如果加密强度高，则持续时间长，反之亦然。持续时间参数 801 可指示记录有效性的持续时间。因而，持续时间参数 801 可在图 9 所示的检索过程中使用。图 9 例示图 7 的相同过程，添加了框 909，在其中检查由持续时间参数 801 指示的持续时间 901 以确定持续时间是否已经期满。如果持续时间参数 801 期满，则记录可能被损坏 911。否则记录是有效的 907。

[0045] 图 10-12 例示另一个实施例，其中可使用选择性发布来允许第一用户发布仅有作为目标的第二用户才能检索的数据。在该选择性发布实施例中，可使用如图 10 所示的记录 1001。记录 1001 可包括由两个 CUI1003、1004 的组合形成的密钥 1002。第一 CUI1003 可与第一用户相关联，而第二 CUI1004 可与第二用户相关联。可通过简单地将第二 CUI 追加到第一 CUI 来形成该组合。该记录可包括消息部分 1005 和持续时间参数 1006。消息 1005 可包含关于发布者的联系人信息、发布者公钥和签名的数据。

[0046] 图 11 例示使用图 10 的记录 1001 的选择性发布过程。发布者可从公钥得到其 CUI1101，获得所选接收者的 CUI1102，构造消息 1103，使用发布者的私钥签署该消息 1104 并基于 CUI 组合密钥 1101 将该消息插入到索引中 1105。另外，消息可使用预期接收者的公钥来加密 1106。

[0047] 图 12 例示与图 7 相似的添加了框 1201、1202、1203 的选择性发布过程的检索过程。希望检索所发布的记录的接收者首先获得发布者的 CUI1201，然后根据组合的 CUI 密钥在索引存储查找记录 1202。在又一个增强的实施例中，消息可使用接收者的公钥来加密。因而，只有接收者可解密预期的数据。在接收者使用 CUI 组合密钥检索消息 1202 之后，接收者可使用其私钥来首先解密记录 1203，之后验证过程和确认按照图 7 进行。在该选择性发布实施例中，接 收者的公钥（用于加密记录）可根据接收者 CUI 来确定，发布者用它来创建组合密钥。

[0048] 在上述实施例的另一个增强方案中，密钥可以是组公钥，它由对等者组拥有。在该实施例中，组的任何成员可按照组公钥查找记录并且执行认证过程。用户组有权访问记录并且可明确地作为所投送消息的接收目标。

[0049] 应当强调的是，尽管上述特定实施例可与公钥交换目录相关联，但联系人信息可表示其它数据。例如，代替联系人信息，记录可以是普通消息投送。因而，所要求保护的系统可用作任何公众可用的索引存储上的一般发布系统。所要求保护的系统还可用于提供除公钥查找以外的目录服务。所要求保护的系统允许现有的分布式索引存储诸如分布式散列表用作安全的目录服务工作而不依赖于服务器。

[0050] 另外，所要求保护的系统可在现有的基于服务器的目录上使用，在其中服务器安全最小化，从而需要由所要求保护的系统提供的认证过程。在自组织系统诸如对等者组和对等网络中，公钥发布和检索的无服务器过程可通过减少作为主机的专用服务器提供目录服务的需求来使得这样的网络的创建更有效率。所要求保护的方法和系统还可最小化用户的牵连，因为公 / 私钥加密过程可消除用户明确地向服务器注册的需求。

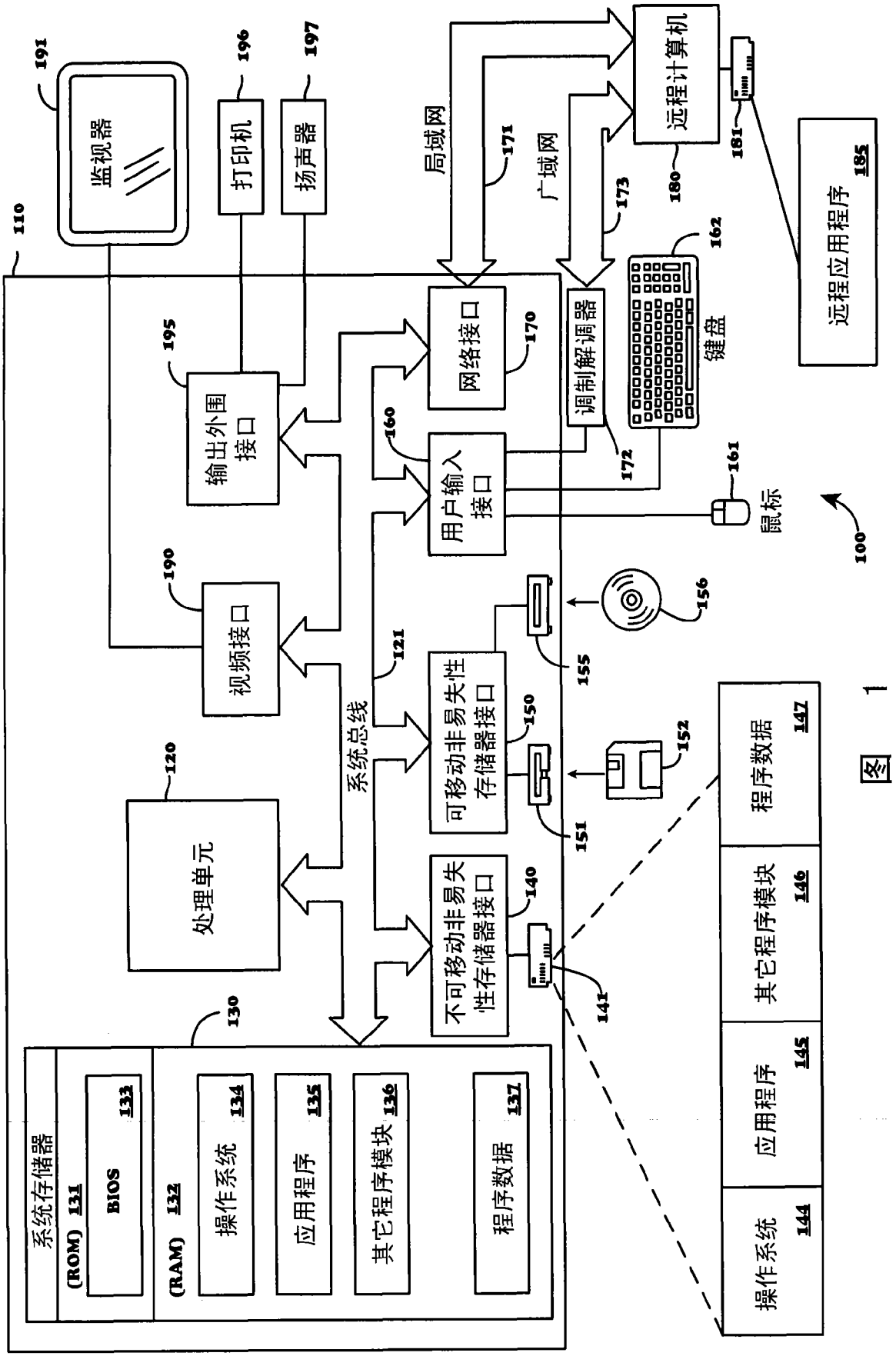

监视器
191
打印机
196
扬声器
197
局域网
171
广域网
173
远程计算机
180
181
远程应用程序
185
110
162
键盘
输出外围接口
195
网络接口
170
调制解调器
172
160
用户输入接口
161
鼠标
100
190
视频接口
156
121
系统总线
155
可移动非易失性存储器接口
150
120
处理单元
152
151
不可移动非易失性存储器接口
140
141
130
系统存储器
(ROM) 131
BIOS 133
(RAM) 132
操作系统 134
应用程序 135
其它程序模块 136
程序数据 137
操作系统 144
应用程序 145
其它程序模块 146
程序数据 147

图 1

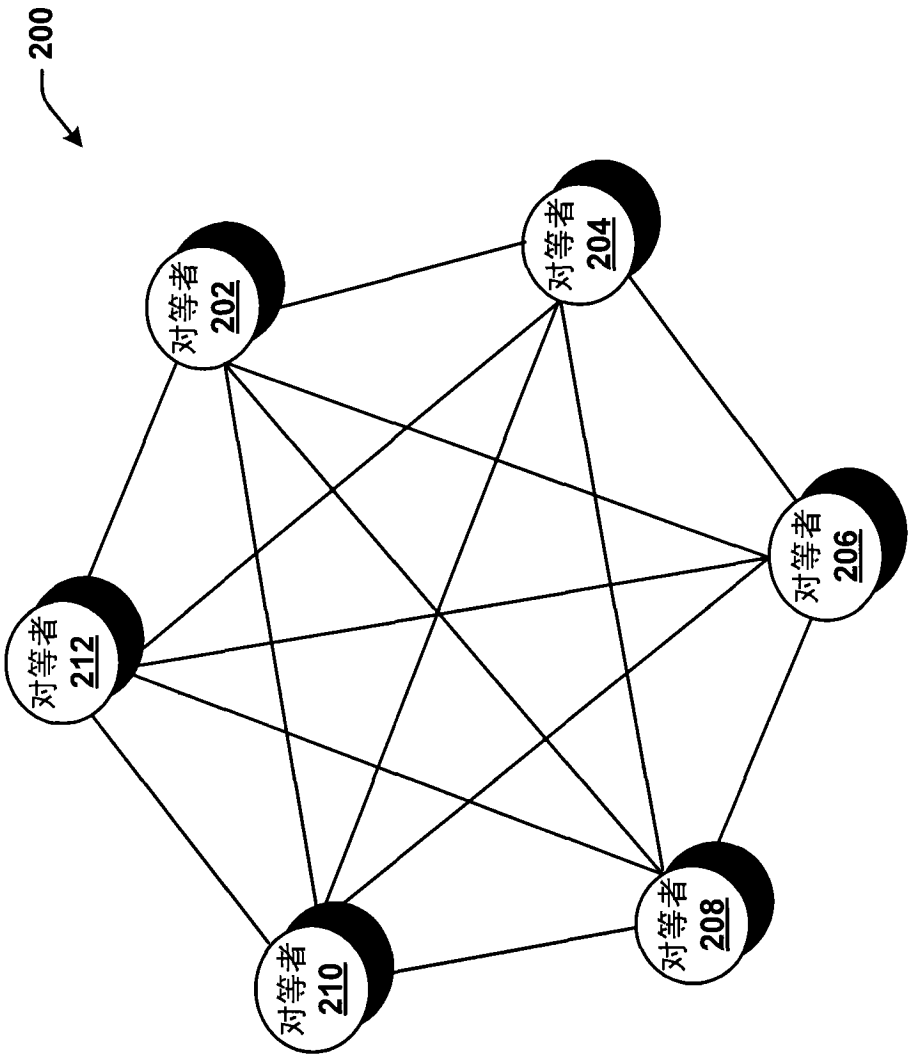


图 2

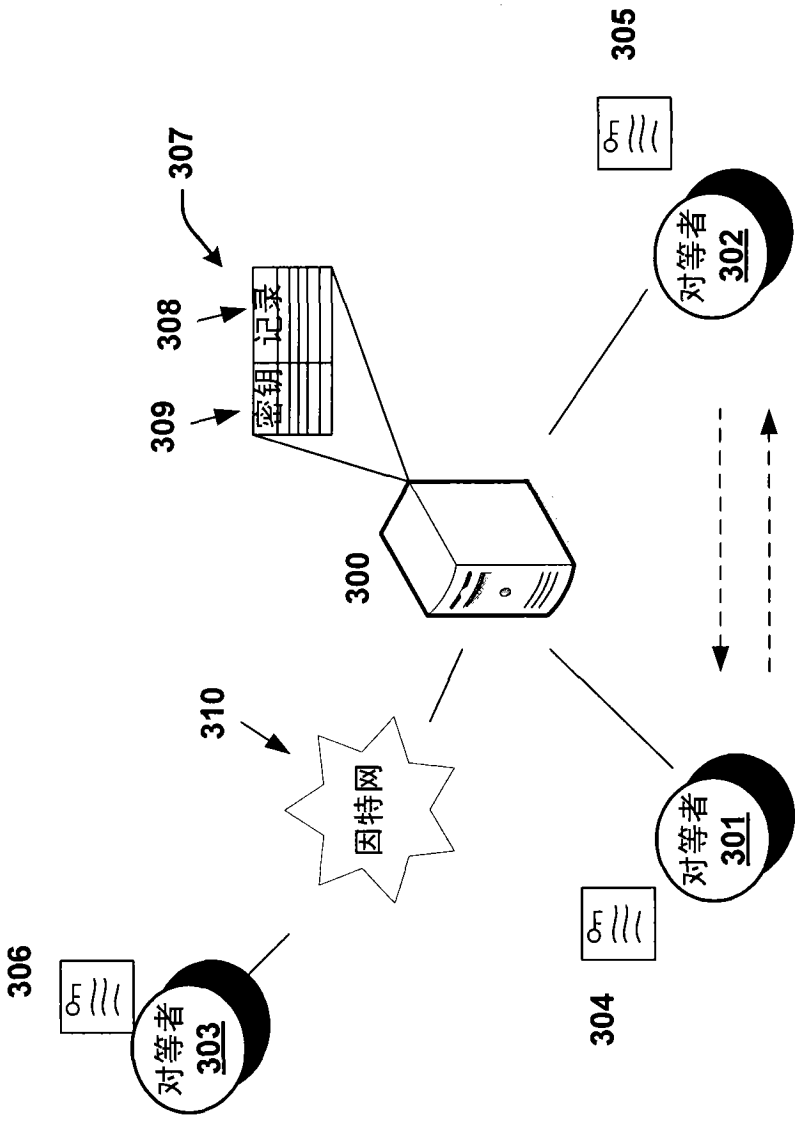


图 3

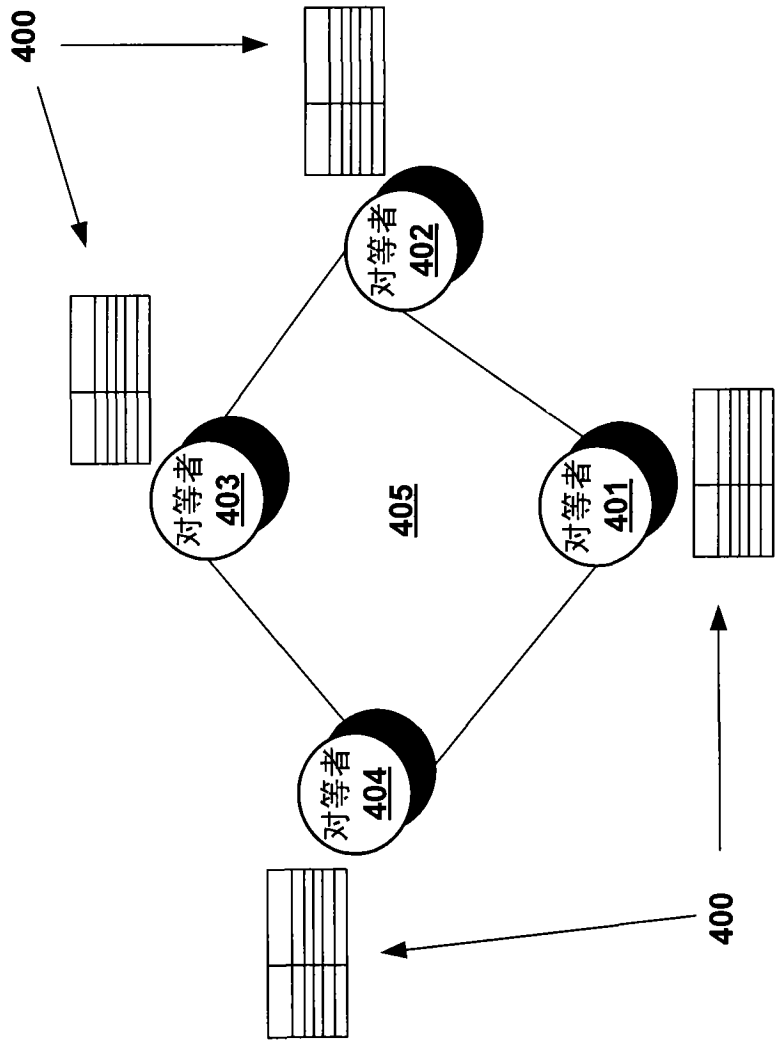


图 4

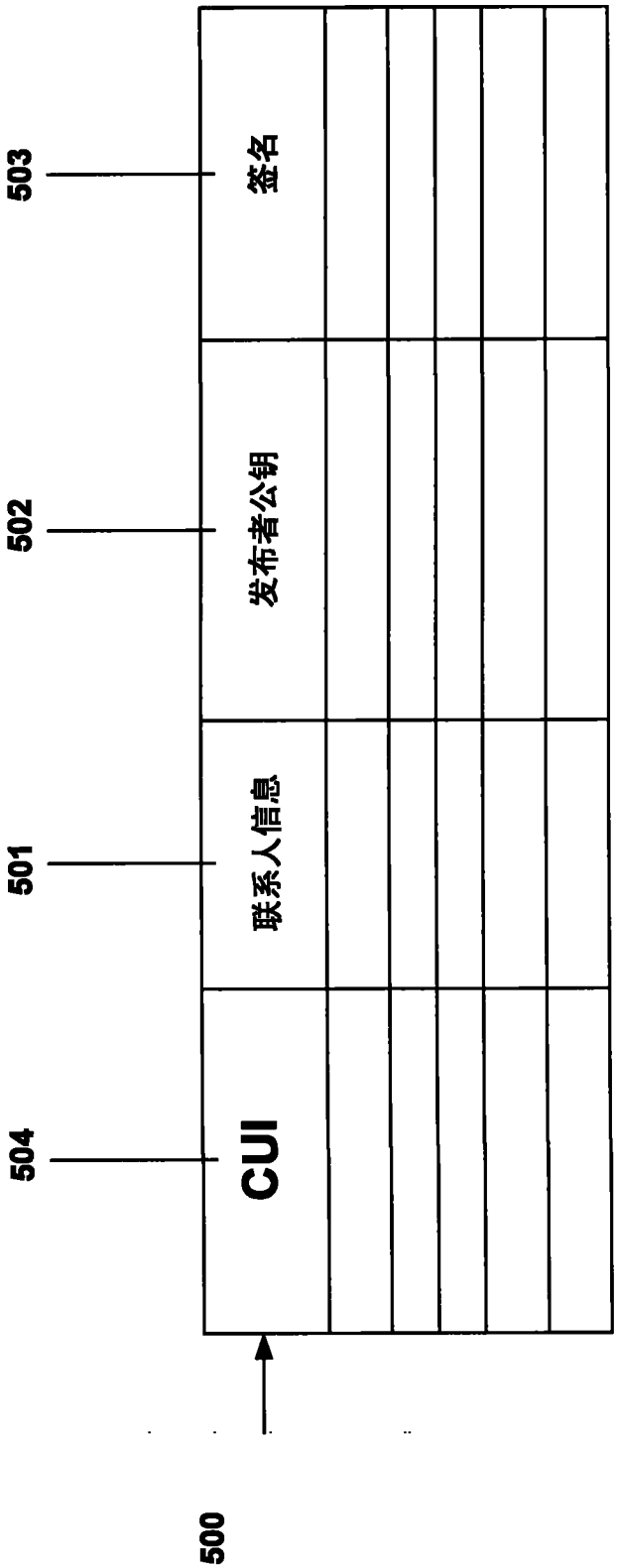


图 5

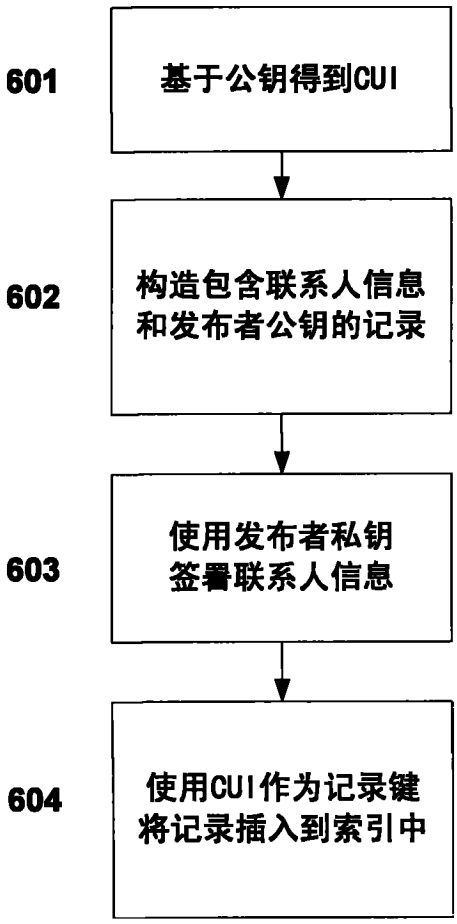

601
基于公钥得到CUI
602
构造包含联系人信息
和发布者公钥的记录
603
使用发布者私钥
签署联系人信息
604
使用CUI作为记录键
将记录插入到索引中

图 6

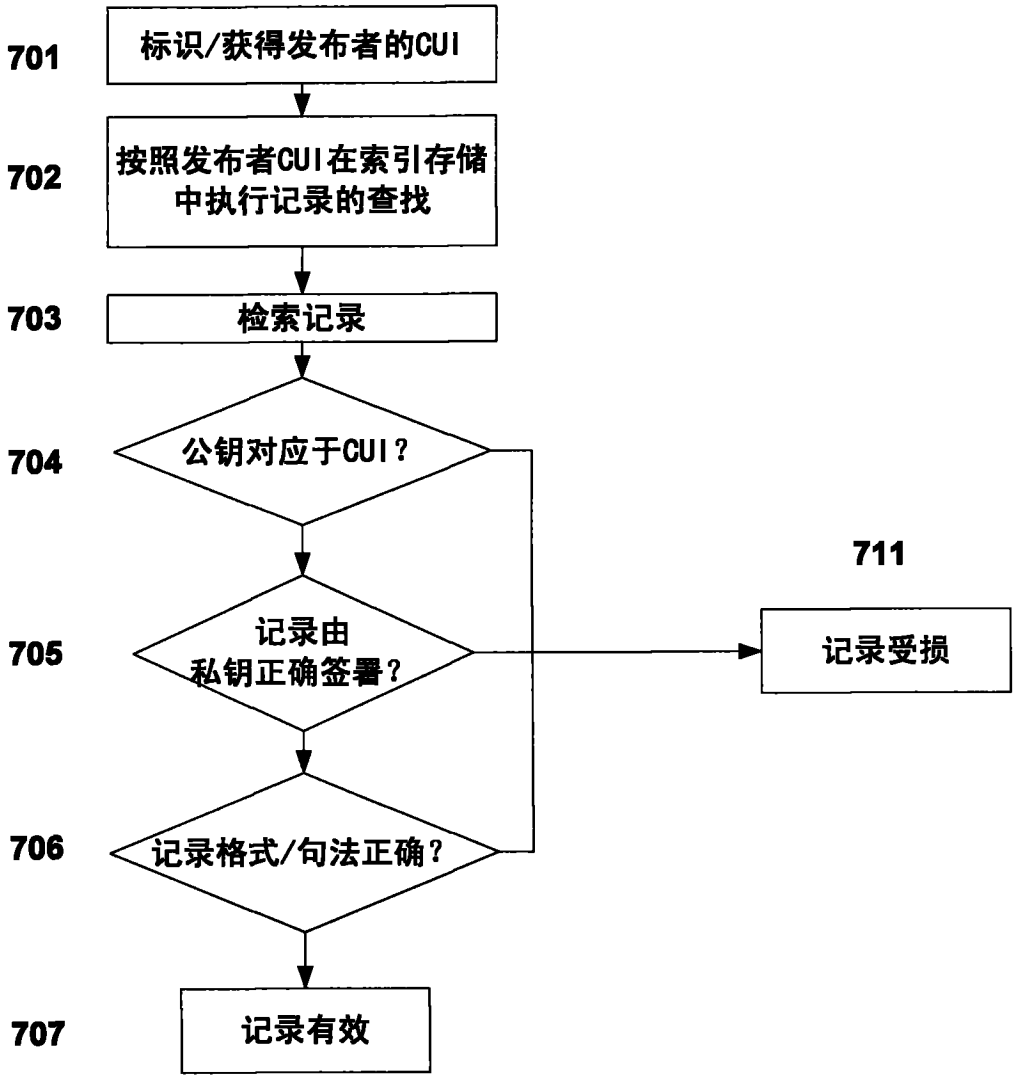

701
标识/获得发布者的CUI
702
按照发布者CUI在索引存储中执行记录的查找
703
检索记录
704
公钥对应于CUI？
705
记录由私钥正确签署？
711
记录受损
706
记录格式/句法正确？
707
记录有效

图 7

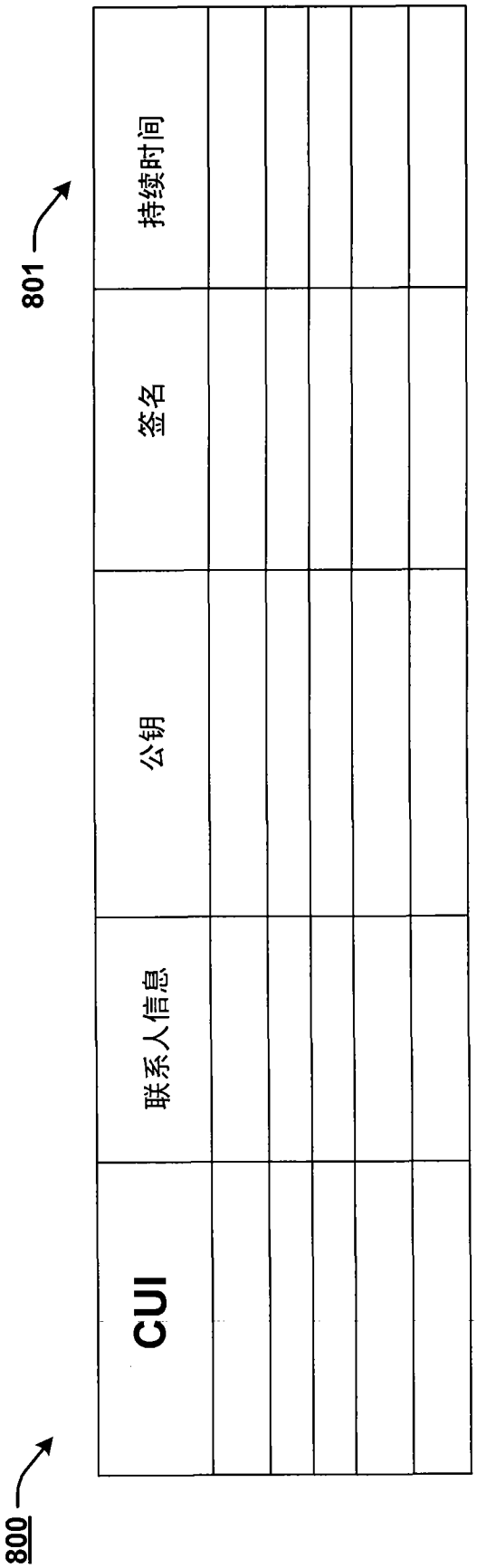


图 8

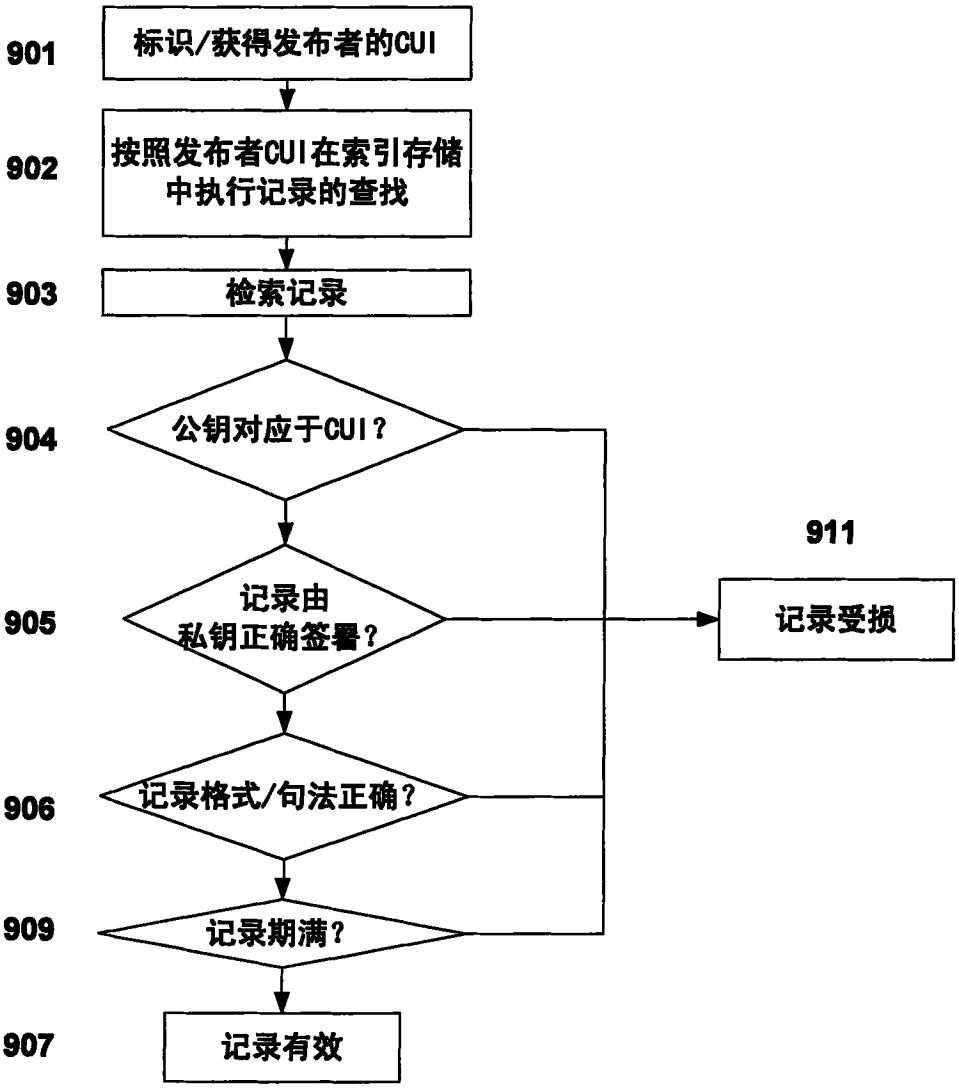

901
标识/获得发布者的CUI
902
按照发布者CUI在索引存储中执行记录的查找
903
检索记录
904
公钥对应于CUI？
905
记录由私钥正确签署？
911
记录受损
906
记录格式/句法正确？
909
记录期满？
907
记录有效

图 9

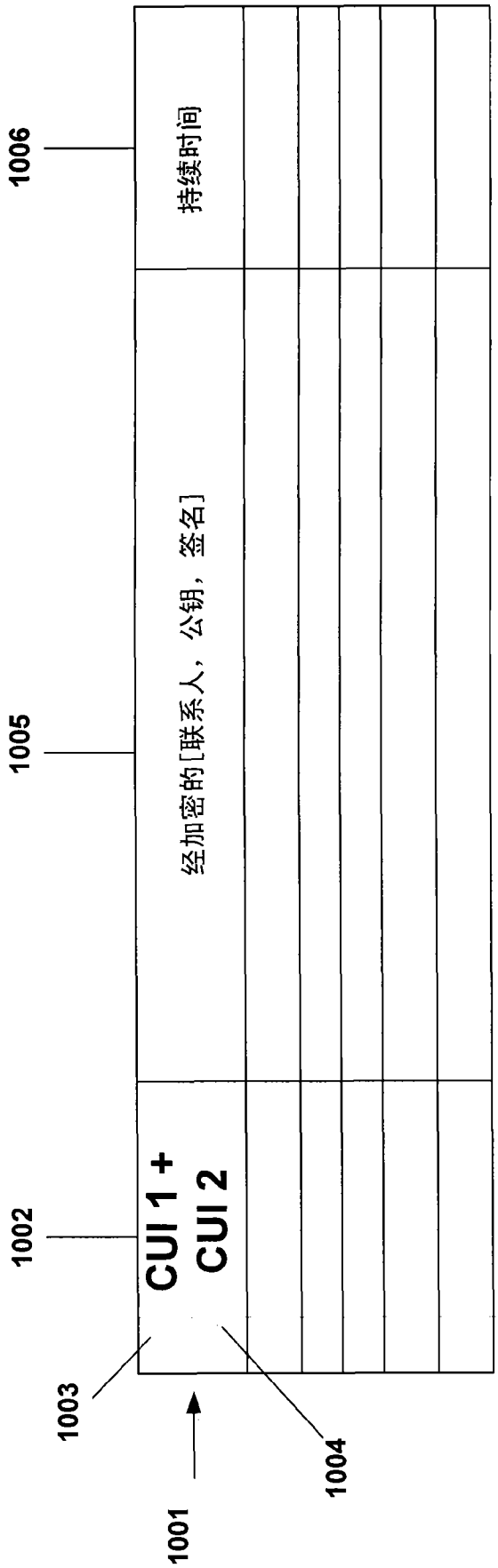


图 10

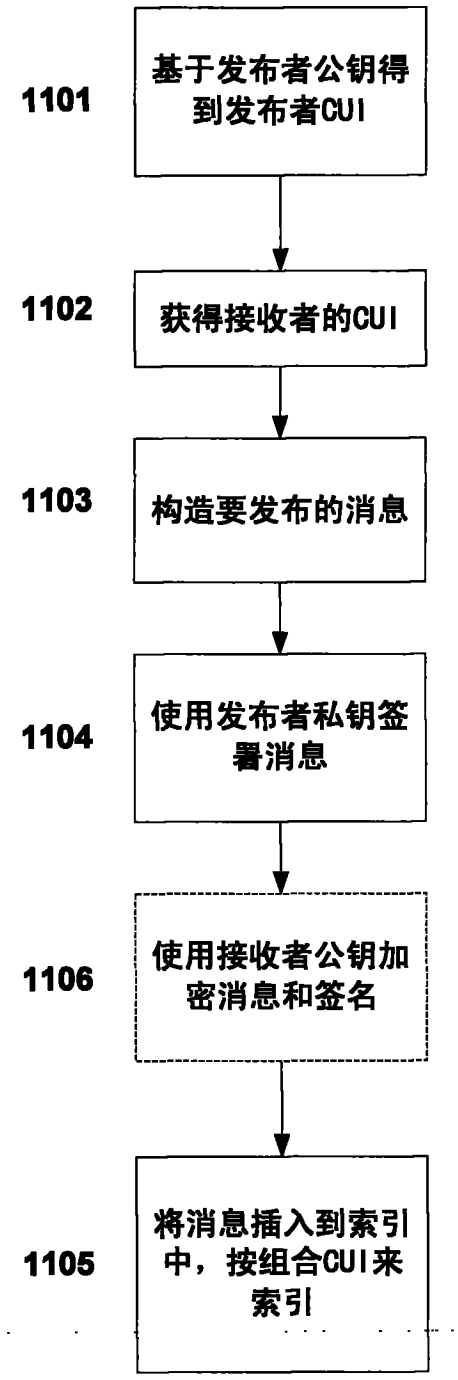

1101
基于发布者公钥得到发布者CUI
1102
获得接收者的CUI
1103
构造要发布的消息
1104
使用发布者私钥签署消息
1106
使用接收者公钥加密消息和签名
1105
将消息插入到索引中，按组合CUI来索引

图 11

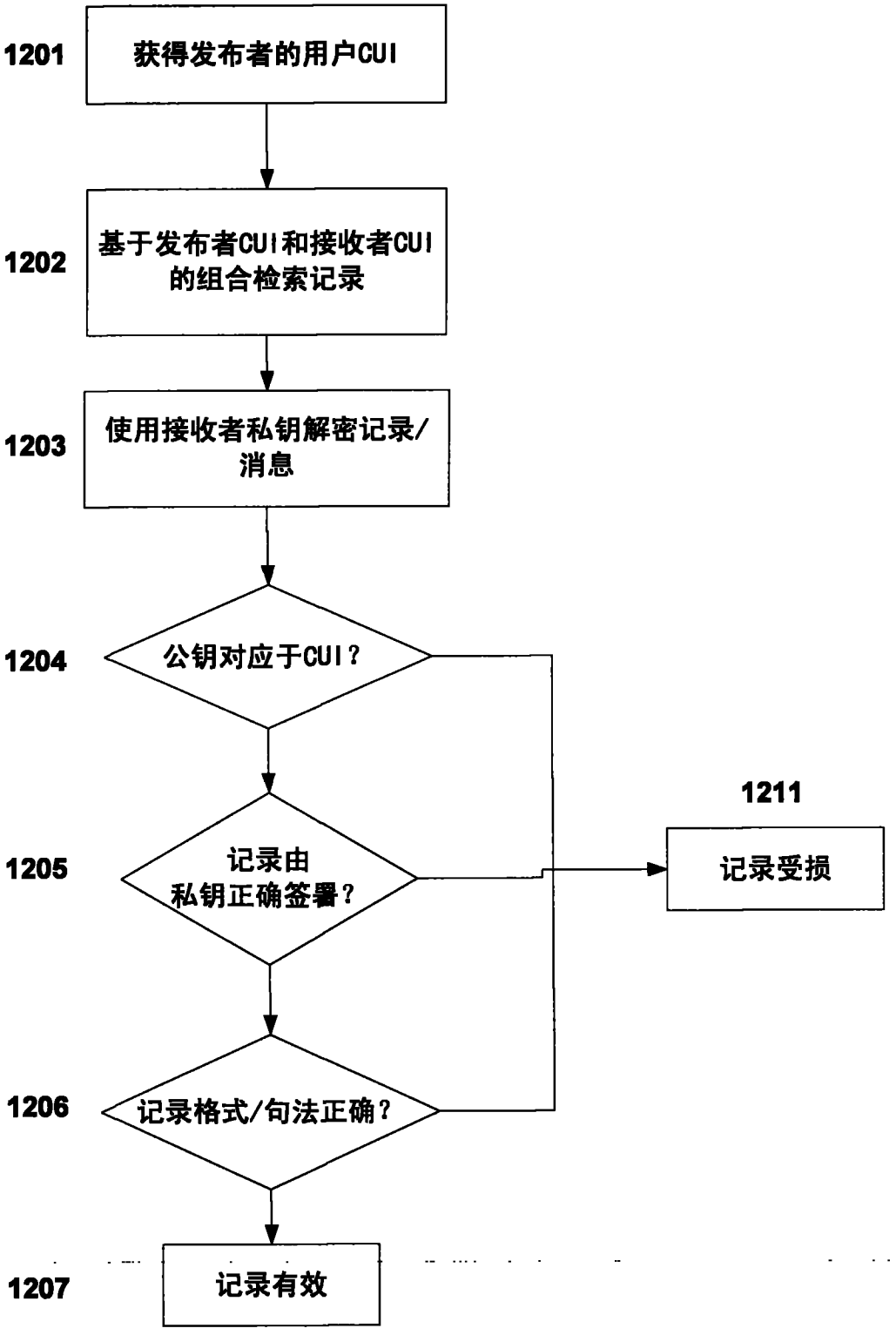

1201
获得发布者的用户CUI
1202
基于发布者CUI和接收者CUI的组合检索记录
1203
使用接收者私钥解密记录/消息
1204
公钥对应于CUI？
1205
记录由私钥正确签署？
1206
记录格式/句法正确？
1207
记录有效
1211
记录受损

图 12