(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 110383755 B
(45)授权公告日 2022.04.19

(21)申请号 201880015812.X
(22)申请日 2018.01.02
(65)同一申请的已公布的文献号
申请公布号 CN 110383755 A
(43)申请公布日 2019.10.25
(30)优先权数据
17150389.9 2017.01.05 EP
(85)PCT国际申请进入国家阶段日
2019.09.04
(86)PCT国际申请的申请数据
PCT/EP2018/050033 2018.01.02
(87)PCT国际申请的公布数据
WO2018/127479 EN 2018.07.12

(73)专利权人 皇家飞利浦有限公司
地址 荷兰艾恩德霍芬
(72)发明人 M·P·博德拉恩德
(74)专利代理机构 永新专利商标代理有限公司 72002
代理人 孟杰雄

(51)Int.Cl.
H04L 9/08(2006.01)
H04L 9/30(2006.01)
H04L 9/32(2006.01)

审查员 李常亮

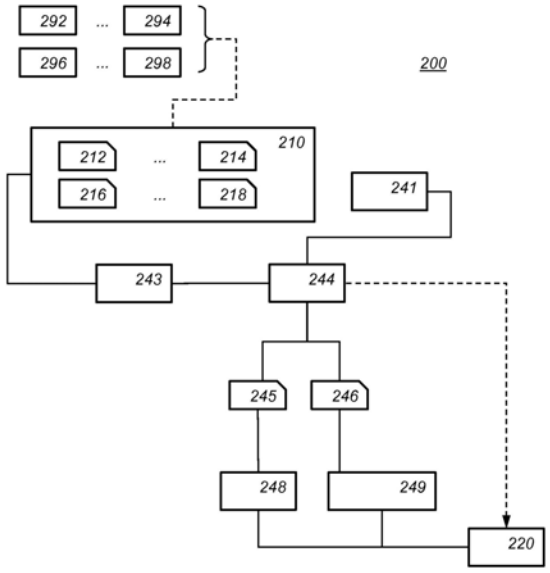
权利要求书3页 说明书20页 附图7页

(54)发明名称

网络设备和可信第三方设备

(57)摘要

一种第一网络节点(100;200)被配置为:-根据第二网络节点的第一身份和保护第一网络节点的机密性的本地密钥材料计算保护机密性的第一共享密钥(245),-根据第二网络节点的第二身份和保护第一网络节点的完整性的本地密钥材料计算保护完整性的第二共享密钥(246),-使用第一共享密钥加密消息,并且-使用第二共享密钥计算关于消息的第一消息认证码。



CN 110383755 B

1.一种第一网络节点(100;200),包括:

密钥存储设备(100;160;210;260),其被布置为存储至少以下项:

保护所述第一网络节点与其他网络节点之间的通信的机密性的本地密钥材料(212、214;213),所述保护通信的本地密钥材料是由用于机密性的可信第三方(TTP)(192;292、294;293)将基于身份的密钥预分配方案的本地密钥材料生成算法用于所述第一网络节点的第一身份来生成的,以及

保护所述第一网络节点与其他网络节点之间的所述通信的完整性的本地密钥材料(216、218;217),所述保护完整性的本地密钥材料是由用于完整性的可信第三方(TTP)(194;296、298;297)将基于身份的密钥预分配方案的本地密钥材料生成算法用于所述第一网络节点的第二身份生成的,

通信接口(120;170;220;265),其被布置用于所述第一网络节点与所述其他网络节点之间的数字通信,以及

处理器电路(130),其被配置为:

获得第二网络节点(150;201)的第一身份和第二身份,

根据所述第二网络节点的所述第一身份和所述保护所述第一网络节点的机密性的本地密钥材料来计算保护机密性的第一共享密钥(245),

根据所述第二网络节点的所述第二身份和所述保护所述第一网络节点的完整性的本地密钥材料来计算保护完整性的第二共享密钥(246),

使用所述第一共享密钥来加密消息,

使用所述第二共享密钥来计算关于所述消息的第一消息认证码,以及

向所述第二网络节点发送加密消息和所述第一消息认证码,

和/或所述处理器电路被配置为:

从第二网络节点接收加密消息和第一消息认证码,

获得第二网络节点的第一身份和第二身份,

根据所述第二网络节点的所述第一身份和所述保护所述第一网络节点的机密性的本地密钥材料来计算保护机密性的第一共享密钥(245),

根据所述第二网络节点的所述第二身份和所述保护所述第一网络节点的完整性的本地密钥材料来计算保护完整性的第二共享密钥(246),

使用所述第一共享密钥来解密所述加密消息,以及

使用所述第二共享密钥来验证所述第一消息认证码。

2.根据权利要求1所述的第一网络节点,其中,所述处理器电路被配置为:

获得与所述第二网络节点的所述第一身份和所述第二身份不同的另一身份,

根据所述另一身份和至少所述保护所述第一网络节点的完整性的本地密钥材料来计算保护完整性的第三密钥(247),

使用所述第三密钥来计算关于至少所述消息的第二消息认证码,

发送所述第二消息认证码。

3.根据权利要求2所述的第一网络节点,其中,所述处理器电路被配置为向所述第二网络节点发送所述另一身份,其中,所述处理器电路被配置为随机地选择所述另一身份。

4.根据权利要求2所述的第一网络节点,其中,所述处理器电路被配置为不向所述第二

网络节点发送所述另一身份,其中,所述处理器电路被配置为:

获得作为固定身份的所述另一身份,

通过将散列函数应用于所述消息来获得所述另一身份。

5.根据权利要求2-4中的任一项所述的第一网络节点,其中,所述第二消息认证码是关于至少所述消息和所述第一消息认证码计算的。

6.根据权利要求2-4中的任一项所述的第一网络节点,其中,所述处理器电路被配置为:

将所述用于机密性的本地密钥材料和所述用于完整性的本地密钥材料组合,从而形成组合的本地密钥材料,所述第三密钥是根据所述另一身份和所述组合的本地密钥材料导出的。

7.根据权利要求2-4中的任一项所述的第一网络节点,其中,所述处理器电路被配置为:

通过首先根据所述另一身份和所述保护所述第一网络节点的完整性的本地密钥材料获得中间第三密钥并且将所述中间第三密钥与所述第一共享密钥组合来计算所述第三密钥。

8.根据权利要求1-4中的任一项所述的第一网络节点,其中,所述第一身份和所述第二身份是相等的。

9.一种用于第一网络节点(100;200)的电子通信方法,包括:

存储至少以下项:

保护所述第一网络节点与其他网络节点之间的通信的机密性的本地密钥材料(212、214;213),所述保护通信的本地密钥材料是由用于机密性的可信第三方(TTP)(192;292、294;293)将基于身份的密钥预分配方案的本地密钥材料生成算法用于所述第一网络节点的第一身份来生成的,以及

保护所述第一网络节点与其他网络节点之间的所述通信的完整性的本地密钥材料(216、218;217),所述保护完整性的本地密钥材料是由用于完整性的可信第三方(TTP)(194;296、298;297)将基于身份的密钥预分配方案的本地密钥材料生成算法用于所述第一网络节点的第二身份生成的,

所述方法包括:

获得第二网络节点(150;201)的第一身份和第二身份,

根据所述第二网络节点的所述第一身份和所述保护所述第一网络节点的机密性的本地密钥材料来计算保护机密性的第一共享密钥(245),

根据所述第二网络节点的所述第二身份和所述保护所述第一网络节点的完整性的本地密钥材料来计算保护完整性的第二共享密钥(246),

使用所述第一共享密钥来加密消息,

使用所述第二共享密钥来计算关于所述消息的第一消息认证码,以及

向所述第二网络节点发送加密消息和所述第一消息认证码,

和/或所述方法包括:

从第二网络节点接收加密消息和第一消息认证码,

获得第二网络节点的第一身份和第二身份,

根据所述第二网络节点的所述第一身份和所述保护所述第一网络节点的机密性的本地密钥材料来计算保护机密性的第一共享密钥(245)，

根据所述第二网络节点的所述第二身份和所述保护所述第一网络节点的完整性的本地密钥材料来计算保护完整性的第二共享密钥(246)，

使用所述第一共享密钥来解密所述加密消息，以及

使用所述第二共享密钥来验证所述第一消息认证码。

10.一种包括表示指令的瞬态或非瞬态数据(1020)的计算机可读介质(1000)，所述指令使处理器系统执行根据权利要求9所述的方法。

网络设备和可信第三方设备

技术领域

[0001] 本发明涉及网络节点、可信第三方设备、电子通信方法、电子可信第三方方法和计算机可读介质。

背景技术

[0002] 在常规公共密钥基础设施中，存在单个可信根，其还被称为可信第三方或者密钥机构。可信第三方签名参与公共密钥基础设施的网络节点的证书。发送网络节点可以验证接收网络节点的证书上的签名以确保其真实性并且使用包含在证书中的公共密钥来加密消息。发送节点可以使用对应于他自己的证书的私有密钥来签名消息。接收网络具有对应于其公共密钥的私有密钥并且利用其将消息解密。使用发送节点的证书以及特别地包含在其中的公共密钥，可以验证签名。

[0003] 尽管广泛，但是存在该系统的许多缺点。首先，当可信根被侵入(hack)时，这损害整个系统。如果攻击者得到对可信根的根密钥材料(在这种情况下，其私有密钥)的访问权，那么攻击者可以生成他自己的证书。接收利用这样的伪造证书签名的消息的网络节点会将其接受为真实的并且对消息的内容进行动作。在过去，例如，入侵的密钥机构已经被用于分布式恶意软件。

[0004] 具有对根密钥材料的访问权的攻击者能够带来很大危害，然而合法法律实施不能得到对加密消息的内容的访问权：入侵的可信根允许证书欺骗，但是不允许合法法律实施获悉利用该系统加密的拦截的消息的内容。

[0005] 对于现代电信系统，获悉合法拦截的消息的内容的能力常常是要求的。例如，考虑ETSI TS 101 331 V1.1.1(2001-08)：“根据相关合法授权，网络运营商、访问提供商、服务提供商应当确保：1)与正被拦截的目标身份相关联的通信的整个内容能够在合法授权的整个时段期间拦截”。

[0006] 在常规公共密钥基础设施中，合法拦截要求可以通过确保公共密钥基础设施中的节点的私有密钥为可用来满足。例如，可信根能够要求在其签名证书之前利用其存放私有密钥。关于向其对应的网络节点之外的各方提供密钥材料的问题在于，利用该密钥材料，能够在没有任何控制的情况下欺骗消息。这减少用于在法律程序期间使用的拦截的消息的值，并且使其易受欺诈行为的影响。

[0007] Garcia-Morchon,O等人的“A Comprehensive and Lightweight Security Architecture to Secure the IoT Throughout the Lifecycle of a Device Based on HIMMO”公开了一种使用由可信第三方生成的基于身份的本地密钥材料保护网络节点之间的通信的保密性的方法。

[0008] DE 10 2012 209408 A1公开了一种用于消息的安全传输的方法，其允许基于基本密钥和发射器的标识符验证消息的完整性。

发明内容

[0009] 呈现了一种根据权利要求限定的网络节点。所述网络节点使用基于身份的密钥预分配方案。各种这样的方案存在并且可以适于本发明。在本文中呈现了基于身份的密钥预分配方案的多个范例。

[0010] 所述网络节点具有从至少两个不同的可信第三方获得的本地密钥材料:用于完整性的至少一个和用于完整性的至少一个。因此,合法拦截机构可以给定仅对与机密性有关的密钥材料的访问权,例如,用于机密性的(一个或多个)可信第三方的根密钥材料或者用于该网络节点的机密性的本地密钥材料。具有这样的密钥材料,合法拦截机构获得拦截并且读取通信的能力。然而,合法拦截机构不能够改变所述消息,至少在不破坏所述消息上的第一消息认证码的情况下不能。如果所述消息在稍后法案中变得相关,则拦截的消息可以存储在由所有方信任的受托人处(例如,公证人),在其之后,第二MAC可以例如使用从所述网络节点获得的本地密钥材料或者从用于完整性的TTP获得的本地(或根)密钥材料由可信第三方自己验证。以这种方式,检查与平衡自然集成在所述系统中。

[0011] 在实施例中,所述第一网络根据另一身份和保护所述第一网络节点的完整性的本地密钥材料计算保护完整性的第三密钥。所述第三密钥可以被用于计算第二MAC。对应于所述另一身份的本地密钥材料不可用于接收第二网络节点。因此,所述第二MAC不能通过所述接收网络节点篡改。这增加了所述系统的不可否认性。

[0012] 呈现了一种如由网络节点执行的电子通信方法,如权利要求中所限定的。

[0013] 在本文中阐述根据本发明的设备和方法的额外的优点。

[0014] 本发明可以例如应用在要求合法拦截和/或要求发送器实际上发送消息的证明的任何通信介质中,例如WhatsApp、电报、5G电话、患者与医生之间的通信等。例如,所述网络节点可以是电话,诸如智能电话、移动计算机、膝上型电脑、平板电脑、笔记本、计算机、智能卡等。例如,所述网络节点可以是传感器网络中的传感器节点、照明网络中的照明单元等。

[0015] 根据本发明的方法可以在计算机上被实施为计算机实施的方法或者在专用硬件或者在两者的组合中。用于根据本发明的方法的可执行代码可以被存储在计算机程序产品上。计算机程序产品的范例包括存储器设备、光学存储设备、集成电路、服务器、在线软件等。优选地,所述计算机程序产品包括被存储在用于当所述程序产品被运行在计算机上时执行根据本发明的方法的计算机可读介质上的非瞬态程序代码。

[0016] 在优选的实施例中,所述计算机程序包括适于当所述计算机程序被运行在计算机上时执行根据本发明的方法的所有步骤的计算机程序代码。优选地,所述计算机程序被实现在计算机可读介质上。

[0017] 根据本发明的另一方面提供一种使所述计算机程序可用于下载的方法。该方面当所述计算机程序被上载到例如苹果的App Store、谷歌的Play Store或微软的Windows Stores中时并且当所述计算机程序可用于从这样的商店下载时被使用。

附图说明

[0018] 将仅通过范例参考附图描述本发明的另外的细节、方面和实施例。为简单和清楚起见,图中的元件被图示,并且不一定按比例绘制。在附图中,与已经描述的元件对应的元件可以具有相同的附图标记。在图中,

[0019] 图1a示意性地示出了网络节点的实施例的范例；

[0020] 图1b示意性地示出了网络节点的实施例的范例；

[0021] 图1c示意性地示出了网络节点的实施例的范例；

[0022] 图2示意性地示出了通信系统的实施例的范例；

[0023] 图3示意性地示出了可信第三方设备的实施例的范例；

[0024] 图4示意性地示出了可信第三方设备的实施例的范例；

[0025] 图5示意性地示出了电子通信方法的实施例的范例；

[0026] 图6示意性地示出了用于完整性的电子可信第三方(TTP)方法的实施例的范例；

[0027] 图7a示意性地示出了根据实施例的具有包括计算机程序的可写部分的计算机可读介质；

[0028] 图7b示意性地示出了根据实施例的处理器系统的表示。

[0029] 图1-5中的附图标记列表：

[0030] 100 第一网络节点

[0031] 110、160 密钥存储设备

[0032] 120、170 通信接口

[0033] 130、180 处理器电路

[0034] 150 第二网络节点

[0035] 190 数字网络

[0036] 192 用于机密性的可信第三方

[0037] 194 用于完整性的可信第三方

[0038] 195 通信系统

[0039] 200、202 第一网络节点

[0040] 201 第二网络节点

[0041] 210、260 密钥存储设备

[0042] 212、213、214 保护机密性的本地密钥材料

[0043] 216、217、214 保护完整性的本地密钥材料

[0044] 220、265 通信接口

[0045] 241、271 身份获得器

[0046] 242 另一身份获得器

[0047] 243、273 组合器

[0048] 244、274 共享密钥单元

[0049] 247 第三密钥

[0050] 245 保护机密性的第一共享密钥

[0051] 246 保护完整性的第二共享密钥

[0052] 248 加密单元

[0053] 249 MAC生成单元

[0054] 278 解密单元

[0055] 279 MAC验证单元

[0056] 292、293、294 用于机密性的可信第三方

[0057] 296、297、298 用于完整性的可信第三方

[0058] 300 可信第三方设备

[0059] 310 密钥存储设备

[0060] 322 第一通信接口

[0061] 324 第二通信接口

[0062] 330 处理器电路

[0063] 400 可信第三方设备

[0064] 410 密钥存储设备

[0065] 422 第一通信接口

[0066] 424 第二通信接口

[0067] 432 本地密钥材料生成器

[0068] 434 MAC验证单元

[0069] 442 第二身份

[0070] 444 发送第二身份和接收第二身份

[0071] 446 消息和消息认证码

具体实施方式

[0072] 尽管本发明容许许多不同形式的实施例，但是在附图中示出并且将在本文中详细描述一个或多个具体实施例，应理解本公开应被认为是本发明的原理的范例，并非旨在将本发明限制于示出和描述的特定实施例。

[0073] 在下文中，为了理解，在操作中描述了实施例的元件。然而，将显而易见的是，相应元件被布置为执行描述为由它们执行的功能。此外，本发明不限于实施例，并且本发明在于本文描述的或在互不相同的从属权利要求中记载的每个或每一个新颖特征或特征组合。

[0074] 本发明利用所谓的基于身份的密钥预分配方案。这些方案提供使用本地基于身份的密钥材料执行密钥协商的方式。下文提供了关于基于身份的密钥预分配方案的一些背景。

[0075] 基于身份的密钥预分配方案具有两个阶段：密钥预分配和密钥导出。与基于身份的密钥预分配方案的两个阶段相关联的是两种算法：分别是本地密钥材料生成算法和密钥建立算法。

[0076] 通过向可信第三方提供根密钥材料来建立基于身份的密钥预分配方案。可信第三方可以是设备的制造商，并且可以例如在其制造期间或在一些其他可信环境中供应设备。备选地，可信第三方可以是证书授权设备，例如，使用特定在线协议来供应设备的设备。

[0077] 在密钥预分配期间，通过在根密钥材料和每个网络节点的标识符上应用本地密钥材料生成算法，为每个网络节点生成本地密钥材料并将其存储在网络节点上。在密钥导出阶段期间，两个网络节点可以通过在其本地密钥材料和另一网络节点的标识符上应用密钥建立算法来导出共享密钥。例如，第一节点可以将密钥建立算法应用在第二网络节点的第二标识符及其自己的第一本地密钥材料上，而第二节点可以将密钥建立算法应用在第一网络节点的第一标识符及其第二本地密钥材料上。密钥建立算法的结果是在两个网络节点之间共享的基于身份的密钥。

[0078] 存在多个基于身份的密钥预分配方案。例如,Oscar Garcia-Morchon,Domingo Gomez-Perez,Jaime Gutierrez,Ronald Rietman,Berry Schoenmakers和Ludo Tolhuizen发表于Cryptology ePrint Archive,Report 2014/698的“HIMMO-A lightweight collusion-resistant key pre-distribution scheme”中描述了基于身份的密钥预分配方案。在同一申请人的提交给EPO的欧洲专利申请“Improved system for key sharing”中描述了HIMMO的改进版本,该申请的代理人案卷号为2015PF001725。类似一些其他基于身份的密钥分配方案,HIMMO具有未处理的密钥可能稍微偏离的缺点。可以接受这一点,即,可以接受在小百分比中密钥协商可能失败。备选地,各方之一可以计算额外的密钥一致数据(还被称为助手数据),其能够是到达共享密钥所需。如果第一网络节点在开始计算共享密钥之前接收到第二网络节点身份,则密钥一致数据通常由具有对这两个身份的访问权的第一网络节点(例如,第一网络节点)生成。

[0079] HIMMO是基于隐藏信息(HI)和混合模块化操作(MMO)问题的基于身份的密钥预分配方案。HIMMO是轻量级和更量子安全的,因为所有现有攻击依赖于格。在HIMMO中,TTP具有一些秘密根密钥材料,例如,二元函数R(x,y)。TTP可以从其根密钥材料(G_A(x)=R(A,y),其中,该操作如在HIMMO中所描述地完成)提取用于节点A的秘密函数G_A(x)。当A和B希望建立公共密钥时,A评价G_A(x=B)并且B评价G_B(x=A)。

[0080] 在由Carlo Blundo等人的“Perfectly-Secure Key Distribution for Dynamic Conferences”中描述了另一可用的基于身份的密钥预分配方案。该方案具有以下优点:密钥协商不会失败,并且不需要密钥一致数据。另一方面,Blundo的方案针对共谋攻击是更没有弹性的。

[0081] 在实施例中,根密钥材料包括二元多项式并且本地密钥材料包括一元多项式。例如,在Blundo的基于身份的密钥预分配方案中,根密钥材料由二元多项式f(x,y)形成。本地密钥材料g和具有标识符ID_1的第一节点通过将二元多项式折叠到一元多项式g(y)=f(ID_1,y)形成。具有本地密钥材料g的节点和第二节点ID_2的标识符通过计算g(ID_2)获得共享密钥。所有多项式计算可以完成对模数m取模。

[0082] 一些基于身份的密钥预分配方案具有以下性质:从不同TTP接收但是针对兼容参数(例如,相同程度和模数)生成的本地密钥材料可以在本地网络节点处组合以形成新本地密钥材料。新本地密钥材料可以仅如由TTP直接生成的密钥材料一样使用,但是具有以下优点:新本地密钥材料尚未由分离的TTP中的任一个看到。在TTP被入侵的情况下,这使这样的组合的新本地密钥材料更安全。

[0083] 关于密钥预分配方案的问题在于,其生成对称密钥。因此,接收器可以伪造用于具有对称密钥的消息的消息认证码并且要求其从发送器接收消息,并且加密系统不具有证明消息欺骗的方式。

[0084] 图1a和图1b均示意性地示出了网络节点的实施例的范例。图1a中所图示的第一网络节点200被布置为与图1b中所图示的第二网络节点201合作。

[0085] 第一网络节点200包括密钥存储设备210,密钥存储设备210被布置为存储由基于身份的密钥预分配方案的本地密钥材料生成算法生成的本地密钥材料。密钥存储设备210包括两种不同类型的本地密钥材料;至少一个本地密钥材料用于每种类型。

[0086] 第一类型的本地密钥材料是保护第一网络节点与其他网络节点之间的通信的机

密性的本地密钥材料。该本地密钥材料先前已经由用于机密性的可信第三方(TTP)将基于身份的密钥预分配方案的本地密钥材料生成算法用于第一网络节点的第一身份生成。

[0087] 在系统中存在用于机密性的至少一个TTP,但是可以存在更多。图1a示出了用于机密性的两个TTP:TTP 292和TTP 294。对于使用的每个TTP,接收本地密钥材料。在这种情况下,密钥存储设备210存储对应于TTP 292和TTP 294的保护机密性的本地密钥材料212和214。可以存在用于机密性的单个TTP,例如,可以从系统移除除TTP 292之外的所有用于机密性的TTP。如果其内容不能在没有对相关密钥材料的访问权的情况下读取,则针对机密性保护通信。

[0088] 第二类型的本地密钥材料是保护第一网络节点与其他网络节点之间的通信的完整性的本地密钥材料。保护完整性的该本地密钥材料先前已经由用于完整性的TTP将基于身份的密钥预分配方案的本地密钥材料生成算法用于第一网络节点的第二身份生成。

[0089] 在系统中存在用于完整性的至少一个TTP,但是可以存在更多。图1a示出了用于完整性的两个TTP:TTP 296和TTP 298。对于使用的每个TTP,接收本地密钥材料。在这种情况下,密钥存储设备210存储对应于TTP 296和TTP 298的保护完整性的本地密钥材料216和218。可以存在用于完整性的单个TTP。例如,可以从系统移除除TTP 296之外的用于完整性的所有TTP。如果例如消息的内容不能在没有对相关密钥材料的访问权的情况下改变未检测,则针对完整性保护消息。

[0090] 用于机密性的TTP和用于完整性的TTP是不同的TTP。这意指其至少使用不同的根密钥材料。可能地,TTP的参数可以相同,使得本地密钥材料可以由节点组合。然而,重要的是,用于机密性的TTP不能生成对应于用于完整性的TTP的根密钥材料的本地密钥材料,并且更特别地,不能生成从由用于完整性的TTP生成的这样的本地密钥材料获得的共享密钥。一般而言,通过选择不同的秘密根密钥材料,该条件可以容易满足。例如,如果使用基于HIMMO或Blundo的系统,则根密钥材料可以包括不同的多项式。在实施例中,将用于机密性的(一个或多个)TTP和用于完整性的(一个或多个)TTP实施在物理上分离的服务器上。用于机密性的(一个或多个)TTP和用于完整性的(一个或多个)TTP可以位于不同的辖区(例如,不同的国家)中。不同TTP可以使用相同方案,但是具有不同的根密钥材料。为了组合密钥材料,一些密钥预分配方案要求TTP使用相同参数(例如模数)但不同的根密钥材料(例如,多项式、矩阵等)。通常,还要求针对相同第一或第二身份生成本地密钥材料。

[0091] 上文提到的第一网络节点的第一和第二身份是适于所使用的基于身份的密钥预分配方案的身份。通常,这些身份不是秘密,尽管本地密钥材料是秘密。身份可以与这样的标识信息相同或者根据这样的标识信息获得:序列号、网络地址(例如IP地址)、MAC地址、真实姓名等。可以根据主身份或者根据凭证生成第一和/或第二身份。例如,X.509证书(可能地没有签名的X.509证书)的散列可以被用作身份。根据标识信息导出身份具有由TTP隐式授权的优点。导出身份可以使用密钥导出函数(KDF)。KDF的范例在例如来自CMLA技术规范,版本:V1.43-20131218的CMLA_KDF或者在“DRM规范”,OMA-TS-DRM-DRM-V2_0_2-20080723-A,Open Mobile Alliance™,版本2.0.2,7.1.2章等中定义的KDF函数中给出。密钥导出函数可以应用于V的条目,例如,在连接之后。

[0092] 第一和第二身份可以存储在第一网络节点200的存储设备中(未分离地示出该存储设备)。备选地,可以导出第一和第二身份的信息可以存储在网络节点200处。

[0093] 在实施例中，第一和第二身份是相等的。实际上，这是实施似乎不具有对安全性的任何不利影响的系统的容易方式。

[0094] 如果使用允许本地密钥材料的组合的基于身份的密钥预分配方案，然后接收用于机密性的多个本地密钥材料或者用于完整性的多个本地密钥材料的网络节点，那么网络节点可以组合多个本地密钥材料并且存储组合的密钥材料，例如，用于机密性的组合的本地密钥材料和/或用于完整性的组合的本地密钥材料。然而，存在保持未组合的本地密钥材料并且根据需要稍后将其组合的优点。

[0095] 第一网络节点200包括通信接口220，通信接口220被布置用于第一网络节点与其他网络节点之间的数字通信。例如，其他节点可以是下文所描述的第二网络节点201。通信接口220可以被配置为通过数字网络(例如，无线网络(诸如Wi-Fi)或有线网络(诸如以太网)、或其组合)通信。例如，数字网络可以是传感器网络或者因特网等。本地密钥材料可以通过其通信接口(例如，通信接口220)被存储在网络节点上；然而，越界方法是可能的，例如，使用存储器设备(例如，记忆棒)传送，而通信接口220是无线网络接口等。

[0096] 第一网络节点200包括身份获得器241，身份获得器241被配置为获得第二网络节点(例如，第二网络节点201)的第一和第二身份。第二网络节点的第一和第二身份也可以是相同的。第二网络节点的第一和第二身份可以以导出第一和第二身份(例如，通过应用散列函数)的标识信息的形式获得。密钥身份、第一身份和/或第二身份可以从其他节点接收、从本地地址本检索、或者从在线地址本检索等。

[0097] 第一网络节点200被布置为向第二网络节点发送通信，例如，数字消息。例如，通信可以是数字消息，例如，网络消息、协议消息、电子邮件、文档等。

[0098] 第一网络节点200可以包括任选的组合器243。在存储设备210包括用于机密性的多个本地密钥材料或者用于完整性的多个本地密钥材料的情况下，组合器243获得用于机密性的单个本地密钥材料和用于完整性的单个本地密钥材料。

[0099] 例如，组合器243可以被布置为组合相同类型的本地密钥材料，针对其，已知第二网络节点具有从相同TTP接收(例如，根据相同根密钥材料生成)的本地密钥材料。例如，第一网络节点200能够已经利用其支持的TTP从第二网络节点201接收消息。在这种情况下，本地密钥材料可以被组合，如对方案适合的，例如，通过添加对模数取模。备选地，组合器243可以不组合但是选择可能地多个本地密钥材料之一，例如，针对每种类型，一个。如果仅用于机密性的单个TTP和用于完整性的单个TTP使用在系统中，那么不需要组合器243。

[0100] 第一网络节点200包括共享密钥单元244。共享密钥单元244被布置为计算两个密钥:保护机密性的第一共享密钥245和保护完整性的第二共享密钥246。

[0101] 保护机密性的第一共享密钥245是根据第二网络节点的第一身份和保护第一网络节点的机密性的本地密钥材料计算的。在实施例中，仅使用一个保护机密性的本地密钥材料，例如，保护机密性的本地密钥材料212。在实施例中，使用保护机密性的组合的本地密钥材料，例如，如由组合器243计算的。例如，共享密钥单元244可以被布置为将密钥建立算法应用到第二网络节点的第一身份和用于机密性的本地密钥材料。

[0102] 保护完整性的第二共享密钥246根据第二网络节点的第二身份和保护第一网络节点的完整性的本地密钥材料来计算。在实施例中，仅使用一个保护完整性的本地密钥材料，例如，保护完整性的本地密钥材料216。在实施例中，使用保护完整性的组合的本地密钥材

料，例如，如由组合器243计算的。例如，共享密钥单元244可以被布置为将密钥建立算法应用到第二网络节点的第二身份和用于机密性的本地密钥材料。

[0103] 如果基于身份的密钥预分配系统要求其，则共享密钥单元244还可以计算密钥一致数据。例如，在一些实例中，密钥一致数据可以是共享密钥的多个最低有效位(在这种情况下，共享密钥可以被选择为相应地更长以补偿秘密的损失)。在图1a中，任选密钥一致数据的发送由从共享密钥单元144到通信接口220的虚线指示。注意，一些方案(例如，Blundo)不要求密钥一致数据。

[0104] 第一网络节点200包括加密单元248。加密单元248被布置为使用第一共享密钥245加密消息。例如，加密单元248可以被布置为应用分组密码(例如，AES、三倍DES、Blowfish等)，分组密码可以被布置用于加密模式，例如，密码分组链接(CBC)、计数器模式(CTR)等。

[0105] 第一网络节点200包括MAC生成单元249。MAC生成单元249被布置为使用第二共享密钥246计算关于消息的第一消息认证码。例如，MAC生成单元249可以被布置为应用MAC算法，例如，基于散列算法(诸如SHA-1、SHA-256等)的HMAC，或者基于分组密码的MAC，例如，CBC-MAC，例如，基于AES、三倍DES、Blowfish等。

[0106] 存在可以关于消息生成MAC的许多方式。例如：

[0107] • MAC-then-Encrypt：计算关于明文消息的MAC，将其附加到消息，并且然后将整体加密。

[0108] • Encrypt-and-MAC：计算关于明文消息的MAC，将明文加密，并且然后将MAC附加在密码文本消息的末尾处。

[0109] • Encrypt-then-MAC:将明文加密，然后计算关于密文的MAC，并且将其附加到密文。注意，在这种情况下，初始化向量(IV)和加密方法标识符可以包括在MACed数据中。

[0110] 最后，加密消息和第一消息认证码通过通信接口220被发送到第二网络节点。如果需要密钥一致数据以保证第一和/或第二密钥的成功生成，那么密钥一致数据也可以发送到第二网络节点。例如，加密消息、第一消息认证码以及可能地密钥一致数据可以包括在一个较大消息中。

[0111] 注意，加密和MAC生成使用不同秘钥，其根据从不同TTP接收的本地密钥材料导出。如果例如从用于机密性的TTP获得用于机密性的TTP的根密钥材料和/或由用于第一网络节点的用于机密性的TTP生成的本地密钥材料，则已经拦截的消息可以由合法当局解密。然而，即使当局具有对该根/本地密钥材料的访问权，其不能欺骗关于这些消息的MAC。将此与机密性和完整性保护两者使用从相同TTP获得的密钥材料完成的系统相比较。在这样的情况下，可以解密消息的任何人必然也能够生成用于该消息的MAC码。换句话说，这样的系统中的合法当局具有伪造证据的能力。即使无合法当局将使用这样的能力，其也减少消息的值作为证据，只要因为其能够已经篡改。

[0112] 如果使用多个TTP，则额外的优点在于，所有TTP必须同意密钥材料的请求是合法的。这使更可能的是，仅执行用于密钥材料的合法正确请求，因为超过一个TTP要验证请求的合法性。

[0113] 图1b示意性地示出了第二网络节点201的实施例的范例，第二网络节点201被布置为与图1a中所图示的第一网络节点200合作。图1a中示出的第一网络节点200被布置为发送消息，而图1b中示出的第二网络节点200被布置为接收消息。图1a和图1b的实施例可以组合

以获得能够发送和接收消息两者的网络。

[0114] 第二网络节点201类似于网络节点200。下面解释了两者之间的突出差异中的一些。

[0115] 类似第一网络节点200,网络节点201还包括密钥存储设备260。密钥存储设备260还存储保护机密性的本地密钥材料和保护完整性的本地密钥材料。第二网络节点201能够已经从不同TTP接收其本地密钥材料,但是如果第一网络节点和第二网络节点要成功通信,则应当存在用于机密性的至少一个TTP和用于完整性的至少一个TTP的重叠。例如,如果仅使用用于机密性的单个TTP和用于完整性的单个TTP,则实现这一点。

[0116] 在图1a和图1b中图示的实施例中,示出了至少公共TTP 292和TTP 296。如果这是仅有公共TTP,那么对应的本地密钥材料要被使用。如果存在更多公共TTP,那么可以组合其本地密钥材料。

[0117] 第二网络节点201包括身份获得器271,身份获得器271被布置为获得第一网络节点的第一和第二身份。身份获得器271可以与身份获得器241相同工作。第一网络节点200的第一和第二身份可以与第一网络节点200的通信(例如,加密消息)一起被接收。身份获得器241和271还可以找到公共数据库、本地地址本等中的第一和/或第二身份。

[0118] 第二网络节点201包括例如与通信接口220相同或者类似类型的通信接口265。通过通信接口265,可以从第一网络节点200接收加密消息和第一消息认证码。

[0119] 第二网络节点201可以包括任选的组合器273以选择和/或组合由公共TTP生成的本地密钥材料。第二网络节点201包括共享密钥单元274,共享密钥单元274被布置为:

[0120] -根据第二网络节点的第一身份和保护第一网络节点的机密性的本地密钥材料来计算保护机密性的第一共享密钥245,

[0121] -根据第二网络节点的第二身份和保护第一网络节点的完整性的本地密钥材料计算保护完整性的第二共享密钥246。

[0122] 共享密钥单元274可以被布置为使用从第一网络节点200接收到的密钥一致数据来计算第一和/或第二身份。例如,密钥一致数据可以通过通信接口265接收,例如,与加密消息和/或第一MAC一起。这已经利用从接口265到共享密钥单元274的虚线图示。

[0123] 第二网络节点201包括解密单元278,解密单元278被布置为使用第一共享密钥将加密消息解密。第二网络节点201包括MAC验证单元279,MAC验证单元279被布置为使用第二共享密钥验证第一消息认证码。

[0124] 如果MAC验证单元279检测到MAC不正确的,则其可以唤起警报,例如,向第二网络节点201的用户发送错误消息,例如,向另一方(例如,向另一服务器等)发送警报消息。

[0125] 注意,第二网络节点201能够解密和验证消息的完整性。然而,合法拦截的消息可以选择性地仅被允许解密,这取决于对密钥材料的合法当局给出的访问权。

[0126] 因此,实施例具有以下优点:

[0127] (a)发送器和接收器可以加密和解密消息并且使用其本地密钥材料验证MAC。

[0128] (b)如果用于机密性的TTP同意,则合法拦截是可能的,而只要用于完整性的TTP不同意,通过合法拦截器欺骗是不可能的。

[0129] 图1c示意性地示出了第一网络节点202的实施例的范例。网络节点202建立在网络节点200上,但是利用另一有利功能扩展。第一网络节点202被配置为向第二网络节点发送

消息。对于接收节点(例如,第二网络),人们可以使用网络节点201,其已经适于忽略由根据图1c的实施例添加的任何额外的元件,例如,第二MAC(参见下文)。

[0130] 除了相对于图1a描述的元件之外,第一网络节点202包括另一身份获得器242。另一获得器242被配置为获得另一身份。另一身份与第二网络节点的第一和第二身份不同。重要的是,第二网络节点不具有对应于另一身份的本地密钥材料。在实施例中,还选择了与第一网络节点的第一和第二身份不同的另一身份。实际上,优选地,没有一个网络节点具有对对应于另一身份的本地密钥材料的访问权,其意指另一身份与由公共网络节点使用的任何身份不同地选择。在这种情况下,公共网络节点是不具有对对应于另一身份或者根密钥材料的本地密钥材料的访问权的网络。

[0131] 例如,可以选择另一身份,使得其对于第二网络节点未知,其隐含他也不具有对应的密钥材料。然而,存在选择具有不同优点的另一身份的许多不同方式。下文讨论了这些选项中的一些。

[0132] 共享密钥单元244被布置为根据另一身份和保护第一网络节点的完整性的至少本地密钥材料计算保护完整性的第三密钥247。例如,共享密钥单元244可以被布置为将密钥建立算法应用到另一身份和用于完整性的本地密钥材料来获得第三密钥247。MAC生成单元249被布置为使用第三密钥计算关于至少消息的第二消息认证码。最后,第二消息认证码被发送到第二网络节点,例如,与加密消息和第一消息认证码一起。备选地,第二消息认证码被发送到受信任当局,其受信任以保持第二MAC,使得如果这曾经是必要的,则可以证明消息的真实性。当向受信任当局发送例如用于完整性的TTP时,可以包括消息标识符,使得促进消息的稍后发现,例如,序列号、时间戳、消息的散列、可能甚至消息本身。还可以包括另一标识符。

[0133] 为了恢复第三密钥,人们可以使用:

[0134] A:另一身份和保护第一网络节点202的完整性的本地密钥材料,或者

[0135] B:对应于保护完整性的本地密钥材料的第一网络节点202的第二身份和通过生成保护第一网络节点202的完整性的本地密钥材料的相同(一个或多个)TTP针对另一身份生成的本地密钥材料。

[0136] 第一网络节点202能够计算第三密钥,因为他具有选项A的所有元素。第二网络节点不能计算第三密钥,因为第二网络节点既不具有选项A的元素(第二网络节点不具有对保护第一网络节点202的完整性的本地密钥材料的访问权),也不具有选项B的元素(第二网络节点不具有对应于另一身份的本地密钥材料,特别地另一身份与第二网络节点不具有本地密钥材料的身份不同)。

[0137] 结果,第二MAC提供消息尚未篡改并且真实地由第一网络节点202写入的良好保证:即使第三密钥是对称密钥,接收方(第二网络节点)不具有对第三密钥的访问权并且不能够欺骗第二MAC。这一点的副作用在于,第二网络节点也不能够验证第二MAC。这不一定是问题,但是特别地并非因为第二网络节点可以验证第一MAC。

[0138] 获得另一身份的一个选项是将另一身份获得器242配置为随机地选择另一身份。如果另一身份是随机的,则自动的是,其不等于第二网络节点的第一和第二身份。在实施例中,选择身份的位大小,使得随机分配的身份之间的冲突是不可能的。在该情况下,而且,随机选择的另一身份将不能够等于另一节点的身份。例如,身份的位大小可以根据系统中的

网络节点的数目和/或期望通信的数目来选择。例如，身份可以是32位、64位、128位、256位或更多等。

[0139] 有趣的是，通过选择随机另一身份，还应确保对应的本地密钥材料尚未由用于保护完整性的(一个或多个)TTP生成。这意指在计算第二MAC时，第一网络节点202是具有对第三密钥的访问权的仅有网络节点。仅当用于保护完整性的(一个或多个)TTP决定计算对应于另一身份的本地密钥材料时，对于其他实体而言计算第三密钥变得可能。因此，该选项给出第二MAC(如果其是正确的)真实地由第一网络节点计算的高保证。代替于完全随机地选择另一身份，其还可以从一些大集选择。

[0140] 第一网络节点202被配置为向第二网络节点或者受信方发送另一身份。以这种方式，将需要稍后计算第三密钥(比如在诉讼案件的情况下)以验证合法拦截的另一身份可用于可以拦截第一地点中的消息的任何拦截器。这同样适用于其需要的密钥一致数据。

[0141] 存在避免发送另一身份并且因此减少由系统引起的开销的各种方式。例如，另一身份可以是固定身份，或者选自允许另外身份的小集合。在这种情况下，另一身份可以为所有或许多网络节点所知。这不是问题，因为网络节点仍然不具有针对另一身份生成的本地密钥材料。这样的密钥材料将被需要以计算第三密钥(与第一网络节点的第二身份一起)。

[0142] 作为另一范例，另一身份可以根据消息自身生成，例如，通过将散列函数应用到消息或KDF等。在实施例中，随机盐在从其导出另一身份之前附接到消息，例如，通过将散列应用到消息和盐的组合。这具有以下优点：另一身份可以根据期望从消息计算，并且因此不需要传送。同时，另一身份具有随机字符，使得不可能尚未生成对应的本地密钥材料。盐可以具有比另一身份更小的位大小，例如，32和64位等。较大的身份是可能的，例如，128位。如果使用盐，则其可以被传递到接收第二MAC的任何方(例如，第二网络节点)。

[0143] 有趣的是，另一身份可以被选择为第一网络节点202的第二身份。注意，通常，密钥根据另一方的身份和一方自己的密钥材料导出。通过根据一方自己的身份和密钥材料计算密钥，获得不能通过任何其他方重新计算的密钥，除了如果其具有对第一网络节点的本地密钥材料的访问权之外。后者将不是针对公共网络节点的情况。然而，用于完整性的保护的(一个或多个)TTP能够计算用于任何身份的本地密钥材料并且因此还可以计算第三密钥。

[0144] 在另一身份已经知道或者可以从消息导出的这些情况下，其不需要向第二网络节点发送另一身份。如果使用盐，则但是其可能需要发送盐。

[0145] 第二MAC在消息上计算，但是如上文对于第一消息认证，存在这样做的各种方式。例如，第二MAC直接在消息的明文上、在加密消息上、在消息与第一MAC上、在加密消息与第一MAC上等计算。在实施例中，第二消息认证码在至少消息和第一消息认证码上计算。后者选项允许验证第一MAC是否改变而不需要知道用于计算第一MAC的密钥。

[0146] 在实施例中，第二AMC在至少明文消息上计算，并且可能地第一MAC。这具有以下优点：用于完整性的TTP可以仅验证并且因此仅改变MAC，如果其具有对明文的访问权。然而，用于完整性的TTP自己不能获得纯文本。TTP取决于用于机密性的TTP。以这种方式，两种类型的TTP彼此保持平衡。

[0147] 计算第三密钥的本地密钥材料可以是计算第二共享密钥的相同本地密钥材料。而且对于第三密钥，可以组合多个TTP的本地密钥材料。实际上，对于第三密钥，甚至不需要确保第二网络节点具有来自相同TTP的密钥材料。在实施例中，而且用于机密性的TTP的本地

密钥材料与用于完整性的TTP的本地密钥材料混合。例如,在实施例中,组合器243被配置为将用于机密性的本地密钥材料和用于完整性的本地密钥材料组合,从而形成组合的本地密钥材料,第三密钥从另一身份和组合的本地密钥材料导出。

[0148] 组合更多本地密钥材料具有以下优点:篡改消息上的MAC对于欺诈TTP变得更难,因为已经使用其本地密钥材料的所有TTP需要参与欺诈。

[0149] 一些密钥预分配方案不具有直接组合本地密钥材料的选项。即使利用组合,这样的方案也可以使用在实施例中,然而,在这种情况下,第一中间密钥分离地针对本地密钥材料计算,其然后组合以形成单个密钥。后者组合可以通过任何密钥导出算法(例如,KDF、或者中间密钥上的直接XOR)完成。例如,在实施例中,共享密钥单元244被配置为通过首先根据另一身份和保护第一网络节点的完整性的本地密钥材料获得中间第三密钥并且将中间第三密钥与第一密钥组合来计算第三密钥。

[0150] 本发明通过例如以下方面中的一个或多个解决多个问题:(a)使用未被用于消息的主体的消息上的MAC的至少1个额外的TTP;和(b)通过发送器将第二消息包括在消息中,未寻址到接收器,但是到仅仅由该额外的TTP管理的另一身份,该消息再次包括消息上的MAC。另一身份可以是第二MAC寻址到的一方的身份,但是这是不必要的。

[0151] 注意,合法拦截实体可以检查欺骗的接收器是否通过将用于另一身份的MAC解密接收消息。合法拦截实体不能伪造该信息。

[0152] 此外,消息常常穿过可以具有关于合法拦截的不同规则的多个辖区。使用本发明的实施例,每个辖区可以得到其要求的拦截和/或验证能力;例如,通过使用适当的辖区的TTP生成第二MAC。例如,多个第二MAC可以在不同的辖区中使用TTP生成。

[0153] 图2示意性地示出了通信系统195的实施例的范例。

[0154] 通信系统195包括多个网络节点。在图2中示出了第一网络节点100和第二网络节点150。可以存在更多网络节点,例如,超过100、1000、10000等。

[0155] 通信系统195包括至少两个TTP:用于机密性的可信第三方192,以及用于完整性的可信第三方194。可以存在每种超过一个TTP。

[0156] 网络节点被配置为通过数字网络190彼此通信,例如,以彼此发送数字消息。网络节点具有被配置为通过数字网络190向其他网络节点通信的通信接口。在图2中示出了第一网络节点110中的通信接口120和第二网络节点150中的通信接口170。

[0157] 在实施例中,网络节点被配置为利用从不同TTP获得的本地密钥材料保护消息的机密性和完整性。本地密钥材料可以存储在密钥存储设备中。密钥存储设备可以是非易失性电子存储器、磁或光存储等。在图2中示出了第一网络节点110中的密钥存储设备110和第二网络节点150中的密钥存储设备160。

[0158] 每个网络节点包括处理器电路。在图2中示出了第一网络节点110中的处理器电路130和第二网络节点150中的处理器电路180。处理器电路被配置为根据实施例针对机密性和完整性保护消息,并且解密和验证消息。例如,处理器电路可以被配置用于利用图1a、1b和1c中的任一项图示的实施例。

[0159] 图3示意性地示出了保护完整性的可信第三方设备400的实施例的范例。在使用用于完整性的单个TTP并且网络节点不混合多个TTP的本地密钥材料以获得第三密钥的情况下,可以使用该TTP设备400。如果本地密钥材料是混合的,则其他方法是可能的。例如,TTP

可以将本地密钥材料(例如,如下文所计算的)提供给另一TTP,所述另一TTP组合本地密钥材料,计算第二或第三密钥并且验证第一或第二MAC。

[0160] TTP 400包括被布置为存储根密钥材料的密钥存储设备410。根密钥材料根据使用的密钥预分配方案。根据根密钥材料和身份,可以计算本地密钥材料。

[0161] TTP 400包括两个通信接口:第一通信接口422和第二通信接口424。这些可以通过出于多个目的共享单个通信接口实施,但是不需要这样。

[0162] 可以以不同的方式保护第一通信接口和第二通信接口。例如,可以使用第一通信接口,例如,在生产环境中,其中,用于本地密钥材料的大量的请求由少量的请求者(例如,移动电话、智能卡等的制造商)制成。例如,为了容纳该需求,第一通信接口可以是请求者认证自身(例如,使用常规X.509验证系统)的数字计算机网络接口。可以使用第二通信接口,例如,通过法律实施。第二通信接口可以以与第一通信接口(例如,受保护的数字计算机网络接口)类似的方式完成,但是其也可以是不同的。

[0163] 例如,第二通信接口424可以使用所谓的带外机构实施,其要求对TTP400的特殊访问,例如,通过服务器的本地访问,例如,通过本地键盘、本地usb端口等。第一通信接口和第二通信接口两者可以要求某种类型的认证,例如,密码认证令牌、软件狗等。

[0164] 第一通信接口422被布置为接收第二身份442。第二身份442对应于保护完整性的本地密钥材料要被计算的网络节点的第二身份。

[0165] TTP 400包括本地密钥材料生成器432。本地密钥材料生成器432被配置为通过将基于身份的密钥预分配方案的本地密钥材料生成算法应用到第二身份和根密钥材料计算保护完整性的第一本地密钥材料。

[0166] 第一通信接口422和本地密钥材料生成器432可以使用在TTP 400中以计算用于网络节点的本地密钥材料。例如,TTP 400可以使用在制造网络节点中,并且给网络节点提供本地密钥材料。例如,TTP 400可以使用通信接口422对用于包括具有对应的本地密钥材料的身份442的本地密钥材料的请求作出反应。除对应于身份442的网络节点之外,本地密钥材料对于所有网络节点是秘密的,因此应当采取适当的护理来保护TTP 400和其接口。

[0167] 第二通信接口424被布置为接收发送第二身份和接收第二身份。发送第二身份和接收第二身份一起被指示为444。第二通信接口424还被布置为接收消息,以及消息认证码。消息和消息认证码一起被指示为446。发送第二身份444对应于网络节点的第二身份,其使用其先前生成的本地密钥材料和接收第二身份(例如,第二网络节点的接收第二身份),以计算用于消息的MAC(上文被称为第一MAC)。该第一MAC要被验证。TTP 400包括AMC验证单元434,其被布置为使用第二共享密钥验证消息认证码和消息446的组合。

[0168] 存在要进行的针对TTP 400的至少两种方式。

[0169] 在第一选项中,本地密钥材料生成器432被配置为通过将基于身份的密钥预分配方案的本地密钥材料生成算法应用到根密钥材料和发送第二身份计算保护完整性的第二本地密钥材料。在这种情况下,获得与如由发送网络节点使用的相同的本地密钥材料。MAC验证单元434被布置为根据保护完整性的第二本地密钥材料和接收第二身份计算第二共享密钥,

[0170] 在第二选项中,本地密钥材料生成器432被配置为通过将基于身份的密钥预分配方案的本地密钥材料生成算法应用到根密钥材料和接收第二身份计算保护完整性的第二

本地密钥材料。MAC验证单元434被布置为根据保护完整性的第二本地密钥材料和发送第二身份计算第二共享密钥，

[0171] 一旦MAC验证单元434已经验证关于消息的MAC，则其可以发送适当的响应消息，例如，其指示MAC是或不是正确的。

[0172] 该TTP 400具有以下优点：无密钥材料需要公开来验证MAC。类似地，TTP 400可以要么根据发送消息的第一网络节点的第二身份要么根据由第一(发送)网络节点选择的另一身份验证第二MAC。另一身份可以通过第二通信接口424接收，例如，如果另一身份是随机身份，或者另一身份可以由TTP 400已知(例如，被存储在TTP 400的本地存储设备中)，或者另一身份可以根据消息计算。

[0173] 图4示意性地示出了保护完整性300的可信第三方设备的实施例的范例。TTP 300可以以与TTP 400相同的方式工作。TTP 400包括密钥存储设备310，例如，(非易失性)电子存储器，例如，磁或光存储设备等。TTP 300包括第一通信接口322和第二通信接口324。通信接口可以是网络接口、键盘、通信端口(例如，usb端口)等。TTP 300包括根据实施例(例如，图3图示的实施例)配置的处理器电路330。

[0174] 发明人已认识到，以下条款也是有利的。因此，申请人给出以下通知：新权利要求可以阐述为这样的条款和/或这样的条款的组合和/或在本申请和/或从其导出的任何另一申请的起诉期间从本描述取得的特征。

[0175] 条款1：一种第一网络节点(100;200)，包括：

[0176] -密钥存储设备(110;160;210;260)，其被布置为存储至少本地密钥材料(216、218;217)，其保护第一网络节点与其他网络节点之间的通信的完整性，保护完整性的本地密钥材料由用于完整性的第三方(TTP)(194;296、298;297)将基于身份的密钥预分配方案的本地密钥材料生成算法用于第一网络节点的第二身份生成，

[0177] -通信接口(120;170;220;265)，其被布置用于第一网络节点与其他网络节点之间的数字通信，以及

[0178] -处理器电路(130)，其被配置为：

[0179] -获得例如与第二网络节点的第一和第二身份不同的另一身份，

[0180] -根据另一身份和保护第一网络节点的完整性的至少本地密钥材料计算保护完整性的第三密钥(247)，

[0181] -使用第三密钥计算关于至少消息的第二消息认证码，

[0182] -例如向第二网络节点发送第二消息认证码。

[0183] 条款2、根据条款1所述的第一网络节点，其中，所述处理器电路(130)被配置为：

[0184] -获得第二网络节点的第二身份(150;201)，

[0185] -根据第二网络节点的第二身份和保护第一网络节点的完整性的本地密钥材料计算保护完整性的第二共享密钥(246)，

[0186] -使用第二共享密钥计算关于消息的第一消息认证码，以及

[0187] -向第二网络节点发送消息和第一消息认证码，

[0188] 根据条款1或2所述的第一网络节点可以与权利要求3-7中的任一项组合。此外，第一网络节点可以利用来自用于机密性的TTP的本地密钥材料扩展以加密消息。

[0189] 图5示意性地示出了用于第一网络节点(诸如第一网络节点100、200、202)的电子

通信方法500的实施例的范例。

[0190] 方法包括：

[0191] -存储510至少：

[0192] -本地密钥材料(212、214;213)，其保护第一网络节点与其他网络节点之间的通信的机密性，保护通信的本地密钥材料由用于机密性的第三方(TTP)(192;292、294;293)将基于身份的密钥预分配方案的本地密钥材料生成算法用于第一网络节点的第一身份生成，以及

[0193] -本地密钥材料(216、218;217)，其保护第一网络节点与其他网络节点之间的通信的完整性，保护完整性的本地密钥材料由用于完整性的第三方(TTP)(194;296、298;297)将基于身份的密钥预分配方案的本地密钥材料生成算法用于第一网络节点的第二身份生成，

[0194] 方法500还包括：

[0195] -获得520第二网络节点的第一和第二身份(150;201)，

[0196] -根据第二网络节点的第一身份和保护第一网络节点的机密性的本地密钥材料计算525保护机密性的第一共享密钥(245)，

[0197] -根据第二网络节点的第二身份和保护第一网络节点的完整性的本地密钥材料计算530保护完整性的第二共享密钥(246)，

[0198] -使用第一共享密钥加密535消息，

[0199] -使用第二共享密钥计算540关于消息的第一消息认证码，以及

[0200] -向第二网络节点发送545加密消息和第一消息认证码，

[0201] 方法500还或代替地可以包括：

[0202] -从第二网络节点接收550加密消息和第一消息认证码，

[0203] -获得555第二网络节点的第一和第二身份，

[0204] -根据第二网络节点的第一身份和保护第一网络节点的机密性的本地密钥材料计算560保护机密性的第一共享密钥(245)，

[0205] -根据第二网络节点的第二身份和保护第一网络节点的完整性的本地密钥材料计算565保护完整性的第二共享密钥(246)，

[0206] -使用第一共享密钥解密570加密消息，

[0207] -使用第二共享密钥验证575第一消息认证码，

[0208] 图6示意性地示出了用于完整性的电子可信第三方(TTP)方法600的实施例的范例。方法600包括：

[0209] -存储610根密钥材料，

[0210] -接收620第二身份，

[0211] -接收630消息、消息认证码、发送第二身份和接收第二身份，

[0212] -通过将基于身份的密钥预分配方案的本地密钥材料生成算法应用到第二身份和根密钥材料计算640保护完整性的第一本地密钥材料，

[0213] -通过将基于身份的密钥预分配方案的本地密钥材料生成算法应用到根密钥材料和发送第二身份计算650保护完整性的第二本地密钥材料，根据保护完整性的第二本地密钥材料和接收第二身份计算第二共享密钥。代替于阶段650，方法还可以执行以下阶段：通过将基于身份的密钥预分配方案的本地密钥材料生成算法应用到根密钥材料和接收第二

身份计算660保护完整性的第二本地密钥材料，并且根据保护完整性的第二本地密钥材料和发送第二身份计算第二共享密钥，并且

[0214] -使用第三密钥验证670关于消息的消息认证码。

[0215] 下文描述了额外的实施例。用于机密性的TTP在本文中还被称为主体TTP或bTTP。用于完整性的TTP在本文中还被称为MAC TTP或mTTP。实施例中的一些具有以下方面中的一个或多个：

[0216] -使用未被用于消息的主体的消息上的MAC的至少1个额外的TTP，使得控制消息是能够仅被拦截(加密/机密性)还是欺骗(认证)是可能的。

[0217] -将寻址到至少由该额外的TTP管理的第三方身份的子消息包括在消息中，该消息包括关于消息主体的MAC。该第三方的密钥材料优选地由额外的TTP分配到额外的TTP外部的任何方。作为选项，其可以甚至是由发送器选择的随机身份(例如，从非常大的空间取得的)。

[0218] -仅将密钥材料从消息主体TTP提供给合法拦截官员，

[0219] -通过将寻址到第三方身份的子消息解密并且检查MAC匹配消息的主体，验证消息由发送器而非接收器发送。这可以使用发送器或者(随机选择的)第三方实体的密钥材料完成。

[0220] -在要求拦截能力的辖区之间复制根密钥材料，并且对于想要传递到辖区2中的B的辖区1中的A方，仅使用在辖区1与2之间共享的消息TTP的主体。

[0221] 实施例中的一些提供以下效果中的一个或多个：

[0222] (a)发送器和接收器两者可以使用消息和MAC TTP的本地密钥材料(KM)将消息和MAC两者加密和解密。

[0223] (b)如果消息TTP同意提供相关密钥材料，则合法拦截是可能的，而由合法拦截器造成的欺骗是不可能的，只要其不具有对MAC TTP的密钥材料的访问权。

[0224] (c)如果在2个(或更多个)辖区之间共享TTP的根密钥材料，则这些辖区可以独立地决定拦截完全由从这些TTP导出的密钥材料保护的消息。

[0225] (d)使用来自MAC TTP或者选定的第三方的信息，人们可以通过将发送到第三方身份的MAC解密检查接收器是否欺骗接接收消息-接收器将不具有使得其能够为此生成适当的密钥的密钥材料。

[0226] 下面是这实际上可以如何使用的第一范例：

[0227] 1、在操作阶段中，发送器和接收器照常通信。其使用MAC验证消息的完整性。

[0228] 2、如果要求用于A方的合法拦截，则消息TTP会将例如A方的本地密钥材料(KM_A)提供给拦截方。只要一个TTP拒绝共享其KM_A，无拦截可以发生，这自动地隐含检查&平衡被改进。MAC TTP不需要共享用于要发生的拦截的任何信息。

[0229] 3、如果由A发送的消息在法庭上用作证据，则可以证明消息尚未欺骗。

[0230] a、拦截方不能欺骗自/至A的消息，因为其未得到对来自MAC TTP的密钥材料的访问权，因此拦截方可以读取&写入消息主体，但是拦截方不能验证或者有意义地写入MAC。

[0231] b、B方也不能欺骗来自A的接收消息，因为其不具有来自随机选定的第三方身份的MAC密钥材料。

[0232] c、法庭可以验证消息未欺骗，例如，通过还从MAC TTP检索本地密钥材料。备选地，

MAC TTP或者选定的第三方身份可以解密和/或验证发送到第三方身份的消息。

[0233] 下面公开了更详细的实施例。系统包括以下四种不同类型的实体：

[0234] 1、客户端C：将消息发送到彼此和从彼此接收消息的设备。

[0235] 2、主体可信第三方bTTP：充当用于保护客户端之间的消息的主体的(一个或多个)可信根的一个或多个服务器。

[0236] 3、MAC可信第三方mTTP：充当用于保护各方之间的MAC的(一个或多个)可信根的一个或多个服务器。

[0237] 4.法律实施L：具有解密自/至客户端的消息的合法权限的一个或多个方。

[0238] 任选地，TTP首先需要编入L以得到对向客户端发出密钥材料的许可。

[0239] 在配准阶段期间，客户端C_a可以通过从所有主体可信第三方bTTPi检索主体密钥材料bKM_a_i自身进行配置。客户端C_a类似地从所有mTTPi检索MAC密钥材料mKM_a_i。获得该密钥材料可以使用相同申请人的EP专利申请“System and method for distribution of identity based key material and certificate”(EP16162597、申请日期2016年3月29日、代理人案号2016P00212EP，通过引用包括在本文)中描述的系统，例如，通过将公共密钥或其散列包括在请求中安全地检索密钥材料，例如，使用根据其权利要求1所述的系统。

[0240] 在操作阶段期间，可以执行以下阶段：

[0241] •客户端C_a计算三个密钥以与客户端C_c通信：

[0242] 主体密钥bK＝所有bKM_a_i(c)的和。

[0243] MAC密钥mK＝所有mKM_a_i(c)的和+bK。注意，+根据密钥预分配方案的规格执行。备选地，密钥材料也可以以不同的方式组合，例如借助于异或或者密钥导出函数。

[0244] 发送器密钥sK(任选的)

[0245] 挑选第三方身份t(随机或预分配的)

[0246] sK＝所有bKM_a_i(t)的和+所有mKM_a_i(t)的和

[0247] •客户端C_a利用mK计算主体上的MAC

[0248] •客户端C_a利用bK:enc_主题|m_MAC(其中，“|”指代连接)将消息的主体加密到C_c和C_a：

[0249] •客户端C_a利用sK:s_MAC计算(任选的)enc_主体上的MAC|m_MAC。注意，作为选项，用于计算sK的另一身份t可以被取得为enc_主体+m_MAC的散列，从而消除传送额外的信息并且隐含地链接信息的需要。

[0250] 另一选项是从绝不由MAC TTP分发的地址范围选择该t。

[0251] 用于t的备选选项是固定的t，或者客户端A信任以保持其KM安全的t(例如，公证人)。

[0252] •客户端C_a向C_b发送消息[enc_主体，m_MAC，{t}，s_MAC]。后者两个参数是任选的。此处，{t}指示如果其被计算为enc_主体+m_MAC的散列，或者如果其被固定在协议中，则这是任选参数。

[0253] •客户端C_c计算两个密钥：

[0254] 主体密钥bK＝所有bKM_c_i(a)的和。

[0255] MAC密钥mK＝所有mKM_c_i(a)的和+bK。

[0256] 如果需要的话，使用密钥一致，

[0257] C_c现在可以使用bK解密enc_主体和m_MAC,并且使用mK验证m_MAC。

[0258] C_c忽略t,s_MAC。

[0259] 对于合法拦截,我们可以在机密性与完整性之间进行区分,

[0260] 在合法拦截(机密性)的情况下:在该用例中,法律允许拦截但是没有消息的修改。

[0261] •L从所有bTTPi检索bKM_a_i,如果L具有解密来自C_a的消息的权限。

[0262] 备选地,如果L仅对C_a与C_b之间的通信感兴趣,则L仅检索根据bKM_a_i生成的对应密钥。

[0263] •在接收到C_a与C_c之间的消息时,L现在计算一个密钥

[0264] 主体密钥bK=所有bKM_a_i(c)的和。

[0265] L可以使用bK解密enc_主体。

[0266] 合法拦截(完整性):

[0267] 在该用例中,法律允许拦截和验证(并且可能地甚至修改)消息。

[0268] •L从所有bTTPi检索bKM_a_i并且从所有mTTPi检索mKM_a_i,如果L具有解密并且修改来自C_a的消息的权限。

[0269] 备选地,如果L仅对C_a与C_b之间的通信感兴趣,则L仅检索用于该通信链路的对应密钥。注意,这不允许生成sK。

[0270] •在接收到C_a与C_c之间的消息时,L现在计算一个密钥

[0271] 主体密钥bK=所有bKM_a_i(c)的和。

[0272] MAC密钥mk

[0273] •L可以使用bK解密enc_主体。L还可以创建任何消息并且将其注入在通信链路中。

[0274] 为了验证消息源,例如,证明消息[enc_主体,m_MAC,t,s_MAC]由C_a发送到C_c(而非反之亦然)。可以完成以下内容:

[0275] •计算sK'=所有bKM_t_i(a)的和+所有mKM_t_i(a)的和

[0276] •L可以从sK'和一致数据获得sK。

[0277] •验证来自enc_主体+m_MAC的s_MAC'并且将其与接收到的s_MAC相比较。

[0278] 在各种实施例中,输入接口可以选自各种备选方案。例如,输入接口可以是局域网或者广域网(例如,因特网)的网络接口、内部或者外部数据存储的存储接口、键盘等。

[0279] 通常,设备200、201、202和400均包括微处理器(未分离地示出在图1a-1c和图3中),其执行存储在设备处的适当的软件;例如,该软件可以下载和/或存储在对应的存储器(例如,易失性存储器(诸如RAM)或者非易失性存储器(诸如闪存)(未分离地示出))中。备选地,设备200、201、202和400可以全部或者部分地以可编程逻辑实现,例如,作为现场可编程门阵列(FPGA)。设备可以全部或者部分地被实施为所谓的专用集成电路(ASIC),即,针对其特定使用定制的集成电路(IC)。例如,电路可以以CMOS实施,例如,使用硬件描述语言,诸如Verilog、VHDL等。

[0280] 在实施例中,设备200可以包括密钥存储设备电路、通信接口电路、身份获得器电路、组合器电路、共享密钥电路、加密电路、MAC生成电路。实施例还可以包括另一身份获得者电路。设备201可以包括来自根据需要适配的设备200的适当的电路和解密电路、MAC验证电路。TTP 400可以包括密钥存储设备电路、第一通信接口电路、第二通信接口电路、本地密

钥材料生成器电路和MAC验证单元电路。

[0281] 电路实施本文所描述的对应单元。电路可以是处理器电路和存储电路，处理器电路运行电子地表示在存储电路中的指令。电路还可以是FPGA、ASIC等。

[0282] 执行根据实施例的方法的许多不同方式是可能的，如对于本领域技术人员将显而易见的；包括方法500和600。例如，可以改变步骤的顺序或者可以并行执行一些步骤。此外，在步骤之间可以插入其他方法步骤。插入的步骤可以表示诸如本文描述的方法的细化，或者可以与该方法无关。此外，在下一步骤开始之前，给定步骤可能尚未完全完成。

[0283] 根据本发明的方法可以使用软件执行，其包括用于使得处理器系统执行根据实施例的方法(诸如方法500或者600)的指令。软件可以仅包括由系统的特定子实体采取的那些步骤。软件可以存储在合适的存储介质中，例如硬盘、软盘、存储器、光盘等。软件可以作为信号沿着线、无线或使用数据网络(例如，因特网)发送。该软件可以可用于下载和/或在服务器上远程使用。可以使用位流来执行根据本发明的方法，该位流被布置为配置可编程逻辑，例如，现场可编程门阵列(FPGA)，以执行该方法。

[0284] 将意识到，本发明还扩展到计算机程序，特别是适于将本发明付诸实践的载体上或载体中的计算机程序。程序可以采取源代码、目标代码、代码中间源和诸如部分编译形式的目标代码的形式，或者适用于实现根据本发明的方法的任何其他形式。涉及计算机程序产品的实施例包括与阐述的方法中的至少一个的处理步骤中的每个相对应的计算机可执行指令。这些指令可以细分为子例程和/或存储在可以静态或动态链接的一个或多个文件中。涉及计算机程序产品的另一实施例包括与阐述的系统和/或产品中的至少一个的模块中的每个相对应的计算机可执行指令。

[0285] 图7a示出了具有包括计算机程序1020的可写部件1010的计算机可读介质1000，计算机程序1020包括用于使得处理器系统执行根据实施例的通信方法或者TTP方法的指令。计算机程序1020可以根据物理标记或者借助于计算机可读介质1000的磁化被实现在计算机可读介质1000上。然而，任何其他适合的实施例也是可以想象的。此外，将意识到，尽管计算机可读介质1000此处被示出为光盘，但是计算机可读介质1000可以是任何适合的计算机可读介质(诸如硬盘、固态存储器、闪存等)，并且可以是非可记录或可记录的。计算机程序1020包括用于使处理器系统执行所述通信方法或者TTP方法的指令。

[0286] 图7b示意性地示出了根据实施例的处理器系统1140的表示。处理器系统包括一个或多个集成电路1110。在图7b中示意性地示出了一个或多个集成电路1110的架构。电路1110包括处理单元1120(例如，CPU)，其用于运行计算机程序部件以执行根据实施例的方法和/或实施其模块或者单元。电路1110包括用于存储编程代码、数据等的存储器1122。存储器1122的部分可以是只读的。电路1110可以包括通信元件1126，例如，天线、连接器或者两者等。电路1110可以包括用于执行方法中定义的处理的部分或全部的专用集成电路1124。处理器1120、存储器1122、专用IC 1124和通信元件1126可以经由相互连接1130(比如说总线)彼此连接。处理器系统1110可以被布置用于分别地使用天线和/或连接器的接触和/或无接触通信。

[0287] 例如，在实施例中，第一网络节点或者TTP设备可以包括处理器电路和存储器电路，处理器被布置为运行存储在存储器电路中的软件。例如，处理器电路可以是Intel Core i7处理器、ARM Cortex-R8等。存储器电路可以是ROM电路、或者非易失性存储器，例如，闪

存。存储器单元可以是易失性存储器(例如,SRAM存储器)。在后者情况下,设备可以包括非易失性软件接口(例如,硬盘驱动器、网络接口等),其被布置用于提供软件。

[0288] 应当注意,上文所提到实施例图示而不是限制本发明,并且本领域的技术人员将能够设计许多备选实施例。

[0289] 在权利要求中,括号内的任何附图标记不应被解释为对权利要求的限制。动词“包括”及其变形词的使用不排除权利要求中记载的元件或步骤之外的元件或步骤的存在。元件前面的词语“一”或“一个”不排除存在多个这样的元件。本发明可以借助于包括若干不同元件的硬件和借助于适当编程的计算机来实施。在列举了若干模块的设备权利要求中,这些模块中的若干个可以由同一个硬件项来实现。在互不相同的从属权利要求中记载了特定措施的仅有事实并不指示不能有利地使用这些措施的组合。在权利要求中,括号中的参考涉及示范性实施例的附图中的附图标记或实施例的公式,从而增加了权利要求的可理解性。这些参考不应解释为对权利要求的限制。

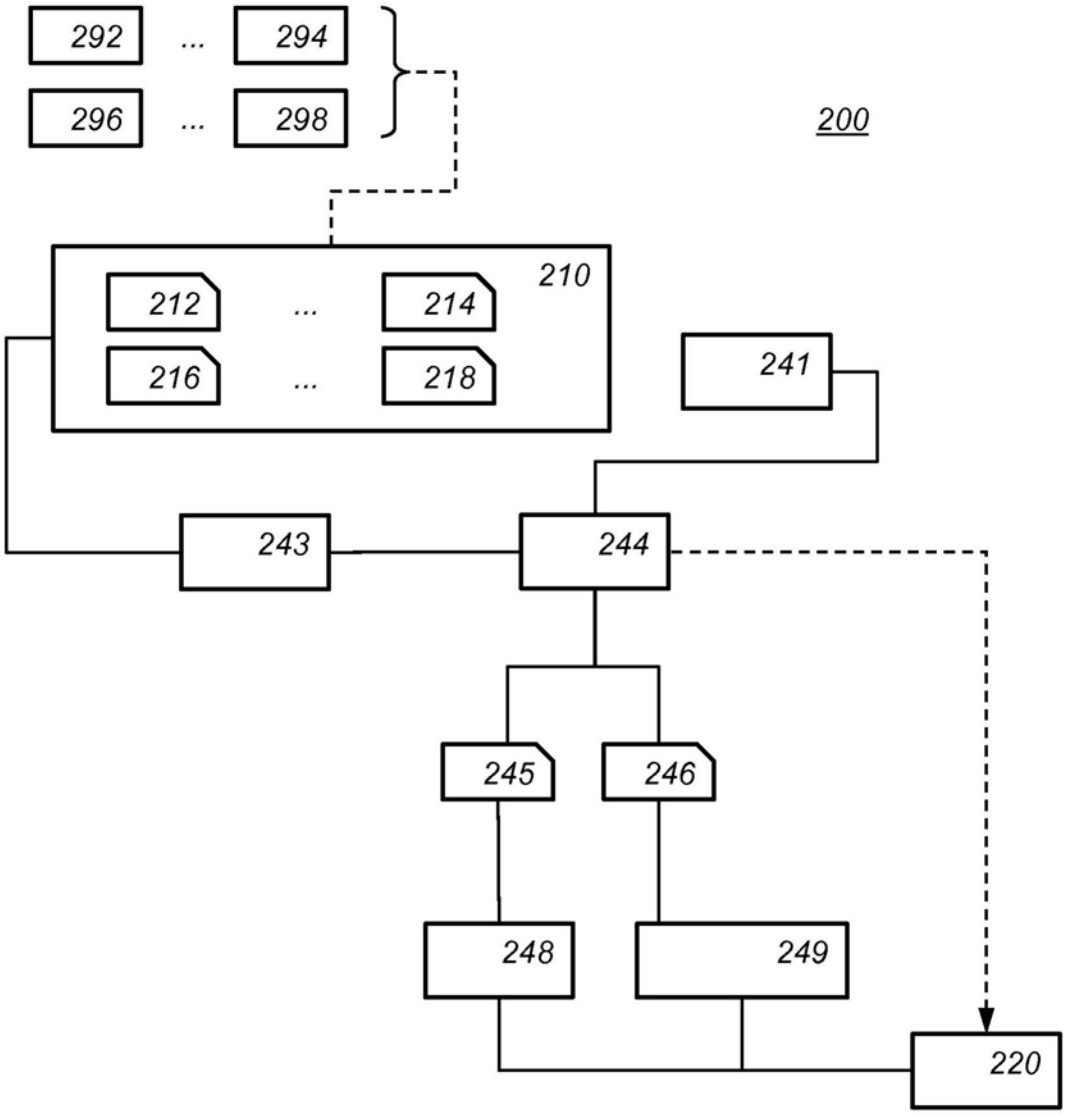

292
...
294
296
...
298
200
210
212
...
214
216
...
218
241
243
244
245
246
248
249
220

图1a

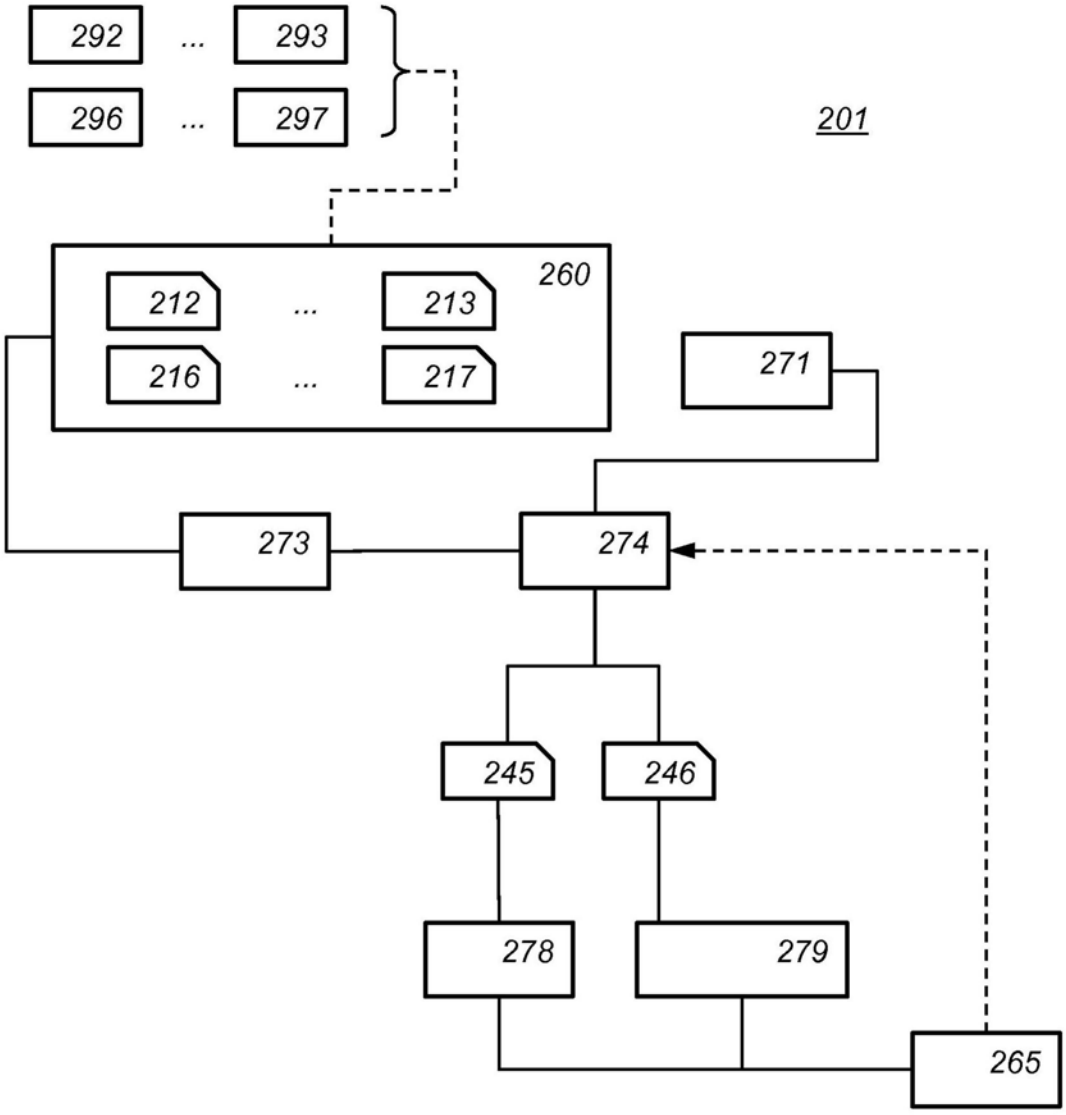

292
...
293
296
...
297
201
260
212
...
213
216
...
217
271
273
274
245
246
278
279
265

图1b

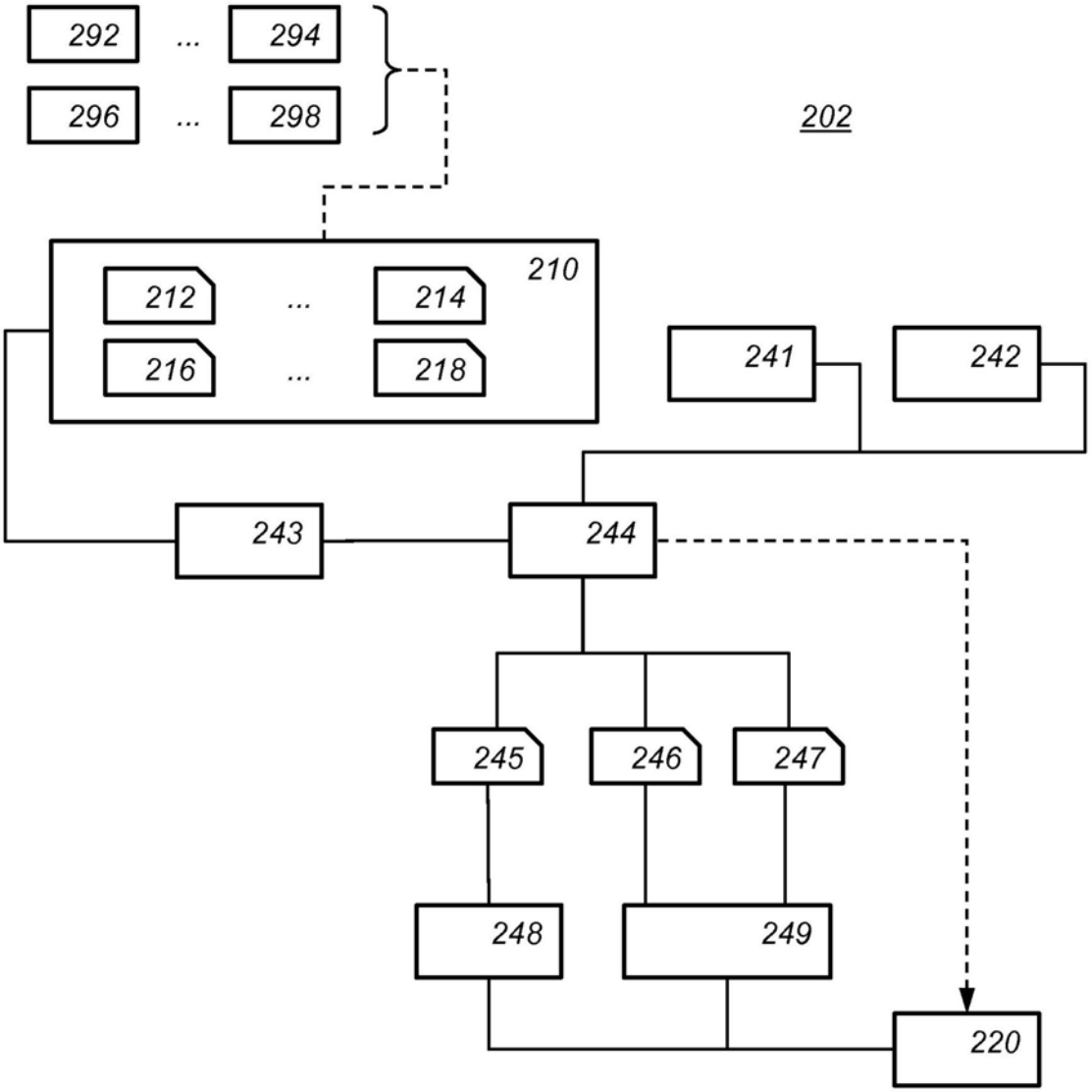

292
...
294
296
...
298
202
210
212
...
214
216
...
218
241
242
243
244
245
246
247
248
249
220

图1c

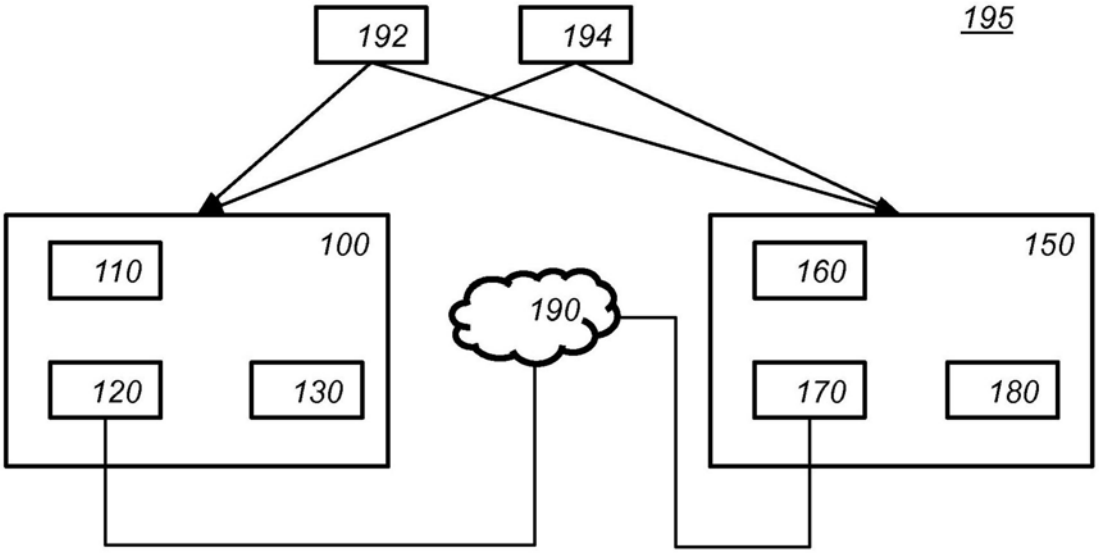

192
194
195
100
110
120
130
190
150
160
170
180

图2

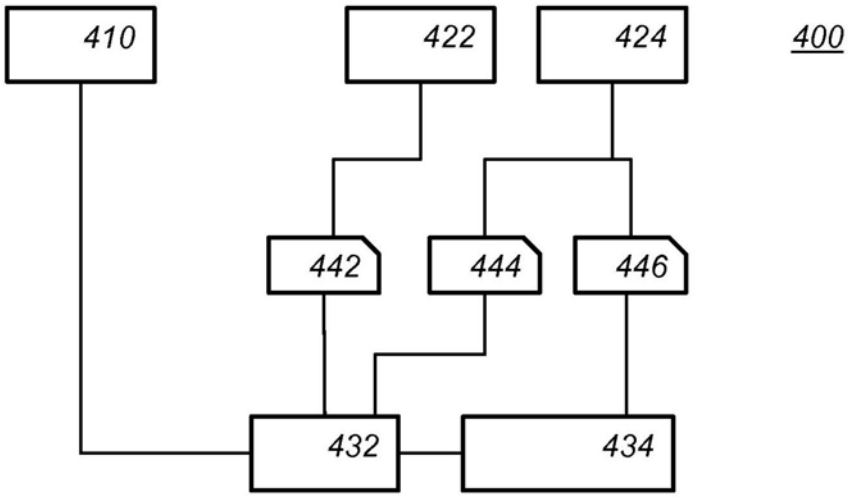

410
422
424
400
442
444
446
432
434

图3

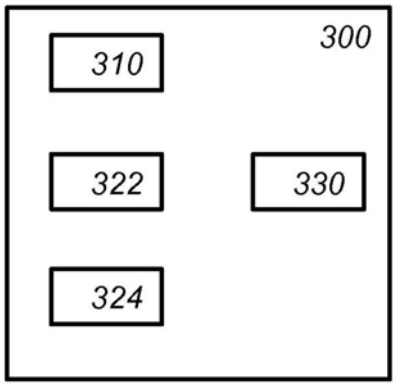

300
310
322
330
324

图4

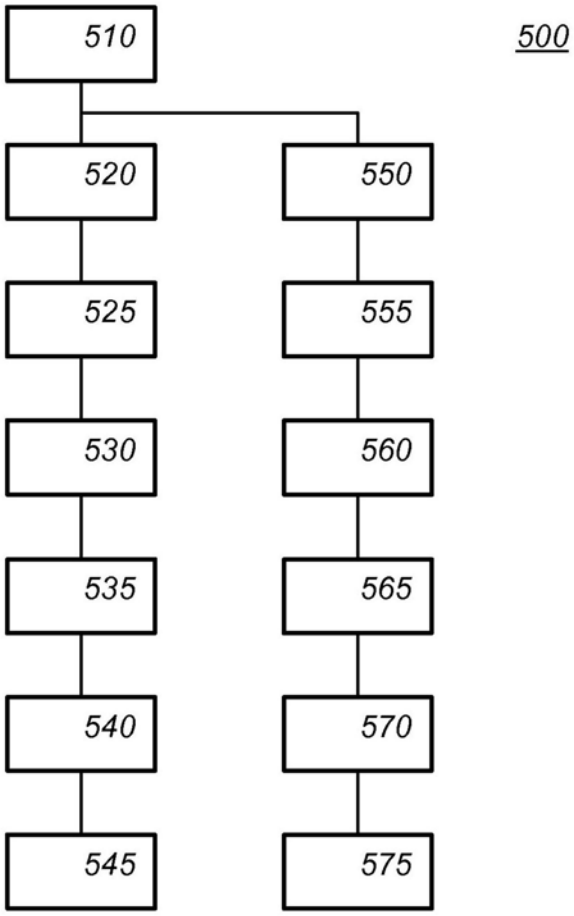

510
500
520
550
525
555
530
560
535
565
540
570
545
575

图5

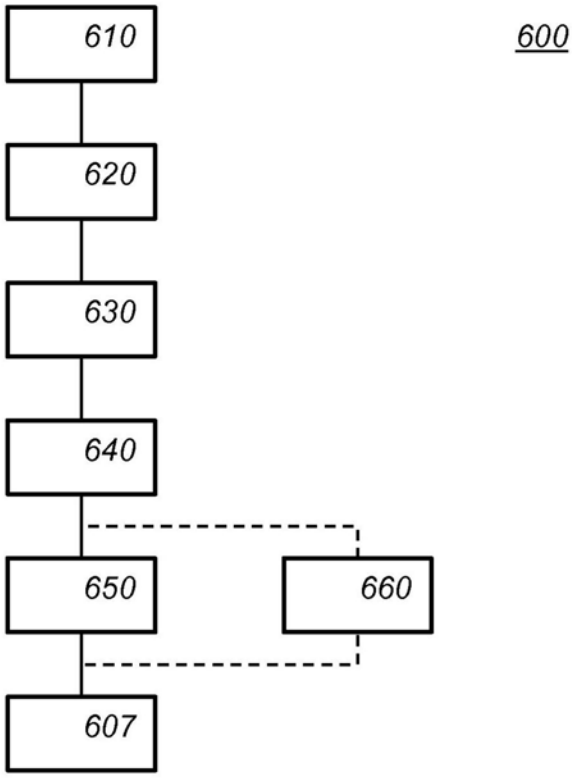


图6

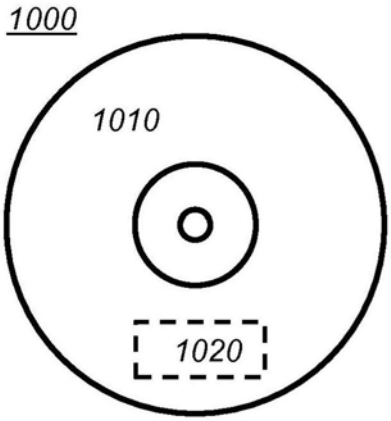


图7a

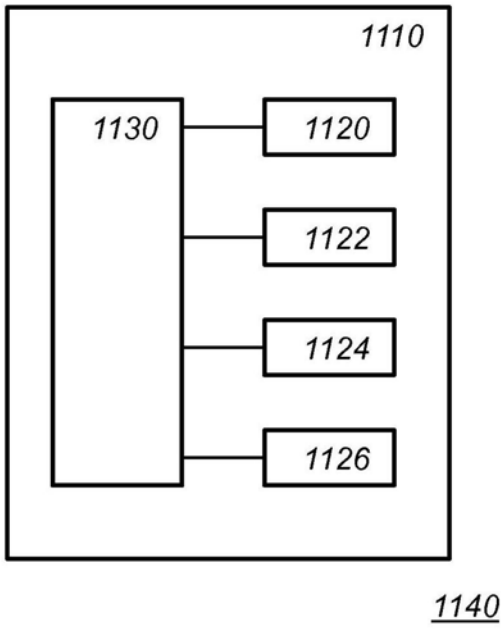


图7b