(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 102934392 B
(45)授权公告日 2015.07.15

(21)申请号 201180027910.3
(22)申请日 2011.04.12
(30)优先权数据
61/323,713 2010.04.13 US
(85)PCT国际申请进入国家阶段日
2012.12.06
(86)PCT国际申请的申请数据
PCT/US2011/032118 2011.04.12
(87)PCT国际申请的公布数据
WO2011/130274 EN 2011.10.20
(73)专利权人 康奈尔大学
地址 美国纽约州
(72)发明人 史蒂芬·B·威克
(74)专利代理机构 北京万慧达知识产权代理有限公司 11111
代理人 戈晓美 杨颖
(51)Int.Cl.
H04L 9/32(2006.01)
H04L 9/14(2006.01)
H04W 12/02(2006.01)
H04W 12/04(2006.01)

(56)对比文件
CN 101241527 A,2008.08.13,
US 2008/0052518 A1,2008.02.28,
CN 101542494 A,2009.09.23,
CN 101589596 A,2009.11.25,
CN 101241527 A,2008.08.13,
US 2005/0144440 A1,2005.06.30,
CN 101241527 A,2008.08.13,

审查员 曾珍

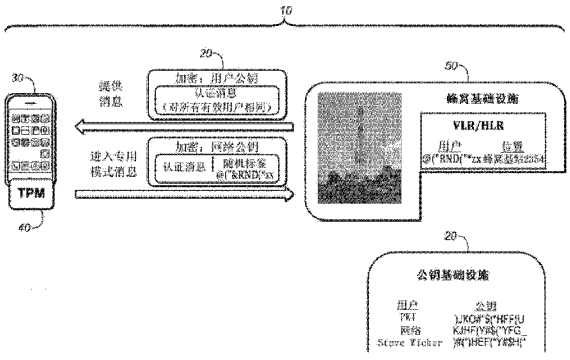
权利要求书6页 说明书22页 附图10页

(54)发明名称

用于信息网络的专用重叠

(57)摘要

本发明公开了一种用于信息网络的专用重叠，使得用户能够掌控该用户的个人信息。用户身份从指向用户设备可在其中被寻呼的小区的数值标签中被分离出来。通过注册和认证机构、例如公钥基础设施及认证机构(PKI)来生成专用重叠。注册和认证机构为网络和所有用户提供用于该网络和用户的公用加密密钥。以适当的方式生成和本地存储私用解密密钥。由于增加了私用解密密钥，能够针对由例如蜂窝、无线网络或由公用事业配给系统注册的设备建立到现有蜂窝、无线或公用事业配给基础设施的专用重叠。



CN 102934392 B

1. 一种用于保护网络中平台的用户隐私的系统，该系统包含：

专用重叠 (10)，该专用重叠包含用于在公钥密码系统中分发经认证公钥的系统 (20)；

其中：

平台 (40) 被包含在用户设备 (30) 内，

该用于分发经认证公钥的系统为该网络 (50) 和该网络的每个授权用户提供针对该网络和每个授权用户的公共加密密钥，

该平台在专用模式下运行，

当该平台以该专用模式运行时，该网络不能将该平台的位置数据与特定用户相关联，

网络执行专用注册，其中该平台周期性地向该网络的每个授权用户传送相同的认证消息，以及

该网络使用用户的公用加密密钥对传送给每个授权用户的认证消息进行加密。

2. 如权利要求 1 所述的用于保护隐私的系统，其中所述用户设备是蜂窝或移动电话、计算机或客户数据采集系统、效用度量表或者有线终端。

3. 如权利要求 2 所述的用于保护隐私的系统，其中所述客户数据采集系统是效用度量表。

4. 如权利要求 1 所述的用于保护隐私的系统，其中所述用于分发经认证公钥的系统是公钥基础设施及认证机构 (PKI)。

5. 如权利要求 1 所述的用于保护隐私的系统，其中：

所述平台是蜂窝平台，并且所述网络是蜂窝网络，

所述平台是无线平台，并且所述网络是无线网络，

或者所述平台是公用事业平台或第三方数据接收和管理平台，并且所述网络是与客户数据采集单元相互通信的通信网络。

6. 如权利要求 1 所述的用于保护隐私的系统，其中生成并本地存储私用解密密钥。

7. 如权利要求 1 所述的用于保护隐私的系统，其中：

所述平台是蜂窝平台，

所述网络是蜂窝网络，以及

所述蜂窝网络将所述用户设备与随机数相关联，从而将所述用户设备与用户身份相分离。

8. 如权利要求 1 所述的用于保护隐私的系统，其中：

所述平台是无线平台，

所述网络是无线网络，以及

所述无线网络将所述用户设备和与用户帐号识别符不同的随机数相关联，从而将所述用户设备与用户身份相分离。

9. 如权利要求 1 所述的用于保护隐私的系统，其中：

所述平台是公用事业平台或第三方数据接收和管理平台，

所述网络是通信网络，以及

所述通信网络将所述用户设备与随机数相关联，从而将所述用户设备与用户身份相分离。

10. 如权利要求 1 所述的用于保护隐私的系统，包含加密芯片 (60)，其中所述平台包含

所述加密芯片，并且其中所述加密芯片被编程以将认证消息保存在加密的安全库内。

11. 如权利要求 10 所述的用于保护隐私的系统，其中所述加密芯片是可信赖平台模块 (TPM)。

12. 如权利要求 10 所述的用于保护隐私的系统，其中所述平台是蜂窝式的，并且所述加密芯片被编程以记录所述用户设备在蜂窝模式下的通话时长。

13. 如权利要求 12 所述的用于保护隐私的系统，其中通话时长是预付费的。

14. 如权利要求 10 所述的用于保护隐私的系统，其中所述平台是无线的，所述加密芯片被编程以记录所述用户设备在无线模式下的无线使用时长。

15. 如权利要求 14 所述的用于保护隐私的系统，其中无线使用时长是预付费的。

16. 如权利要求 10 所述的用于保护隐私的系统，其中所述加密芯片被编程以支持远程证明，从而所述网络远程确定所述用户设备是否被授权。

17. 如权利要求 10 所述的用于保护隐私的系统，其中所述加密芯片被编程以支持远程证明，从而所述网络远程确定所述用户设备是否被克隆。

18. 如权利要求 10 所述的用于保护隐私的系统，其中所述加密芯片被编程以支持远程证明，从而所述网络远程确定所述用户设备的硬件和 / 或软件是否被改变。

19. 一种用于保护网络中平台的用户隐私的方法，该方法包括 ：

提供专用重叠 (10)，该专用重叠包含在公钥密码系统中分配经认证公钥的系统 (20)；

该平台在专用模式下运行，其中当该平台以该专用模式运行时，该网络不能将该平台的位置数据与特定用户相关联，

执行专用注册，其中专用注册包括 ：

该网络周期性地向该网络的每个授权用户传送相同的认证消息 ；以及

该网络使用用户的公用加密密钥对传送给每个授权用户的认证消息进行加密，

其中 ：

该平台 (40) 被包含在用户设备 (30) 内，以及

该用于分发经认证公钥的系统为该网络和该网络的每个授权用户提供针对该网络和每个授权用户的公共加密密钥。

20. 如权利要求 19 所述的方法，其中所述用户设备是蜂窝或移动电话、计算机或客户数据采集系统。

21. 如权利要求 20 所述的方法，其中所述客户数据采集系统是效用度量表。

22. 如权利要求 19 所述的方法，其中所述用于分发经认证公钥的系统是公钥基础设施及认证机构 (PKI)。

23. 如权利要求 19 所述的方法，其中 ：

该平台是蜂窝平台，并且该网络是蜂窝网络，

该平台是无线平台，并且该网络是无线网络，

或者该平台是公用事业平台或第三方数据接收和管理平台，并且该网络是与客户数据采集单元通信的通信网络。

24. 如权利要求 19 所述的方法，其中生成并本地地存储私用解密密钥。

25. 如权利要求 19 所述的方法，其中 ：

该平台是蜂窝平台，以及

该网络是蜂窝网络，

该方法还包含步骤：该蜂窝网络将该用户设备与随机数关联，从而将该用户设备与用户身份相分离。

26. 如权利要求 19 所述的方法，其中：

该平台是无线平台，以及

该网络是无线网络，

该方法还包含步骤：该无线网络将该用户设备与随机数关联，从而将该用户设备与用户身份相分离。

27. 如权利要求 19 所述的方法，其中：

该平台是公用事业平台或第三方数据接收和管理平台，

该网络是通信网络，以及

该通信网络将该用户设备和随机数关联，从而将该用户设备与用户身份相分离。

28. 如权利要求 19 所述的方法，其中该专用重叠包含加密芯片，其中该平台包含加密芯片，并且其中该加密芯片被编程以将认证消息保存在加密的安全库内。

29. 如权利要求 28 所述的方法，其中该加密芯片是可信赖平台模块 (TPM)。

30. 如权利要求 28 所述的方法，其中该平台是蜂窝式的，且该加密芯片被编程以记录该用户设备在蜂窝模式下的通话时长。

31. 如权利要求 30 所述的方法，其中通话时长是预付费的。

32. 如权利要求 28 所述的方法，其中该平台是无线的，且该加密芯片被编程以记录该用户设备在无线模式下的无线使用时长。

33. 如权利要求 32 所述的方法，其中无线使用时长是预付费的。

34. 如权利要求 28 所述的方法，其中该加密芯片被编程以支持远程证明，该方法还包括步骤：该网络远程地确定该用户设备是否被授权。

35. 如权利要求 28 所述的方法，其中该加密芯片被编程以支持远程证明，该方法还包括步骤：该网络远程地确定该用户设备是否被克隆。

36. 如权利要求 28 所述的方法，其中该加密芯片被编程以支持远程证明，从而该网络远程地确定该用户设备的硬件和 / 或软件是否被改变。

37. 如权利要求 19 所述的方法，其中该网络周期性地传送相同的认证消息的步骤被每日执行。

38. 如权利要求 19 所述的方法，其中以专用模式运行平台的步骤包含如下步骤：

该平台向该网络发送专用授权注册 (PER) 消息；以及

该平台使用该网络的公用加密密钥对 PER 加密，其中该 PER 包含该认证消息和随机设备标签 (RET)。

39. 如权利要求 38 所述的方法，其中该 PER 内的该认证消息相当于零确认证明，其向网络表示 PER 由有效用户发送；并且该 PER 内的认证消息不对该用户进行标识。

40. 如权利要求 38 所述的方法，其中该 RET 是随机数。

41. 如权利要求 38 所述的方法，其中该方法包含如下步骤：

将该 RET 输入到该网络的访问位置寄存器 (VLR) 和归属位置寄存器 (HLR)；以及

将该 RET 当作电话号码、帐户识别符或者用户 ID 数据传送，从而该 VLR 和 HLR 收集建

立和保持对该平台的蜂窝电话或数据呼叫、无线数据连接或数据传输所需的信息，但不将所述信息与特定的用户、电话号码、帐号识别符或用户 ID 相关联。

42. 如权利要求 41 所述的方法，其中该蜂窝电话或数据呼叫、无线数据连接或者数据传输是呼入或呼出的。

43. 如权利要求 41 所述的方法，其中包含将该 RET 与临时 IP 地址相关联的步骤。

44. 如权利要求 42 所述的方法，其中该蜂窝电话呼叫是被叫通话，该方法包含如下步骤：

将用户的 RET 和该蜂窝网络的业务提供商的身份分发给用户希望接收蜂窝电话呼叫的各方，其中该分发步骤使用公钥加密。

45. 如权利要求 44 所述的方法，其中该用户执行该分发步骤。

46. 如权利要求 44 所述的方法，其中该用于分发经认证公钥的系统执行该分发步骤。

47. 如权利要求 19 所述的方法，其中该方法包含在该平台内嵌入加密芯片的步骤，其中该加密芯片被编程以将认证消息保存在加密的安全库内。

48. 如权利要求 47 所述的方法，其中该加密芯片是可信赖平台模块 (TPM)。

49. 如权利要求 47 所述的方法，其中当该设备处于蜂窝模式时，该加密芯片被编程以记录蜂窝电话通话时长。

50. 如权利要求 49 所述的方法，其中通话时长是预付费的。

51. 如权利要求 47 所述的方法，其中该加密芯片被编程以支持远程证明，该方法包含该网络远程确定该设备是否被授权的步骤。

52. 如权利要求 47 所述的方法，其中该加密芯片被编程以支持远程证明，该方法包含该网络远程确定该设备是否被克隆的步骤。

53. 如权利要求 48 所述的方法，其中该 TPM 被编程以支持远程证明，该方法包含该网络远程确定该设备的硬件和 / 或软件是否被改变的步骤。

54. 一种用于确定用户设备是否被授权的方法，其中该用户是网络中平台的用户，该方法包括：

提供专用重叠，该专用重叠包含用于在公钥密码系统中分发经认证公钥的系统和加密芯片；

该平台在专用模式下运行，其中当该平台以该专用模式运行时，该网络不能将该平台的位置数据与特定用户相关联；

执行专用注册，其中专用注册包括：

该网络周期性地向该网络的每个授权用户传送相同的认证消息；以及

该网络使用用户的公用加密密钥对传送给每个授权用户的认证消息进行加密；以及

该网络远程确定所述用户设备是否被授权；

其中：

该平台被包含在用户设备内，

所述平台包含所述加密芯片，

所述加密芯片被编程以将认证消息保存在加密的安全库内，

所述加密芯片被编程以支持远程证明，以及

该用于分发经认证公钥的系统为该网络和该网络的每个授权用户提供针对该网络和

每个授权用户的公共加密密钥。

55. 一种用于确定用户设备是否被克隆的方法，其中该用户是网络中平台的用户，该方法包括：

提供专用重叠，该专用重叠包含在公钥密码系统中分发经认证公钥的系统和加密芯片；

该平台在专用模式下运行，其中当该平台以该专用模式运行时，该网络不能将该平台的位置数据与特定用户相关联；

执行专用注册，其中专用注册包括：

该网络周期性地向该网络的每个授权用户传送相同的认证消息；以及

该网络使用用户的公用加密密钥对传送给每个授权用户的认证消息进行加密；以及

该网络远程确定所述用户设备是否被授权；

其中：

该平台被包含在用户设备内，

所述平台包含所述加密芯片，

所述加密芯片被编程以将认证消息保存在加密的安全库内，

所述加密芯片被编程以支持远程证明，以及

该用于分发经认证公钥的系统为该网络和该网络的每个授权用户提供针对该网络和每个授权用户的公共加密密钥。

56. 一种用于确定用户设备的硬件或软件是否被改变或篡改的方法，其中该用户是网络中平台的用户，该方法包括：

提供专用重叠，该专用重叠包含用于在公钥密码系统中分发经认证公钥的系统和加密芯片；

该平台在专用模式下运行，其中当该平台以该专用模式运行时，该网络不能将该平台的位置数据与特定用户相关联；

执行专用注册，其中专用注册包括：

该网络周期性地向该网络的每个授权用户传送相同的认证消息；以及

该网络使用用户的公用加密密钥对传送给每个授权用户的认证消息进行加密；以及

该网络远程确定所述用户设备是否被授权；

其中：

该平台被包含在用户设备内，

所述平台包含所述加密芯片，

所述加密芯片被编程以将认证消息保存在加密的安全库内，

所述加密芯片被编程以支持远程证明，以及

该用于分发经认证公钥的系统为网络和该网络的每个授权用户提供针对该网络和每个授权用户的公共加密密钥。

57. 一种用于向用户收费的方法，其中该用户是网络中平台的用户，该方法包括：

提供专用重叠，该专用重叠包含用于在公钥密码系统中分发经认证公钥的系统和加密芯片；

该平台在专用模式下运行，其中当该平台以该专用模式运行时，该网络不能将该平台

的位置数据与特定用户相关联；

执行专用注册，其中专用注册包括：

该网络周期性地向该网络的每个授权用户传送相同的认证消息；以及

该网络使用用户的公用加密密钥对传送给每个授权用户的认证消息进行加密；以及

该网络远程确定所述用户设备是否被授权；

其中：

该平台被包含在用户设备内，

所述平台包含所述加密芯片，

所述加密芯片被编程以将认证消息保存在加密的安全库内，

所述加密芯片被编程以支持远程证明，以及

该用于分发经认证公钥的系统为该网络和该网络的每个授权用户提供针对该网络和每个授权用户的公共加密密钥。

58. 如权利要求 54，55，56 或 57 所述的方法，其中：

所述平台是蜂窝平台，并且所述网络是蜂窝网络，

所述平台是无线平台，并且所述网络是无线网络，

或者所述平台是公用事业平台或第三方数据接收及管理平台，且所述网络是与客户数据采集单元相互通信的通信网络。

用于信息网络的专用重叠

[0001] 相关申请的交叉引用

[0002] 本申请要求 2010 年 4 月 13 日申请的，发明名称为“蜂窝网络的专用重叠”的共同未决美国临时专利申请第 61/323,713 号的优先权和利益，在此将该专利申请以引用方式全部并入。

[0003] 关于联邦科研资助或开发的声明

[0004] 本发明根据第 0424422 号合同获得联邦科学基金会的政府支持。政府对于该发明具有一定的权利。

1. 技术领域

[0005] 本发明涉及用于保护信息网络中平台的用户隐私的系统和方法。本发明还涉及用于蜂窝、无线或第三方数据接收和管理系统的用户的专用(或私用) 重叠(private overlay)。

2. 背景技术

[0006] 公钥加密技术

[0007] 公钥加密考虑到两种不同的密钥，一种用于加密，另一种用于解密。任何使用了加密密钥进行加密的明文仅能由具有解密密钥的人进行解密。如果设计得当，不经过解决非常困难的数学问题是不可能由一个密钥获得另一个密钥的。因此，或许可以通过在线投递公开加密密钥，使得任何人可以对消息进行加密，并将其发送给所期望的用户，而不用担心该消息会被任何不具有该机密的解密密钥的人读取。只要该解密密钥被保持为机密，该信息就保持安全。Diffie 和 Hellman 在 1976 年提出了公钥加密技术。接下来的显著进步是由 Rivest, Shamir 和 Adleman 以及他们关于 RSA (此缩写包含每个发明人的姓氏的首字母)密码系统的发明在 20 世纪 70 年代后期所实现的。RSA 密码系统使用本领域已知算法实现公钥加密(该算法主要依赖于对大数进行模幂乘)。RSA 加密算法的安全性被假定基于将非常大的数字分解为 A×B 的形式的难度，其中 A 和 B 是大的质数。尽管从未被确定地证明，但是通常认为从相应的加密密钥获得较好选择的 RSA 解密密钥(或反之)的唯一方式是分解两个大质数的乘积。这是易于理解的、但已知非常困难的问题。RSA 密钥比对称系统密钥大很多，但并没有大到无法实现的程度。本领域中通常认为 3072 位的 RSA 密钥与对称密钥系统中的 128 位密钥提供了相同级别的安全性(例如参见 http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf)。具有两种不同密钥的另一个值得注意的方面是该系统能够被用于产生安全的数字签名以及提供安全的通信。

[0008] 公钥加密技术在可信赖通信中起到了相当重要的作用。但是仍遗漏了一部分：当我们使用公钥向例如在线销售商发送如我们的信用卡信息时，我们希望能确保确实是该在线销售商提供了该公钥。

[0009] 本领域中已知的解决该问题的方法是采取公钥证书的形式。公钥证书将公钥与个人或企业身份绑定，这与护照将个人信息(姓名、出生日期、出生地，等) 与护照照片绑定的

方式大致相同。

[0010] 目前，电子商务零售商到注册机构(registration authority)，并提供足够的文件来证明他们的企业身份。一旦他们的身份得到验证，相关的认证机构就生成公钥，并将该公钥置于证书上，将该证书和与该密钥相关的实体的信息进行绑定。该认证机构对该证书进行数字签名，从而使得已认证实体的顾客可对该证书进行验证。注册和认证机构以及其他相关职能机构通常被发现属于称作公钥基础设施(Public KeyInfrastructure，PKI)的单个实体。已经出现了一些作为支配性网络商务 PKI 的大公司，例如 VeriSign。它们通过多种方式建立了信任，包括可靠性、高达 250,000 美元的现金授权(参见 http://www.verisign.com/ssl/buy-ssl-certificates/index.html ? tid = a box)，并且事实是，如果它们滥用了对于它们的信任，那么它们作为公司的价值将会在一夜间消失。许多网络浏览器被设置为自动地从已知 PKI 接收证书，因此不需要个人用户考虑这些事情。

[0011] 例如，假定一个买家希望到一个在线书商的网站来购买一本书的几份副本。这个买家首先在他的浏览器顶部的 URL 栏内输入该书商的 URL，然后进入该书商的主页。这个买家随后将书的副本放入一个虚拟的购物车中，然后结算。此时开始执行对于大多数用户未知的加密处理。该书商将含有公共加密密钥的证书发送到买家的浏览器。如果买家愿意，他可以通过点击所显示的锁定图标来实际查看该证书，该锁定图标表示在一些浏览器内的安全浏览。这些证书包含大量信息，包括签名权限、公共加密密钥以及预期的加密算法。对于该实例，该证书由认证服务商例如 VeriSign 签名，并调用具有特定长度即 2040 位的密钥进行 RSA 加密。在核实该证书之后，这个买家的浏览器产生用于对称密钥密码系统的 128 或 256 位的密钥。该密钥可以使用证书上的 RSA 公共加密密钥来进行加密，并且所产生的密文被发送给在线销售商。销售商和买方现在共享了一个机密的对称密钥，并且现在可以安全地交流。电子商务的成功依赖于通过公钥加密技术和可信的第三方，例如认证服务商如 VeriSign，所产生的信任。

[0012] 保护信息网络的隐私

[0013] 从一开始，固定电话就是受监管的技术。监管的可能性随着蜂窝电话而增大，这是由于注册消息提供了固定的位置信息流。最近，由于非电话的计算和视频功能被聚集到蜂窝平台，并且无线平台和无线网络的使用得到了扩展，监管度的影响逐渐变得更加重要。

[0014] 本领域需要一种用于保护例如蜂窝和无线网络的信息网络的隐私的系统，该系统使得用户掌管他或她的个人信息。

[0015] 第 2 部分或者本申请的任何其他部分中引用或标注的任何参考文献，不应认为该参考文献被许可作为本发明的现有技术。

3. 发明内容

[0016] 一种用于保护网络中平台的用户隐私的系统，该系统包含 ：

[0017] 专用重叠 10，该专用重叠包含在公钥密码系统中分发认证公钥的系统 20 ；

[0018] 其中 ：

[0019] 该平台 40 被包含在用户设备 30 内，以及

[0020] 该用于分发经认证公钥的系统为网络 50 和该网络的每个授权用户提供针对该网络和每个授权用户的公共加密密钥。

[0021] 在本系统的一个实施例中，所述用户设备是蜂窝或移动电话、计算机或客户数据采集系统、效用度量表(Utiliy meter)或者有线终端。

[0022] 在本系统的另一个实施例中，所述客户数据收集系统是效用度量表。

[0023] 在本系统的又一个实施例中，所述用于分发经认证公钥的系统是公钥基础设施及认证机构(PKI)。

[0024] 在本系统的又一个实施例中，所述平台是蜂窝平台，所述网络是蜂窝网络，所述平台是无线平台且所述网络是无线网络，或者所述平台是公用事业平台或第三方数据接收和管理平台，且所述网络是与客户数据采集单元相互通信的通信网络。

[0025] 在本系统的又一个实施例中，所述客户数据采集单元是电表、燃气表或效用度量表。

[0026] 在本系统的又一个实施例中，生成并本地地存储私用解密密钥。

[0027] 在本系统的又一个实施例中，所述平台是蜂窝平台，所述网络是蜂窝网络，并且所述蜂窝网络将用户设备与随机数相关联，从而将所述用户设备与用户身份相分离。

[0028] 在本系统的又一个实施例中，所述平台是无线平台且所述网络是无线网络，并且所述无线网络将用户设备和与用户帐号识别符不同的随机数相关联，从而将所述用户设备与用户身份相分离。

[0029] 在本系统的又一个实施例中，所述平台是公用事业平台或第三方数据接收和管理平台，且所述网络是通信网络，所述通信网络将用户设备与随机数相关联，从而将所述用户设备与用户身份相分离。

[0030] 在又一个实施例中，所述系统包含一加密芯片 60，其中所述平台包含所述加密芯片，并且其中所述加密芯片被编程以将认证消息保存在加密的安全库内。

[0031] 在本系统的又一个实施例中，所述加密芯片是一个可信赖平台模块(TPM)。

[0032] 在本系统的又一个实施例中，所述平台是蜂窝式的，并且所述加密芯片被编程以记录用户设备在蜂窝模式下的通话时长。

[0033] 在本系统的又一个实施例中，通话时长是预付费的。

[0034] 在本系统的又一个实施例中，所述平台是无线的，所述加密芯片被编程以记录用户设备在无线模式下的无线使用时长。

[0035] 在本系统的又一个实施例中，无线使用时长是预付费的。

[0036] 在本系统的又一个实施例中，所述加密芯片被编程以支持远程证明，从而所述网络远程确定用户设备是否被授权。

[0037] 在本系统的又一个实施例中，所述加密芯片被编程以支持远程证明，从而所述网络远程确定用户设备是否被克隆。

[0038] 在本系统的又一个实施例中，所述加密芯片被编程以支持远程证明，从而所述网络远程确定用户设备硬件和 / 或软件是否被改变。

[0039] 还提供了一种用于保护网络上平台用户的隐私的方法，该方法包括如下步骤：

[0040] 提供专用重叠 10，该专用重叠包含在公钥密码系统中分发经认证公钥的系统 20；

[0041] 其中：

[0042] 该平台 40 被包含在用户设备 30 内，以及

[0043] 该用于分发经认证公钥的系统为网络 50 和该网络的每个授权用户提供针对该网

络和每个授权用户的公共加密密钥。

[0044] 在该方法的另一个实施例中，用户设备是蜂窝或移动电话、计算机或客户数据采集系统。

[0045] 在该方法的另一个实施例中，客户数据采集单元是效用度量表。

[0046] 在该方法的另一个实施例中，该用于分发经认证公钥的系统是公钥基础设施及认证机构(PKI)。

[0047] 在该方法的另一个实施例中，该平台是蜂窝平台，且该网络是蜂窝网络，该平台是无线平台，且该网络是无线网络，或者该平台是公用事业平台或第三方数据接收和管理平台，且该网络是与客户数据采集单元通信的通信网络。

[0048] 在该方法的另一个实施例中，客户数据采集单元是电表、燃气表或效用度量表。

[0049] 在该方法的另一个实施例中，生成并本地地存储私用解密密钥。

[0050] 在该方法的另一个实施例中，该平台是蜂窝平台，且该网络是蜂窝网络，该方法还包含步骤：蜂窝网络将用户设备与随机数关联，从而将该用户设备与用户身份相分离。

[0051] 在该方法的另一个实施例中，该平台是无线平台，该网络是无线网络，且该方法还包含步骤：无线网络将用户设备与随机数关联，从而将该用户设备与用户身份相分离。

[0052] 在该方法的另一个实施例中，该平台是公用事业平台或第三方数据接收和管理平台，该网络是通信网络，且该通信网络将用户设备和随机数关联，从而将用户设备与用户身份相分离。

[0053] 在该方法的另一个实施例中，专用重叠包含加密芯片，其中该平台包含加密芯片，并且其中该加密芯片被编程以将认证消息保存在加密的安全库内。

[0054] 在该方法的另一个实施例中，该加密芯片是可信赖平台模块(TPM)。

[0055] 在该方法的另一个实施例中，该平台是蜂窝式的，且该加密芯片被编程以记录该用户设备在蜂窝模式下的通话时长。

[0056] 在该方法的另一个实施例中，通话时长是预付费的。

[0057] 在该方法的另一个实施例中，该平台是无线平台，且该加密芯片被编程以记录用户设备在无线模式下的无线使用时长。

[0058] 在该方法的另一个实施例中，无线使用时长是预付费的。

[0059] 在该方法的另一个实施例中，该加密芯片被编程以支持远程证明，该方法还包括步骤：网络远程地确定用户设备是否被授权。

[0060] 在该方法的另一个实施例中，该加密芯片被编程以支持远程证明，该方法还包括步骤：网络远程地确定用户设备是否被克隆。

[0061] 在该方法的另一个实施例中，该加密芯片被编程以支持远程证明，从而网络远程地确定用户设备的硬件和/或软件是否被改变。

[0062] 在另一个实施例中，该方法还包括在专用模式下运行平台的步骤，其中当平台以专用模式运行时，网络不能将平台的位置数据与特定用户相关联。

[0063] 在该方法的另一个实施例中，以专用模式运行平台的步骤包含执行专用注册的步骤，

[0064] 其中专用注册包含如下步骤：

[0065] 网络周期性地向网络的每个授权用户传送相同的认证消息；以及

[0066] 网络使用用户的公用加密密钥对传送给每个授权用户的认证消息进行加密。

[0067] 在该方法的另一个实施例中，网络周期性地传送相同的认证消息的步骤被每日执行。

[0068] 在该方法的另一个实施例中，以专用模式运行平台的步骤包含如下步骤：

[0069] 平台向网络发送专用授权注册(Privacy Enabling Registration，PER)消息；以及

[0070] 平台使用网络的公用加密密钥对 PER 加密，其中 PER 包含认证消息和随机设备标签(Random Equipment Tag，RET)。

[0071] 在该方法的另一个实施例中，PER 内的认证消息相当于零确认证明(zero-acknowledge proof)，其向网络表示 PER 由有效用户发送，且不对该用户进行标识。

[0072] 在该方法的另一个实施例中，RET 是随机数。

[0073] 在另一个实施例中，该方法包含如下步骤：

[0074] 将 RET 输入到网络的访问位置寄存器(Visitor Location Register，VLR)和归属位置寄存器(Home Location Register，HLR)；以及将 RET 当作电话号码、帐户识别符或者用户 ID 数据传送，从而 VLR 和 HLR 收集建立和保持对于平台的蜂窝电话或数据呼叫、无线数据连接或数据传输所需的信息，但不将所述信息与特定的用户、电话号码、帐号识别符或用户 ID 相关联。

[0075] 在该方法的另一个实施例中，蜂窝电话或数据呼叫、无线数据连接或者数据传输是呼入或呼出的。

[0076] 在另一个实施例中，该方法包含将 RET 与临时 IP 地址相关联的步骤。

[0077] 在该方法的另一个实施例中，蜂窝电话呼叫是被叫通话，该方法包含如下步骤：将用户的 RET 和蜂窝网络的业务提供商的身份(例如网络 ID)分发给用户希望接收到蜂窝电话呼叫的各方，其中该分发步骤使用公钥加密。

[0078] 在该方法的另一个实施例中，用户执行该分发步骤。

[0079] 在该方法的另一个实施例中，用于分发经认证公钥的系统执行该分发步骤。

[0080] 在另一个实施例中，该方法包含在蜂窝平台内嵌入加密芯片的步骤，其中加密芯片被编程以将认证消息保存在加密的安全库内。

[0081] 在该方法的另一个实施例中，该加密芯片是可信赖平台模块(TPM)。

[0082] 在该方法的另一个实施例中，加密芯片被编程以记录设备处于蜂窝模式下的蜂窝电话通话时长。

[0083] 在该方法的另一个实施例中，通话时长是预付费的。

[0084] 在该方法的另一个实施例中，加密芯片被编程以支持远程证明，该方法包含网络远程确定设备是否被授权的步骤。

[0085] 在该方法的另一个实施例中，加密芯片被编程以支持远程证明，该方法包含网络远程确定设备是否被克隆的步骤。

[0086] 在该方法的另一个实施例中，TPM 被编程以支持远程证明，该方法包含网络远程确定设备硬件和 / 或软件是否被改变的步骤。

[0087] 还提供了一种用于确定用户设备是否被授权的方法，其中该用户是网络上平台的用户。在一个实施例中，该方法包括提供专用重叠的步骤，该专用重叠包含用于在公钥密码

系统中分发经认证公钥的系统：

[0088] 其中：

[0089] 该平台被包含在用户设备内，以及

[0090] 该用于分发经认证公钥的系统为网络和该网络的每个授权用户提供针对该网络和每个授权用户的公共加密密钥。

[0091] 还提供了一种用于确定用户设备是否被克隆的方法，其中该用户是网络上平台的用户。在一个实施例中，该方法包括提供专用重叠的步骤，该专用重叠包含在公钥密码系统中分发经认证公钥的系统：

[0092] 其中：

[0093] 该平台被包含在用户设备内，以及

[0094] 该用于分发经认证公钥的系统为网络和该网络的每个授权用户提供针对该网络和每个授权用户的公共加密密钥。

[0095] 还提供了一种用于确定用户设备硬件或软件是否被改变或篡改的方法，其中该用户是网络中平台的用户。在一个实施例中，该方法包括提供专用重叠的步骤，该专用重叠包含用于在公钥密码系统中分发经认证公钥的系统：

[0096] 其中：

[0097] 该平台被包含在用户设备内，以及该用于分发经认证公钥的系统为网络和该网络的每个授权用户提供针对该网络和每个授权用户的公共加密密钥。

[0098] 还提供了一种用于向用户收费的方法，其中该用户是网络中平台的用户。在一个实施例中，该方法包括提供专用重叠的步骤，该专用重叠包含在公钥密码系统中分发经认证公钥的系统：

[0099] 其中：

[0100] 该平台被包含在用户设备内，以及该用于分发经认证公钥的系统为网络和该网络的每个授权用户提供针对该网络和每个授权用户的公共加密密钥。

[0101] 在特定的实施例中，所述平台是蜂窝平台，所述网络是蜂窝网络，所述平台是无线平台且所述网络是无线网络，或者所述平台是公用事业平台或第三方数据接收和管理平台，且所述网络是与客户数据采集单元相互通信的通信网络。

4. 附图说明

[0102] 本文将结合附图具体阐释本发明，其中相同的附图标记文字表示在几幅视图中相同的器件。应理解的是，在一些情况下，本发明的不同方面被夸大或放大示出以便于理解本发明。

[0103] 图 1 是用于蜂窝系统的专用(或私用)重叠 10 的示意性实施例。专用重叠 10 使用现有通信、信息或数据网络 50 (例如蜂窝网络)的基础设施来提供服务(例如蜂窝语音和数据业务)，而不会生成与该用户绑定的位置和使用记录。在右下方的是用于在公钥密码系统 20 中分发经认证公钥的系统的基础设施的细节。在该实施例中，分发经认证公钥的系统是公钥基础设施和认证机构(PKI)，可信赖平台模块 TPM 或者加密芯片 60，访问位置寄存器 VLR，归属位置寄存器 HLR，用户随机标签，@(*&RND(*zx。

[0104] 图 2 是由可信赖平台模块(TPM)多样服务的改进表格；选自 Trusted Computing

Group(TCG)Specification Architecture Overview,Revision 1.4,第 36 页;具体细节参见章节 5.3。

[0105] 图 3 是 TPM 组成架构改进图,TPM 正文第一部分。具体细节参见章节 5.3。

[0106] 图 4 是用于蜂窝或无线系统的专用重叠的实施例的示意图。服务供应商例如是蜂窝或无线服务供应商。TPM 可信赖平台模块或加密芯片 60。

[0107] 图 5 是对需求响应可能性的评估。由联邦能源监管委员会修改(2009 年 6 月)。A National assessment of demand response potential,StaffRep.,http://www.ferc.gov/legal/staff-reports/06-09-demand-response.pdf)。具体细节参看章节 6.3。

[0108] 图 6 是假设场景下的密钥差异。由联邦能源监管委员会修改(2009 年 6 月)。A National assessment of demand response potential,Staff Rep.,http://www.ferc.gov/legal/staff-reports/06-09-demand-response.pdf)。具体细节参看章节 6.3。

[0109] 图 7a-d 是行为提取算法。(a) 累计的功率消耗数据,(b) 推断出的切换事件,(c) 几个被标识的加载事件,以及 (d) 参考间隔和估计间隔的比较。参见 M.Lisovich,D.Mulligan 和 S.B.Wicker 撰写的 Inferring personalinformation from demand-response system,IEEE Security Privacy Mag., 第 8 卷,第 1 期,第 11-20 页,1/2 月 2010。具体细节参看章节 6.3。

[0110] 图 8 是高级计量基础设施(Advanced Metering Infrastructure,AMI)建模模块。根据 Engineering Power Research Institute,Advanced MeteringInfastructure,http://www.ferc.gov/eventcalendar/Files/20070423091846-EPRI%20-%20Advanced%20Metering.pdf)。具体细节参看章节 6.3。

[0111] 图 9 是考虑隐私的需求响应架构。具体细节参看章节 6.3。

5. 具体实施方式

[0112] 专用重叠 10 被提供以用于信息网络或网络系统(例如蜂窝电话网络、无线计算机网络、有线计算机网络、通信网络、第三方数据接收和管理系统、或者公用事业配给系统(Utility Distribution System)),其使得用户掌管他或她的个人信息。用户的身份被与指向用户设备 30 可以在其中被寻呼的小区的数值标签相分离。专用重叠 10 由附加的公钥基础设施及认证机构(PKI)或其他注册和认证机构 20 生成。这类注册和认证机构是本领域公知的。PKI (或其他注册和认证机构)20 为蜂窝电话、无线计算或效用度量系统或网络以及网络的所有用户提供针对该网络和用户的公钥。私用解密密钥被以适当的方式生成并且被本地地存储。这类生成和存储私用解密密钥的方法是本领域公知的。通过增加上述方式,可以针对由蜂窝或无线网络或公用设施或者第三方数据接收和管理系统注册的设备建立连接到现有的蜂窝、无线、第三方数据接收和管理、或者公用事业配给基础设施 50 的专用重叠 10。

[0113] 出于清楚地公开的目的,且不应作为限制性的,本发明的具体描述被分为如下的子章节。

[0114] 5.1 用于保护用户隐私的系统

[0115] 提供了一种用于保护网络内平台 40 的用户隐私的系统。该系统包含:

[0116] 专用重叠 10,该专用重叠 10 包含用于在公钥密码系统内分发经认证公钥的系统

20；

[0117] 其中：

[0118] 该平台 40 被包含在用户设备 30 内，以及

[0119] 该用于分发经认证公钥的系统 20 为网络以及该网络的每个授权用户提供针对该网络和每个授权用户的公用加密密钥。

[0120] 在一个实施例中，该用户设备 30 是蜂窝电话、计算机或客户数据采集单元。可采用本领域已知的任何客户数据采集单元。例如，在一个实施例中，该客户数据采集单元用于公用事业管理或配给，例如效用度量表，诸如电表、燃气表或水表。

[0121] 在一个特定的实施例中，该专用重叠 10 可用于 3G 和 4G 蜂窝系统。

[0122] 在另一个实施例中，该平台 40 是蜂窝平台，且该网络是蜂窝网络（图 1 和 4）。在另一个实施例中，该平台是无线平台，且该网络是无线网络（图 4）。在另一个实施例中，该平台是客户数据采集平台，且该网络是通信网络（图 8）。

[0123] 在另一个实施例中，该分发认证公钥系统 20 是公钥基础设施及认证机构（PKI），或者本领域已知的其他注册和认证机构。

[0124] 在另一个实施例中，生成并本地地存储私用解密密钥。

[0125] 在另一个实施例中，蜂窝网络 50 将用户设备（例如蜂窝或无线电话）和不同于电话号码的随机数关联，从而将该用户设备与用户身份相分离（图 1）。

[0126] 在另一个实施例中，该平台 40 是无线平台，该网络 50 是无线网络，且该无线网络将用户设备 30 和与用户帐号识别符不同的随机数关联，从而将该用户设备与用户身份相分离（图 4）。

[0127] 在另一个实施例中，该平台 40 是公用事业或第三方数据接收和管理平台，该网络 50 是通信网络，且该通信网络将用户设备 30（例如电表、燃气表或水表）和随机数关联，从而将用户设备 30 与用户身份相分离。

[0128] 在另一个实施例中，该系统包含加密芯片 60，其中该加密芯片 60 被嵌入在平台 40 中，并被编程以将认证消息保存在加密的安全库内。

[0129] 在另一个实施例中，该加密芯片 60 是可信赖平台模块（TrustablePlatform Module，TPM）。

[0130] 在另一个实施例中，该平台 40 是蜂窝平台，且该加密芯片 60 被编程以记录该用户设备在蜂窝模式下的通话时长。

[0131] 在另一个实施例中，该蜂窝电话通话时长是预付费的。

[0132] 在另一个实施例中，该平台 40 是无线的，且该加密芯片 60 被编程以记录用户设备在无线模式下的无线使用时长。

[0133] 在另一个实施例中，无线使用时长是预付费的。

[0134] 在另一个实施例中，该加密芯片 60 被编程以支持远程证明，从而网络 50 远程地确定用户设备 30 是否被授权。

[0135] 在另一个实施例中，该加密芯片被编程以支持远程证明，从而网络远程地确定用户设备是否被克隆或者是否被篡改。

[0136] 在另一个实施例中，该加密芯片被编程以支持远程证明，从而网络远程地确定用户设备的硬件和 / 或软件是否被改变。

[0137] 本文所提供的专用重叠可以被用于保护蜂窝网络内的蜂窝平台的用户(例如蜂窝电话)或者无线网络内的无线设备的隐私。该系统包含用于在公钥密码系统内分发经认证公钥的系统,其中在公钥密码系统内分发经认证公钥的系统为网络和该蜂窝网络的授权用户提供针对该网络和授权用户的公用加密密钥。可采用本领域公知技术由该网络和授权用户安全地生成并存储私用解密密钥。

[0138] 图 1 示意性地示出了专用重叠 10 的实施例,其用于保护网络例如蜂窝(或无线)网络中平台 40 的用户的隐私的系统。专用重叠 10 包含用于在公钥密码系统 20 内分发经认证公钥的系统。这类系统是本领域公知的。平台 40 被包含在用户设备 30 中(在该实施例中,用户设备是蜂窝电话),且用于分发认证公钥的系统 20 为网络和网络的每个授权用户提供针对该网络和每个授权用户的公用加密密钥。

[0139] 专用重叠使用现有的蜂窝基础设施来提供蜂窝语音和数据业务,而不生成与该用户相关联的位置和使用记录。如图 1 所示,向所有授权用户发送相同的认证消息(“加密的 : 用户公钥”)。

[0140] 如图 1 所示,用户发送认证消息(对于所有有效用户是相同的)以及来自于用户设备 30 的随机标签(如图 1 所示,@(*&RND(*zx) 以进入专用模式(“加密的 :网络公钥”)。该认证消息相当于零确认证明。本实施例中的加密芯片,可信赖平台模块(TPM)60,确保仅有一个有效用户获知该认证消息,但网络不知道哪个用户发送了该消息。随机标签作为专用授权用户(privacy-enabled user)的电话号码。专用授权电话包括 TPM。TPM 能够执行必要的公钥加密功能,并能够记录和实施通话时长限制。可以通过远程证明来防止克隆。

[0141] 仍如图 1 所示,随机标签可用于现有的蜂窝基础设施中,以替换用于注册和呼叫路由选择的用户 ID。不对网络基础设施 50 (在本实施例中,蜂窝网络基础设施)进行更改是必需的。PKI 或认证机构 20 支持专用消息传送(文本或呼叫控制)。用户生成公用加密密钥并发送到认证机构或 PKI 20。相应的解密密钥被机密地保存在加密芯片 60 例如 TPM 中。这允许用户安全地交换随机标签,从而使得用户可以互相呼叫并考虑安全的呼叫组。

[0142] 如图 1 具体所示,下面是认证机构的公钥基础设施提供的公钥实例 :

[0143] 公钥基础设施

[0144]

用户	公钥
PKI	)JKO#*$(HFF(U
网络	KJHF(Y#$(*YFG_
个人用户	)#(*)HEF(*Y#$H(*

[0145] (“Steve Wicker”)

[0146] 在本文所提供的专用重叠的一个实施例中,用户身份被与指向用户设备 30 的可在其中被寻呼的小区的数值标签相分离。专用重叠 10 仅需要为网络附加认证机构例如公钥基础设施和认证机构(PKI)20。PKI 为网络和所有用户提供公用加密密钥和私用解密密钥。另外,可以按下述方式来为现有蜂窝基础设施建立专用重叠。首先用户具有已经注册到蜂窝网络的蜂窝电话。可以由网络每天(或以适当的间隔)一次向每个授权用户传送相同的认证消息来启动专用注册。使用每个用户的公用加密密钥来对发送到所有用户的相同认证消息进行加密。

[0147] 对本领域技术人员来说，显然上述实施例能够很容易地改变以与无线网络中的任何无线设备一同使用(参见图 4)，或者与第三方数据接收和管理系统(参见图 8)或者公用事业配给系统中的通信网络内的客户数据采集单元(例如效用度量表)一同使用。

[0148] 5.2 用于保护网络内平台的用户隐私的方法

[0149] 还提供了一种用于保护网络内平台 40 的用户隐私的方法。该方法包含如下步骤：提供专用重叠 10，专用重叠 10 包含用于在公钥密码系统内分发经认证公钥的系统 20，其中平台 40 被包含在用户设备 30 内，并且该分发认证公钥系统 20 为网络以及该网络的每个授权用户提供针对该网络和每个授权用户的公用加密密钥。

[0150] 用户设备 30 可以例如是蜂窝电话、计算机或客户数据采集单元。

[0151] 在该方法的另一个实施例中，该分发认证公钥系统 20 是公钥基础设施及认证机构(PKI)。

[0152] 在该方法的另一个实施例中，该平台是蜂窝平台，且该网络是蜂窝网络。在另一个实施例中，该平台是无线平台，且该网络是无线网络。在另一个实施例中，该平台是客户数据采集平台，且该网络是通信网络。

[0153] 在该方法的另一个实施例中，生成并本地地存储私用解密密钥。可借助于本领域公知技术由该网络和授权用户安全地生成并存储私用解密密钥。网络将用户设备和不同于电话号码的随机数相关联，从而将该用户设备与用户身份相分离。

[0154] 在该方法的另一个实施例中，该平台是蜂窝平台，且该网络是蜂窝网络，该方法还包含步骤：蜂窝网络将用户设备和不同于电话号码的随机数相关联，从而将该用户设备与用户身份相分离。

[0155] 在该方法的另一个实施例中，该平台是无线平台，该网络是无线网络，且该方法还包含步骤：无线网络将用户设备和不同于个人相关帐号的随机数关联，从而将该用户设备与用户身份相分离。

[0156] 在该方法的另一个实施例中，该平台是公用事业或第三方数据接收和管理平台，该网络是通信网络，且该通信网络将用户设备(例如电表、燃气表或水表)和随机数关联，从而将用户设备与用户身份相分离。

[0157] 在该方法的另一个实施例中，专用重叠包含加密芯片，其中该加密芯片被嵌入在蜂窝平台中，并被编程以将认证消息保存在加密的安全库内。

[0158] 在该方法的另一个实施例中，该加密芯片是可信赖平台模块(TPM)。

[0159] 在该方法的另一个实施例中，该平台是蜂窝式的，且该加密芯片被编程以记录该用户设备在蜂窝模式下的通话时长。

[0160] 在该方法的另一个实施例中，该蜂窝电话通话时长是预付费的。

[0161] 在该方法的另一个实施例中，该平台是无线的，且该加密芯片 60 被编程以记录用户设备在无线模式下的无线使用时长。

[0162] 在该方法的另一个实施例中，无线使用时长是预付费的。

[0163] 在该方法的另一个实施例中，该加密芯片被编程以支持远程证明，该方法还包括步骤：网络远程地确定用户设备是否被授权。

[0164] 在该方法的另一个实施例中，该加密芯片被编程以支持远程证明，该方法还包括步骤：网络远程地确定用户设备是否被克隆。

[0165] 在该方法的另一个实施例中，该加密芯片被编程以支持远程证明，并且该方法包括步骤：网络远程地确定用户设备的硬件和 / 或软件是否被改变。

[0166] 在另一个实施例中，该方法还包括在专用模式（例如专用蜂窝或无线模式）下运行平台的步骤，其中当平台以专用模式运行时，网络不能将平台的位置数据与特定用户相关联。

[0167] 在该方法的另一个实施例中，以专用模式运行平台的步骤包含执行专用注册的步骤，其中专用注册包含如下步骤：

[0168] 网络周期性地（例如，以小时为间隔，每 12 小时，每日，每周等）向网络的每个授权用户传送相同的认证消息；并且网络使用用户的公用加密密钥来对传送给每个授权用户的认证消息进行加密。

[0169] 在该方法的另一个实施例中，网络周期性地传送相同的认证消息的步骤被每日执行。

[0170] 在该方法的另一个实施例中，以专用模式运行平台（例如蜂窝或无线平台）的步骤包含如下步骤：

[0171] 平台向网络发送专用授权注册（PER）消息；以及

[0172] 平台使用网络的公用加密密钥对 PER 加密，其中 PER 包含认证消息和随机设备标签（RET）。

[0173] 在该方法的另一个实施例中，PER 内的认证消息相当于零确认证明，其向网络表示 PER 由有效用户发送，并且 PER 内的认证消息不对该用户进行标识。

[0174] 在该方法的另一个实施例中，RET 是随机数。

[0175] 在另一个实施例中，该方法包含如下步骤：

[0176] 将 RET 输入到网络的访问位置寄存器（VLR）和归属位置寄存器（HLR）；以及

[0177] 将 RET 当作电话号码或帐户识别符，从而 VLR 和 HLR 收集建立和保持对平台的蜂窝电话或数据呼叫或无线数据连接所需的信息，但不将该信息与特定的用户、电话号码或用户帐号识别符相关联。

[0178] 在该方法的另一个实施例中，蜂窝电话或数据呼叫或者无线数据连接是呼入或呼出。

[0179] 在另一个实施例中，该方法包含将 RET 与临时 IP 地址相关联的步骤。

[0180] 在该方法的另一个实施例中，蜂窝电话呼叫是被叫通话，该方法包含如下步骤：

[0181] 将用户的 RET 和蜂窝网络的业务提供商的身份（例如网络 ID）分发给用户希望接收的蜂窝电话呼叫的各方，其中该分发步骤使用公钥加密。

[0182] 在该方法的另一个实施例中，用户执行该分发步骤。

[0183] 在该方法的另一个实施例中，认证机构执行该分发步骤。

[0184] 在另一个实施例中，该方法包含在蜂窝平台内嵌入加密芯片（例如 TPM）的步骤，其中加密芯片被编程以将认证消息保存在加密安全库内。

[0185] 在该方法的另一个实施例中，加密芯片（TPM）被编程以记录设备处于蜂窝模式下的蜂窝电话通话时长。

[0186] 在该方法的另一个实施例中，通话时长是预付费的。当超过所允许的通话时长时，加密芯片（例如 TPM）能够终止专用模式。

[0187] 在该方法的另一个实施例中，加密芯片(例如 TPM)支持远程证明，该方法包含网络远程确定设备是否被授权的步骤。例如，网络联系加密芯片，并使加密芯片对专用软件和设备 ID 执行计算，以确定该设备是否有效(即，该设备是否是克隆机)，以及确定硬件和 / 或软件是否被篡改。

[0188] 在该方法的另一个实施例中，加密芯片被编程以支持远程证明，该方法包含网络远程地确定设备是否被克隆的步骤。

[0189] 在该方法的另一个实施例中，加密芯片被编程以支持远程证明，该方法包含网络远程地确定硬件和 / 或软件是否被改变的步骤。

[0190] 5.3 加密芯片或可信赖平台模块(TPM)

[0191] 为了防止蜂窝或无线设备被克隆，用户设备可被设置有加密芯片例如可信赖平台模块(TPM)，其被编程以将认证消息保存在加密安全库内。TPM 和其他适合的加密芯片是本领域公知的。当用户希望进入专用蜂窝(或无线)模式时，用户可以使得用户设备向网络发送专用授权注册(PER)消息。PER 包含认证消息和随机设备标签(RET)，并且被使用网络的公用加密密钥加密。PER 内的认证消息相当于零确认证明，其向网络表示 PER 由有效用户发送，但并不实际地对该用户进行标识。RET 是随机数，其被输入到归属位置寄存器(HLR)和访问位置寄存器(VLR)中，并且看上去被当作电话号码或用户帐户识别符(个人帐户)。这种 HLR/VLR 记录被认为是私人蜂窝或无线环境(wireless context)。其会包含在标准 HLR/VLR 记录内可以找到的所有信息，但并不与特定的个人或他的电话号码或个人帐户相关联。只要用户设备保持在专用蜂窝或无线模式下，随后的注册消息将包括与用户电话号码或个人帐户不同的 RET。

[0192] 建立蜂窝电话呼叫、移动性管理以及漫游将完全和以前一样处理，区别在于 HLR 和 VLR 位置信息与 RET 而不是电话号码相关联。通过将 RET 与临时 IP 地址相关联，可保持数据呼叫的私密性。

[0193] 对于用户的主要操作区别在于被叫通话(在蜂窝平台下)或数据连接进入(在无线平台下)。对于在专用蜂窝模式下的用户设备能够完成被叫通话的唯一方法是如果主叫方获知被叫方的 RET 和网络 ID。(后者是必需的，以使得呼叫建立请求可以被送到适当的 HLR)。因此专用蜂窝模式下的用户必须将他或她的 RET 通过公钥加密分发给他或她希望能接收呼叫的各方。这类分发可通过认证机构实现。显然，此时要解决计费和通讯协助执法法案(CALEA)问题。服务提供商可能希望限制对每个 PER 所允许的通话时长。还可以依赖于用户设备内的 TPM 来实施用户设备在专用蜂窝模式下的每日或每月的限制。可以让用户为专用蜂窝时长预先付费，以使得电话看起来像是预付费蜂窝电话，从而部分地减轻 CALEA 的顾虑。

[0194] 可信赖平台模块(TPM)是 Trusted Computing Group™(TCG)开发的一组标准。这些标准是本领域公知的(例如参见 TCG SpecificationAechitecture Overview，Specification，Revision 1.4，2007 年 8 月 2 日；TPMMain Part 1Design Principles，Specification Version 1.2，Level 2 Revision103，2007 年 7 月 9 日，Trusted Computing Group Design，Implementation andUsage Principles，Version 2.01，Authorship:TCG Best Practices Committee，2005 年 12 月 1 日；所有文件均可以 PDF 格式在 www，trustedcomputinggroup.org 上下载，或者由 Trusted ComputingGroup™，

Beaverton,OR 获得。

[0195] TPM 执行很多功能,包括安全地生成和使用加密密钥。这些密钥被用于多种标准用途,包括远程证明、绑定、签名和印章(seal)。

[0196] 远程证明是一种通常通过不可伪造的哈希算法验证计算设备的硬件和软件的状态的机制。

[0197] 根据 TCG Specification Aechitecture Overview,Specification,Revision 1.4(可以 PDF 格式在 www,trustedcomputinggroup.org 上下载,或者由 Trusted Computing Group ™,Beaverton,OR 获得),“证明(attestation)是核对信息准确性的处理。外部实体可证明被隐藏的位置、受保护的性能以及可信根(Root ofTrust)。平台可以证明会影响平台完整性(可信赖度)的平台特性的具体说明。所有证明形式需要证明实体的可靠的证据。证明可以从几个维度来理解,由 TPM 证明,对平台证明,平台的证明和平台的认证。”(TCG Specification Aechitecture Overview,Specification,Revision 1.4,第 5 页)

[0198] 通过维持一组平台配置寄存器(Platform Configuration Register,PCR)来执行对 TPM 自身的证明。TPM 功能性的“快照”被测量并存储。这些测量结果的散列版本被称为“摘要”(digest)。PCR 包含测量摘要。

[0199] 根据 TCG Specification Aechitecture Overview,Specification,Revision 1.4,“测量内核生成测量事件。测量事件由两类数据组成:1)测量值—嵌入数据或程序代码的表示,和 2)测量摘要—这些数值的散列值。数据被生成消息摘要的测量内核扫描。摘要是机器操作状态的快照。这两类数据元素(测量值和测量摘要)被分开存储。测量摘要被使用 RTR 和 RTS 功能存储在 TPM 中。测量值可以任凭由测量内核虚拟地存储在任意位置。实际上,该数据可能根本未被存储,而是在任何需要序列表示形式的时刻被重新计算…TPM 包含一组被称作平台配置寄存器(PCR)的寄存器,其内含测量摘要。代数形式而言,对 PCR 的更新如下:PCR[n] ← SHA-1(PCR[n]+ 测量数据)。PCR 数据是临时的,在系统重启时其被重置。验证测量事件需要重新生成测量摘要。”(TCGSpecification Aechitecture Overview,Specification,Revision 1.4,第 8 页)

[0200] 绑定是使用公钥对消息加密。公钥加密技术使用一对密钥,一个公钥和一个私钥,以利于信息安全而不需要传输安全密钥。需要注意到,TPM 将私钥存储为“不可移动”密钥,即私钥不能被传输到另一个设备。TPM 通过将密钥保持在不可被篡改或访问的安全位置内来确保这类密钥的安全性。

[0201] 根据 TCG Specification Aechitecture Overview,Specification,Revision 1.4,“TCG 定义了四类受保护的消息交换:绑定、签名、印章绑定(Sealed-Binding)(又称印章)以及印章签名(Sealed-Signing) …绑定是使用公钥加密消息的传统操作。即发送者使用预期接收者的公钥加密消息。该消息仅能使用接收者的私钥解密恢复。当私钥被作为不可移动密钥由 TPM 管理时,仅有生成该密钥的 TPM 能够使用该密钥。因此,使用该公钥加密的消息被“绑定”到 TPM 的特定实例。生成可以在多个 TPM 设备之间转移的可移动密钥也是可行的。就其本身而言,绑定并没除了加密以外的特殊意义。”(TCG SpecificationAechitecture Overview,Specification,Revision 1.4,第 15 页)

[0202] 签名是生成数字签名。如上所述,数字签名通常被用于加强不可否认性(non-repudiation);关键在于确保对该消息签名的一方是他们所声称的人,而并非防止其

他人阅读该信息。

[0203] 根据 TCG Specification Aechitecture Overview，Specification,Revision 1.4,“签名在传统意义上也把消息的完整性与用于生成签名的密钥相关联。TPM把一些管理密钥标签为仅用于签名的密钥,这意味着这些密钥仅用于计算签名数据的散列值,并加密这些散列值。因此,它们不会被误理解为加密密钥。”(TCG Specification Aechitecture Overview,Specification,Revision 1.4,第 15 页)

[0204] 印章不仅要求接收用户具有必需的私钥,而且要求解密硬件处于特定的状态。该状态通过使用平台配置寄存器(PCR)来证明。

[0205] 根据 TCG Specification Aechitecture Overview，Specification,Revision 1.4,“印章是绑定的进一步操作。印章消息被绑定到消息发送者规定的一组平台度量。平台度量规定了在允许解密前必须存在的平台配置状态。印章将加密消息(实际上是用于加密消息的对称密钥)与一组 PCR 寄存器数值和一个不可移动非对称密钥相关联…通过选择一些 PCR 寄存器数值以及将 PCR 数值和用于加密消息的对称密钥进行非对称加密来生成印章消息。具有非对称解密密钥的 TPM 可能仅在平台配置与发送者规定的 PCR 寄存器数值匹配时才解密对称密钥。印章是 TPM 的非常有用的特征。其确保受保护的消息仅仅当平台在非常特定的已知配置下运行时才可恢复。”(TCG Specification Aechitecture Overview，Specification,Revision 1.4,第 15-16 页)

[0206] 签名也可以被印章,即关联到 PCR 寄存器的状态。根据 TCGSpecification Aechitecture Overview，Specification,Revision 1.4,“印章 - 签名…签名操作也可以链接到 PCR 寄存器,作为增加确保对消息签名的平台满足特定配置需求的方式。验证者指示签名必须包括一些特定 PCR 寄存器。签名者在签名操作期间采集所规定 PCR 寄存器的数值,并把这些数值包括在消息内,并用作计算签名消息摘要的一部分。随后验证者检查签名消息内的 PCR 值,这与在生成签名时检查签名平台配置是等同的。”(TCG Specification Aechitecture Overview,Specification,Revision1.4,第 15 页)

[0207] TPM 提供多种其他服务。在 TCG Specification AechitectureOverview 的章节 4.6.3 内汇总了标准 TPM 指令。图 2 所示的选录标注了 Sign,GetRandom 和 StirRandom 指令可用于常规的加密用途,例如生成密钥。

[0208] 如从 TPM Main Part 3commands,Specification Version 摘出的下述选录可以看出,TPM 的 GetRandom 指令从随机数发生器返回所请求数量的字节：

[0209] “13.6TPM_GetRandom

[0210] 信息注释开始：

[0211] GetRandom 从随机数发生器向主叫方返回下一个 bytesRequested 字节。

[0212] 推荐的是,TPM 以允许 TPM 返回 RNG 字节的方式执行 RNG,从而使得 bytesRequested 的字节小于可用字节数量的发生频率很低。

[0213] 操作

[0214] 1.TPM 确定 bytesRequsted 的数量是否可从 TPM 获得。

[0215] 2. 将 randomBytesSize 设为可从 RNG 获得的字节数。这个数可能小于 randomBytesSize。

[0216] 3. 将 randomBytes 设为从 RNG 获得的下一个 randomBytesSize 字节。”(TPM Main

Part 3Commands.Specification Version 1.2, 第 91 页)。

[0217] StirRandom 指令通过更新随机数发生器的状态为随机数发生器的状态增加熵。

[0218] “13.7TPM_StirRandom

[0219] 信息注释开始：

[0220] StirRandom 为 RNG 状态增加熵。

[0221] 操作

[0222] TPM 使用适当的混合功能更新当前 RNG 的状态。”

[0223] (TPM Main Part 3Commands.Specification Version 1.2, 第 92 页)

[0224] 该标准中关注设计原理的部分可从“TPM Main Part 1 DesignPrinciples. Specification Version 1.2,Level 2Revision 103,2007 年 7 月 9 日，可以 PDF 格式在 www,trustedcomputinggroup.org 上下载，或者由 TrustedComputing Group™, Beaverton,OR 获得,本文中简称为“TPM Main Part1”。如下所述，TPM Main Part 1 列出了如果所得到的 TPM 要与标准兼容,设计者所必须遵循的需求：

[0225] “TPM 设计者必须阅读和实施 TPM Main specification(部分 1-4)的信息,并阅读针对所期望平台的平台专用文献。平台专用文献包含可能影响 TPM 设计和实施的规范声明。”(TPM Main Part 1, 第 1 页)

[0226] TPM 的基本要素如图 3 所示。上述附图的左上方所示的加密协处理器被设计用于和该结构内其他元件一起执行下述的各种加密功能。

[0227] TPM Main Part 1 声明“加密协处理器,图 2 :C1 执行 TPM 内的加密操作。TPM 采用传统方式执行传统的加密操作。这些操作包括如下形式：

[0228] 不对称密钥生成(RSA)

[0229] 不对称加密 / 解密(RSA)

[0230] 散列计算(SHA-1)

[0231] 随机数发生(RNG)

[0232] TPM 使用这些功能来执行随机数据的发生、不对称密钥的生成、已存储数据的签名和保密。

[0233] TPM 可能在 TPM 内部使用对称加密,但不会对 TPM 的常规用户公开任何对称算法函数。

[0234] TPM 可以执行附加的不对称算法。执行不同算法的 TPM 设备具有不同的执行签名和封装的算法。

[0235] (TPM Main Part 1, 第 12 页)

[0236] 如上所述,加密算法可以是对称和不对称的(公钥)。这些算法的密钥也被称为对称或不对称的。如下所述，TPM 并未被设计为提供开放的对称密钥加密技术。这限制由另一设备使用来生成、存储和保护这些密钥。使用随机数发生器(RNG)执行对称密钥的生成。一旦生成密钥后,执行绑定和印章以便于密钥的传送。

[0237] TPM Main Part 1 声明“由于 TPM 不具有开放的对称算法,TPM 仅是对称密钥的生成器、存储设备和保护器。可使用 TPM RNG 生成对称密钥。存储和保护可通过 TPM 的 BIND 和 SEAL 功能来实现。如果主叫方想确保在传送给主叫方时未绑定 / 未印章之后,对称密钥的释放不会开放,那么主叫方应使用带有机密协议的传送会话…对于不对称算法,TPM 生成

并操作 RSA 密钥。这些密钥可仅由 TPM 持有，或者由 TPM 的呼叫者共同持有。如果密钥的私用部分在 TPM 外部使用，主叫方以及密钥的用户有责任确保保护好该密钥。”（TPM Main Part 1, 第 13 页）

[0238] 下列实例仅用于阐释，而不是限制性的。

[0239] 6. 实例

[0240] 6.1 实例 1 :专用蜂窝覆盖

[0241] 该实例阐释了用于蜂窝系统的专用重叠通过严格分离设备身份和用户身份来保护用户的隐私。

[0242] 引言 :公钥加密技术

[0243] 公共密钥加密涉及两种不同的密钥，一种用于加密，另一种用于解密。任何使用了加密密钥进行加密的明文仅能由具有解密密钥的人进行解密。如果设计得当，不经过解决非常困难的数学问题是不可能由一个密钥获得另一个密钥的。因此可以公开加密密钥，可能将其在线粘贴，以使得任何人可加密消息，并把被加密的消息发送给所期望的用户，而不用担心该消息能够被任何不具有该机密的解密密钥的人读取。只要该解密密钥被保持为机密，该消息就保持安全。Diffie 和 Hellman 在 1976 年引入了公钥加密技术。接下来的显著进步是在 70 年代后期由 Rivest, Shamir 和 Adleman 以及他们关于 RSA(此缩写包含每个发明人的姓氏的首字母)密码系统的发明所实现的。RSA 密码系统使用本领域已知算法实现公钥加密(该算法主要依赖于对大数进行模幂乘)。RSA 加密算法的安全性被假定基于将非常大的数字分解为 A×B 的形式的难度，其中 A 和 B 是大的质数。尽管从未被确定地证明，但是通常认为从相应的加密密钥获得较好选择的 RSA 解密密钥(或反之)的唯一方式是分解两个大质数的乘积。这是易于理解的、但已知非常困难的问题。RSA 密钥比对称系统密钥大很多，但并没有大到无法实现的程度。本领域中通常认为 3072 位的 RSA 密钥与对称密钥系统中的 128 位密钥提供了相同级别的安全性(例如参见 http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf)。具有两种不同密钥的另一个值得注意的方面是该系统能够被用于产生安全的数字签名以及提供安全的通信。

[0244] 例如，假定一个买家写信给在线书商希望定购一本书的几百份副本。一旦接收到该信件，该书商希望核实确实是发信的那个个人用户。进一步假定该买家公开了一个 RSA 解密密钥，同时保持相应的加密密钥为机密。买家向书商一起发送该信件的明文拷贝和加密拷贝，后者使用买家的机密加密密钥进行了加密。当销售商使用买家的公开解密密钥时，销售商恢复出明文，并检查是否与买家的信相同。随后销售商确信买家确实发送了该信件，因为仅有买家持有生成加密拷贝所需的加密密钥。这种保证可以被形式化，如下所述。本实例中的密文是任何人可以阅读但仅有买家可生成的签名。数字签名在许多方面实际上都比旧式的各种签名更加安全，因为数字签名不能够被传送给不同的文件——它总是与在生成该签名时所加密的文本相关联的。

[0245] 进一步假定一组个人生成两组密钥，第一组用于内容加密，第二组用于生成数字签名。这组人公开了第一组的加密密钥以及第二组的解密密钥，同时保持每对密钥的另一半为机密。假定这组人中的一个成员 Alice 想向这一组的另一个成员 Bob 发送一个签名的机密消息。Alice 首先使用她的机密加密密钥对消息加密，从而将消息转换成签名。随后她使用 Bob 的公开加密密钥对签名加密。因此原始消息被加密两次，第一次使用 Alice 的机

密加密密钥，然后使用 Bob 的公开加密密钥。当 Bob 接收到密文时，他首先使用他的机密解密密钥来恢复签名。然后他使用 Alice 的公开解密密钥来恢复原始消息，同时使他本人确信这封信确实来自 Alice。

[0246] 因此公钥加密技术在可信赖通信中起到重要作用。但仍有一方面不足：在上述 Alice 和 Bob 的通信中，Alice 假定 Bob 的公用加密密钥确实由 Bob 生成。但是如果 Eve（窃听者）公开了密钥而伪装成来自 Bob 会怎么样？如果她能够做到这点，那么任何可能来自 Bob 的机密消息都可以被 Eve 阅读。为了防止这一点，公钥必须被认证。换句话说，Bob 签名机密消息的接收者必须确信 Bob 的密钥确实由 Bob 生成，并且仅有 Bob 具有相应的私钥。或者用更现代的术语来解释，当我们使用公钥例如向在线销售商发送信用卡信息时，我们期望确保确实是在线销售商提供了该密钥。

[0247] 目前本领域对该问题的已知解决方法采用了公钥证书的形式。公钥证书将公钥和用户身份绑定，其形式与护照将个人信息（姓名、出生日期、出生地等）与护照照片绑定的形式大致相同。护照是可信赖的第三方—联邦政府颁发的官方文件。

[0248] 只有请求人提供了足够的文件证明该用户是她所声称的人，联邦政府才会颁发护照。一旦联邦护照机构接收到所有必需的文件和几张照片，该机构将会核实文件并颁发护照。机场和移民机构想必熟悉这一过程。当他们看到一份护照，并把所附照片与持有者的脸进行比较，随后他们希望把文件上的数据与持有者关联。公钥证书可以基本相同的方式生成和使用。

[0249] 目前，电子商务零售商到注册机构提供足够的文件来证明他们的企业身份。一旦他们的身份得到验证，相关的认证机构就生成公钥，并将该公钥置于证书上，将该证书和与该密钥相关的实体的信息进行绑定。该认证机构对该证书进行数字签名，从而使得已认证实体的顾客可对该证书进行验证。注册和认证机构以及其他相关职能机构通常被发现属于称作公钥基础设施（PKI）的单个实体。已经出现了一些作为支配性网络商务 PKI 的大公司，例如 VeriSign。它们通过多种方式建立了信任，包括可靠性、高达 250,000 美元的现金授权（参看 http://www.verisign.com/ssl/buy-ssl-certificates/index.html?tid=a_box），并且事实是，如果它们滥用了对于它们的信任，那么它们作为公司的价值将会在一夜间消失。许多网络浏览器被设置为自动地从已知 PKI 接收证书，因此不需要个人用户考虑这些事情。

[0250] 例如，假定一个买家希望到一个在线书商的网站来购买一本书的几份副本。这个买家首先在他的浏览器顶部的 URL 栏内输入该书商的 URL，然后进入该书商的主页。这个买家随后将书的副本放入一个虚拟的购物车中，然后结算。此时开始执行对于大多数用户未知的加密处理。该书商将含有公共加密密钥的证书发送到买家的浏览器。如果买家愿意，他可以通过点击所显示的锁定图标来实际查看该证书，该图标表示在一些浏览器内的安全浏览。这些证书包含大量信息，包括签名权限、公共加密密钥以及所使用的加密算法。对于该实例，该证书由认证服务商例如 VeriSign 签名，并调用具有特定长度即 2040 位的密钥进行 RSA 加密。在核实该证书之后，这个买家的浏览器产生用于对称密钥密码系统的 128 或 256 位的密钥。使用证书上的 RSA 公共加密密钥对该密钥进行加密，并且所产生的密文被发送给在线销售商。销售商和买方现在共享了机密对称密钥，并且他们现在可以安全地交流。电子商务的成功依赖于通过公钥加密技术和可信的第三方，例如认证服务商如 VeriSign，

所产生的信任。

[0251] 虽然一些政府部门做出了努力，商业部门享受到市场的扩展，同时公众也享受到巨大的购买机会。下列实例阐释使用本文所公开的方法时，公钥密钥加密技术可被修改为支持个人的私密利益。

[0252] 专用蜂窝覆盖

[0253] 只要蜂窝概念需要一台设备位于特定小区内，蜂窝系统内就存在 MSC 能够将用户设备定位到一个或少量的小区地点的程度的需求。但是重要的是应注意到，是设备而不是特定的人即用户需要被定位。本文所提供的用于蜂窝系统的专用重叠(图 1 和 4)通过严格分离设备身份和用户身份来保护用户的隐私。在本实例中所述的专用蜂窝覆盖的实施例采用了用于在公钥密码系统内分发经认证公钥的系统。使用 PKI 类型的处理来认证密钥，这对本领域技术人员来说是公知的。

[0254] 用于在公钥密码系统－认证机构或 PKI（或其等同功能）内分发认证公钥的系统为网络和所有用户提供公用加密密钥以及私用解密密钥。现有蜂窝基础体系增加专用重叠可如下建立。

[0255] 本实例具体描述了一个实施例，其中使用具有标准性能的蜂窝电话，该蜂窝电话被增加了在专用模式下运行的功能，即网络不能够将电话的位置数据与特定用户关联的模式。对于本领域技术人员来说，显然使用本领域已知的其他蜂窝或无线平台也是可以预想到的。

[0256] 专用模式基于专用注册过程，该过程由网络每天(或以适当的间隔）一次向每个授权用户发送相同的认证消息来启动。使用该用户的公用加密密钥对发送到每个用户的认证消息进行加密。

[0257] 当用户希望进入专用蜂窝模式时，用户使得蜂窝平台向网络发送专用授权注册(PER)消息。由认证消息和随机设备标签(RET)组成的 PER 使用网络的公用加密密钥对 PER 加密。PER 内的认证消息相当于零确认证明，向网络表明 PER 由有效用户发送，但实际上不用于标识该用户(下面将解决克隆的问题)。

[0258] RET 是随机数，其可以被输入到访问位置寄存器(VLR）和归属位置寄存器(HLR)，并被当作电话号码。VLR 和 HLR 收集建立和保持对于蜂窝平台的电话呼叫所需的所有信息，但不把所述信息与特定的用户或电话号码相关联。只要用户保持专用蜂窝模式，随后的注册消息包括与用户电话号码不同的 RET。

[0259] 建立蜂窝电话呼叫、移动性管理以及漫游将完全和以前一样处理，区别在于 HLR 和 VLR 位置信息与 RET 而不是电话号码相关联。通过将 RET 与临时 IP 地址相关联，可保持数据呼叫的私密性。本领域已知的通用分组无线业务(GPRS）标准的一个版本可用于任何匿名的分组数据协议(Packet Data Protocol,PDP)环境。该环境将 SGSN 处的 PDP 地址与临时的逻辑连接识别符相关联；IMSI 不与 PDP 地址相关联，因此环境是匿名的。具体细节在 ETSI GSM 03.60 的章节 9.2.2.3 的早期版本中有过具体描述，但后来从该标准中删除。

[0260] 被叫通话要求主叫方已知 RET。为了将 RET 与正确的 HLR 相关联，主叫方可识别为被叫方提供服务的服务提供商。因此专用蜂窝模式下的用户可使用公钥加密来向他或她愿意接收呼叫的各方分发他或她的 RET 以及服务提供商的身份。可以使用为被叫通话建立的专用环境来建立专用模式下蜂窝平台的呼叫，或者可替换的，使用不同的随机字符串基于

每次呼叫来注册呼出通话。这会减少与单个随机字符串相关的信息量，从而减少了服务提供商将专用环境与特定用户关联的能力。

[0261] 克隆和收费问题都可以通过在蜂窝平台内建立可信赖平台模块（TPM）解决。TPM（或等同设备）可被编程以将认证消息保存在加密安全库内，因此试图将认证消息转移到另一个平台的任何人均不能够获得该认证消息。因此当网络接收到 PER 消息时，网络可以确保发送该消息的电话实际上从网络接收到了认证消息。远程证明可被用于确保控制 TPM 的软件没有被改变。

[0262] 至于收费，服务提供商面对一个不便的任务是为未知方提供服务。解决方法仍然在于 TPM。可通过平台内软件控制该平台可用的专用通话时长的数值，其中该软件可以通过远程证明来认证。在一个实施例中，专用通话时长是预付费的。将专用模式按照预付费业务来考虑具有潜在的与通信协助执行法案（CALEA）相关的显著优点，因为 CALEA 目前不覆盖预付费蜂窝电话。在美国以及其他许多国家，人们可购买和使用预付费蜂窝电话，而不用将姓名和电话相关联。因此本文公开的专用重叠为后付费蜂窝电话用户提供了预付费电话的专用益处。

[0263] 6.2 实例 2：匿名认证

[0264] 本实例和实例 6.3 考虑了对于信息网络应用考虑隐私的设计的实际情形。本实例描述了一种专用重叠，其解决了对于信息网络（例如蜂窝、无线）常见的问题－用户认证的需求，同时努力减少数据和个人的识别度。本实例具体介绍了无属性需求产生了能够支持实践工程师在他或她开发考虑隐私系统的工具的需求。在章节 6.3，实例 3 中，公开了一种考虑隐私的需求响应系统。在实例 3 中，还解决了几个架构性问题，强调了分布式处理需求的重要性。

[0265] 在许多不同的场景下，移动计算和通信网络中出现了认证问题，从蜂窝电话呼叫到在咖啡店内访问互联网。因此认证问题是向服务提供商证明你就是你声称的那个人。但是如果在减小设备和个人的识别度的理念下再深入探究一点点，就会看出从服务提供商的出发点来看，问题的真正实质是确保能够为所提供的服务接收到费用。因此无属性需求可能被满足；服务提供商不是必须知道向谁提供业务，而只要确保支付到位即可。如果可以建立匿名认证，则运行服务所必需的任何数据采集（例如被叫通话被路由到蜂窝电话所需的位置信息）都是匿名的。

[0266] 匿名认证的特点是零确认证明。用户可能希望向服务提供商证明他或她是授权用户池中的一员，而不用提供任何个人识别信息。章节 6.1 的实例 1（图 1）公开了对于蜂窝电话的特定应用方案的一种可行的解决方法，尽管有经验的从业人员显然理解该方法可以应用到许多应用中，例如无线网络或公用通信网络或第三方数据和接收管理。可提供能够为网络和用户分发公钥的公钥基础设施（PKI）。服务提供商周期性地为所有被授权使用网络的用户分发认证消息。认证消息对于所有用户都是相同的，但使用各个特定用户的公钥进行加密。加密后的认证消息可使用电子邮件、无线控制信道或者任何适用于该应用的手段进行传送。在一些实施例中，认证消息是不可转移的，此时可以采用加密库技术，例如可信赖平台模块（TPM）。

[0267] 如果用户希望认证以获得服务，认证消息和用于标识设备的随机标签一起被发回到网络。使用网络的公钥对认证消息进行加密。一旦接收到该消息，网络就得知用户请求

访问是有效的，因为用户知道认证消息。但是网络不知道用户的身份。随后网络可以根据需求使用随机标签联系用户设备并为用户设备提供访问权限。

[0268] 上述专用重叠的实例阐释了无属性需求的应用：建立了一种用于保护用户隐私的系统，如果需要的话，网络可和用户设备交互以及追踪该用户设备，而不用知道该设备属于谁。这种设计用于保护用户的隐私，并允许专用和匿名使用。

[0269] 6.3 实例 3：需求响应和分布式处理

[0270] 公用事业采用了微网格以及其他提供能源生产中的节省成本的系统，其增加了网格可靠性和灵活性，并生成新的客户 - 公用事业交互模式(例如参看 Federal Energy Regulatory Commission,(2009 年 9 月),2009Assessment of demand response and advanced metering,Staff Rep.http://www.ferc.gov/legal/sraff-reports/sep-09-demand-response.pdf)。需求响应系统在这一方面起到关键作用。一般而言，需求响应系统通过终端使用者对电力价格随时间的变化来调整电力消费行为(M.H.Albadi 和 E.F.El-Saadany,A summary of demand response in electricity markets,Electric Power syst.Res., 第 78 卷 , 第 1989-1996 页，2008 年)。不管是为客户提供价格信息还是由公用事业公司直接控制设备而产生的调整，都会改变需求时间、瞬时需求等级、或者在给定时间周期内的总需求(OECD, Internation Energy Agency,The Power to Choose - DemandResponse in Liberalized Electricity Markets, 巴黎，法国，2003)。总体目标是平衡电力随时间的消费，以减轻使得发电机在线和离线的公用事业(昂贵)需求。

[0271] 需求响应系统所需的电力消费信息的精度级别要远比每月支出精细的多。原因很简单：如果一天当中根据价格调整消费行为，那么消费信息必须具有与价格信息相同级别的精度，从而适当地向客户收费。解决方案是高级计量基础设施(AMI)，它不同于过去的每月一次地读表，其是可以按分钟来对电力消费进行采样和记录的技术。AMI 开发已经进行了数年。联邦能源监管委员会预计在 2009 年将在全国安装 795 万台高级计量表(Federal Energy Regulatory Commission,(2009 年 9 月),2009Assessment of demand response and advanced metering,Staff Rep.http://www.ferc.gov/legal/sraff-reports/sep-09-demand-response.pdf)。到 2009 年为止，19 个州的 29 家公用事业公司宣布或实施了高级计量试点或者全面部署程序。

[0272] 需求响应的潜在影响是巨大的。如图 5 所示(Federal EnergyRegulatory Commission,(2009 年 9 月),2009Assessment of demandresponse and advanced metering,Staff Rep.http://www.ferc.gov/legal/sraff-reports/sep-09-demand-response.pdf)，根据 AMI 分布的水平，美国在电力需求的夏季高峰期，电力总负荷的潜在节省可从 4％到 20％。这对美国对外国石油和相关资源的需求的正面影响是很难夸大的。

[0273] 更具体地参看图 5，可以看出节能程度是 AMI 参与率的函数。图 6 给出了不同场景的注释。

[0274] 比较图 6 和图 5，注意到 B 选择加入参与场景的节能预计 9％，而强制的统一方式是 20％。如果调整者要求用户在他们的家里安装高级计量表，那么峰值消费额外降低 11％是可行的。这个问题将具有全国性的意义，因为除非 AMI 被正确安装，否则它将造成严重的隐私威胁。

[0275] Lisovich 等人表示高级计量系统采集的具体电力消费数据泄漏了室内活动的信息(参见 M.Lisovich,D.Mulligan 和 S.B.Wicker,Inferringpersonal information from demand-response systems,IEEE Security PrivacyMag. 第 8 卷第 1 期,第 11-20 页,2010 年 1/2 月)。另外,这些数据可以和其他易获得的信息组合,甚至能发现所有者的更多活动信息(M.Lisovich,D.Mulligan 和 S.B.Wicker,Inferring personal informationfrom demand-response systems,IEEE Security Privacy Mag. 第 8 卷第 1 期,第 11-20 页,2010 年 1/2 月)。这一结果是根据在标准学生宿舍(具有了适当的隐私保护,并且获得了住宿人员的明确许可)中进行的实验而获得的。所制造的电力使用监控仪被连接到住宿人员的断路器面板以采集实时的电力消费数据。这些数据以每 1 秒或 15 秒的间隔获得,分辨率为 1w,该数据被传送到在工作站上运行的非侵入式负载监测(NILM)应用程序。随后在工作站上运行行为提取算法以试图仅基于电力消耗来预测行为。使用视频数据来建立对该实验的控制。

[0276] 该实验的一些结果在图 7a-d 中介绍。图 7(a) 描述了几天中累计的电力消费数据。垂直轴用瓦特标注,而水平轴表示几天中的时间流逝。每天内几个主要的电力消费峰值表明住所内的活动。

[0277] 图 7(b) 示出了对于几百秒内采集的电力消费数据应用边缘检测算法的结果。边缘检测算法相当简单并且是本领域公知的 :这幅图表示相邻时间的电力消费样本间的差值。垂直轴表示 Δ(t) = P(t)-P(t-1),其中 P(t) 是在时刻 t 的电力消耗采样。水平轴表示时间。注意到现在可以分离出特定的切换事件 ;很容易看出冰箱和微波炉生成的电力消耗瞬变。

[0278] 图 7(c) 是负荷识别程的屏幕截图。其显示出如何对一天(水平轴的单元是天)内的事件进行分离和分类。通过这类信息,我们可以估计出个体在室内的行为。

[0279] 图 7(d) 示出电力消费数据可被用于估计与个人行为相关的变量。参考线表示实际行为。在“参考作息线”之上,零表示居住者在入睡 ;一表示他醒着。在“参考存在线”上,零表示住所的居住者不在家 ;一表示他在家。估计线表示我们对这些事件的估计结果。注意到参考数据和估计数据相当接近。

[0280] 既然电力消费数据产生了隐私问题,那么很显然集中的采集会使得采用公用事业设施的用户感到不安。然而集中采集看起来是将要实施的方向。在下面从 2006FERC “Assessment of Demand Response andAdvanced Metering”的摘要中,AMI 被定义为提供集中采集的系统。看起来并没有对客户隐私需求更敏感的架构选择的考虑。

[0281] 出于这篇报告的目的,委员会人员将“高级计量”如下定义 :“高级计量是每小时地或以更高的频率来记录客户消费的计量系统,其通过通信网络将每天的或更高频率传送的测量结果传送到集中采集点”(Federal Energy Regulatory Commission,Assessment of demand responseand advanced metering,Washington,DC,Staff Rep.,Docket No.AD06-2-000,2006 年 8 月,第 6 页)。

[0282] 上述定义已经被公用事业设施引用,并被本领域认可(E.Steel 和 J.Angwin,On the web’s cutting edge,anonymity in name only,Wall Street J.,04.8 月 2010)。该定义也已经在 FERC 公开的高级计量基础设施(AMI)文献中以图示表示,参看图 8(Engineering Power Research Institute,Advanced Metering Infrastucture.http://

www.ferc.gov/eventcalendar/Files/2-0070423091846-EPRI%20-%20Advanced%20Metering.pdf)。注意到参考文献是对于第三方数据接收和管理的可能性做出的。这有争议地增加了所获得数据的不符合规范使用的可能性，包括市场人员和其他人的商业化和随后的再使用。

[0283] 需求响应系统的长期未来是有风险的。消费者对于潜在的侵犯隐私变得警醒，从而有动机促使立法寻求该系统的昂贵替换形式。司法措施也可能使得该项目具有风险。无论是来自公众的呼吁或者司法行为，放弃隐私的系统最终会没有出路。

[0284] 但是通过考虑隐私设计的放大镜来看需求响应系统，保有隐私的技术方案是很明显的。需求响应系统的目标是，不管是诱导还是直接控制，通过使用更精细的价格信息来调整消费行为。利益－消费行为分别很大。当考虑分布式处理需求时，显然不是必需采集电力消费数据，而实际上需要分发价格数据。更精细的消费信息需求从不会离开近邻，因此减轻了大多数的隐私顾虑。

[0285] 考虑隐私的需求响应结构必须解释几个不同的数据流。对于每个数据流，需要执行隐私分析，并且如果需要的话，采用考虑隐私的设计。首先，在寻求改变客户行为的系统内，价格数据必须被提供给客户，以使得他／她具有做出消费决策的基础。这不存在隐私顾虑，因为公用事业公司可以把价格广播到住所的计量表和／或客户的家用计算机上的应用程序。

[0286] 其次，在直接控制系统中，公用事业公司必须向设备发送信号以控制设备在一天当中的电力消耗。尽管这会产生严重的安全隐患，但并不会产生关于客户在家中的行为及偏好的信息。

[0287] 第三个数据流更加有问题。客户特定的消费数据必须提供给公用事业公司以用于收费。此时存在一个问题，因为人们不能在不产生前述隐私问题的情况下向公用事业公司传送消费数据。人们也不能传送实时消耗数据，因为这对于将信息转换成消费数据是不重要的。解决方法是累加住所的价格加权后的消费数据，然后将累加成本每周或每月发送到公用事业公司。这意味着计量表需要可信赖平台模块或等同形式的安全级别。

[0288] 最后，公用事业公司需要暂时精确的消费数据，但以客户级别累加，以预测需求并维持价格模型。通常，在子站点级别累加后的实际电力消耗数据已经足够用于预测新的传输和分配线的需求，以及为所预测需求服务所需的生产。近邻的累加器可以被用于组合和匿名数据，从而提供所需的暂时精度，而不会生成关于个人行为的信息。可以通过累加一定数量的客户的电力消费数据来执行匿名操作，因此不能分离出单个客户的数据。上述解决方案被嵌入在图 9 所示的架构中。

[0289] 本发明不局限于本文所述的特定实施例。实际上，对于本领域技术人员来言，除了本文所述形式之外，显然可根据前述说明对于本发明做出各种修改。这类修改应落入所附权利要求书的范围内。

[0290] 本文所应用的参考文献被以全文引用方式且通用地并入，就如同每篇公开文献、专利或专利申请被单独且特别指定为其通过全文引用方式且通用地并入一样。

[0291] 任何公开文献的引用是出于早于申请日的公开的目的，并且其不应被解释为承认本发明无权由于在先发明而早于这些公开文献。

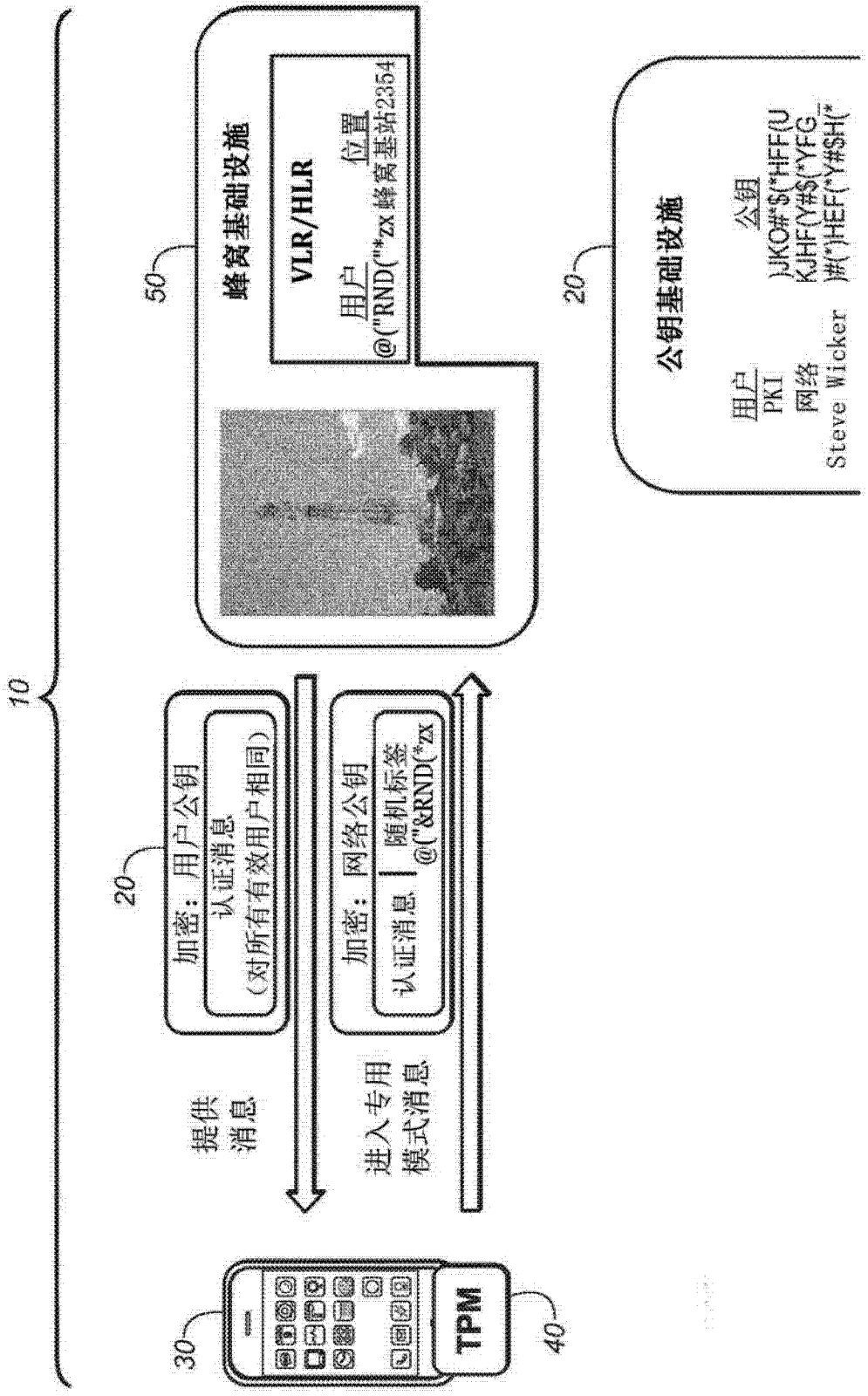

10
蜂窝基础设施
50
VLR/HLR
用户 位置
@("RND("*zx 蜂窝基站2354
公钥基础设施
20
用户 公钥
PKI JJKO#*$(*HFF(U
网络 KJHF(Y#$(*YFG
Steve Wicker)##(")HEF(*Y#$H(*
20
加密：用户公钥
认证消息
（对所有有效用户相同）
提供
消息
加密：网络公钥
认证消息 | 随机标签
@("&RND("zx
进入专用
模式消息
30
TPM
40

图 1

TPM的各种服务	加密命令	*TPM_Sign* *TPM_GetRandom* *TPM_StirRandom*	这些命令提供常规加密服务
	核查命令	*TPM_GetAuditEvent* *TPM_GetAuditEventSigned* *TPM_SetOrdinalAuditStatus* *TPM_GetOrdinalAuditStatus*	这些命令被用于采集核查追踪数据和控制核查特征
	性能报告命令	*TPM_GetCapability* *TPM_GetCapabilitySigned* *TPM_GetCapabilityOwner*	这些命令提供TPM的部分及所实现的功能的信息

图 2

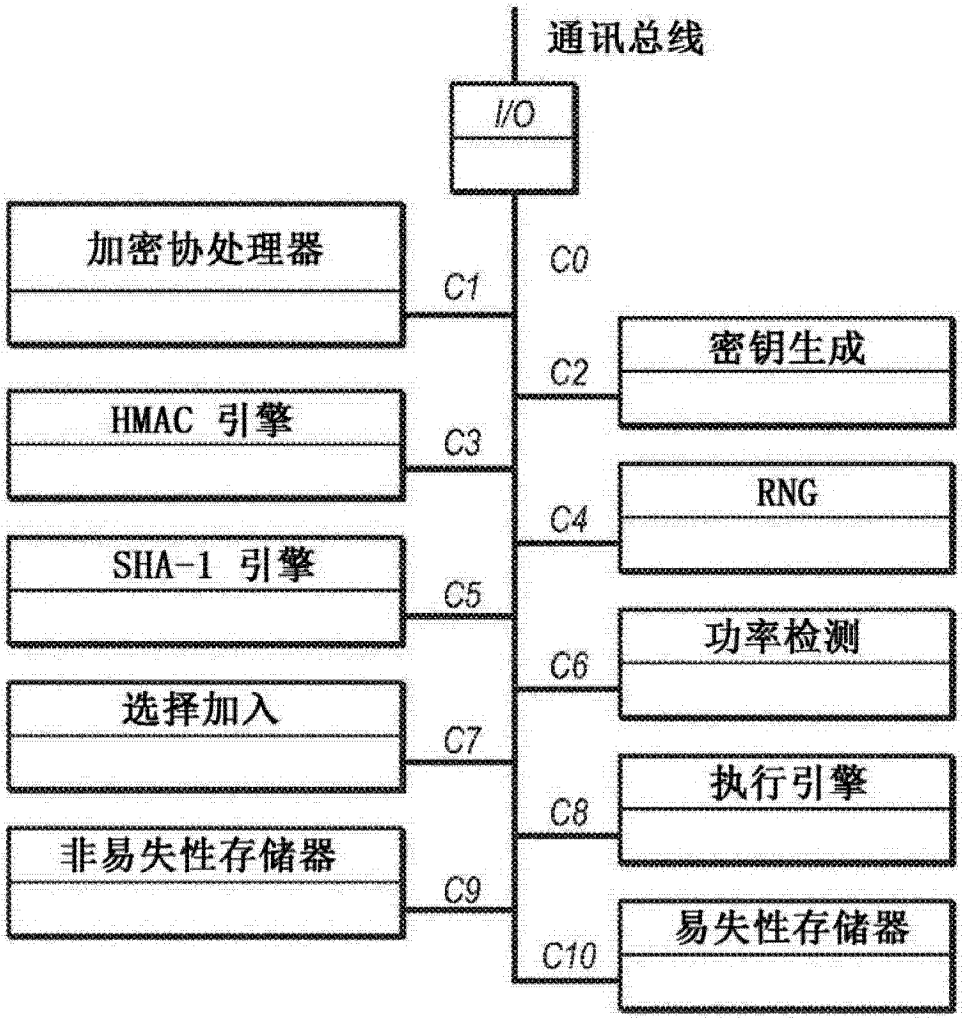


图 3

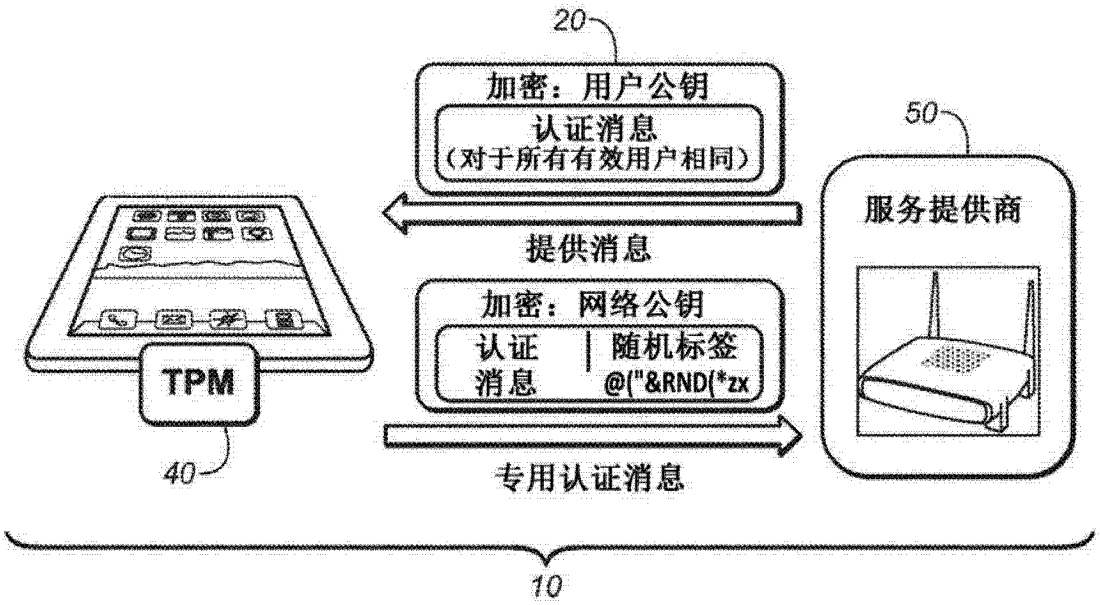

20
加密：用户公钥
认证消息
（对于所有有效用户相同）
50
服务提供商
提供消息
加密：网络公钥
认证消息
随机标签
@("&RND(*zx
TPM
40
专用认证消息
10

图 4

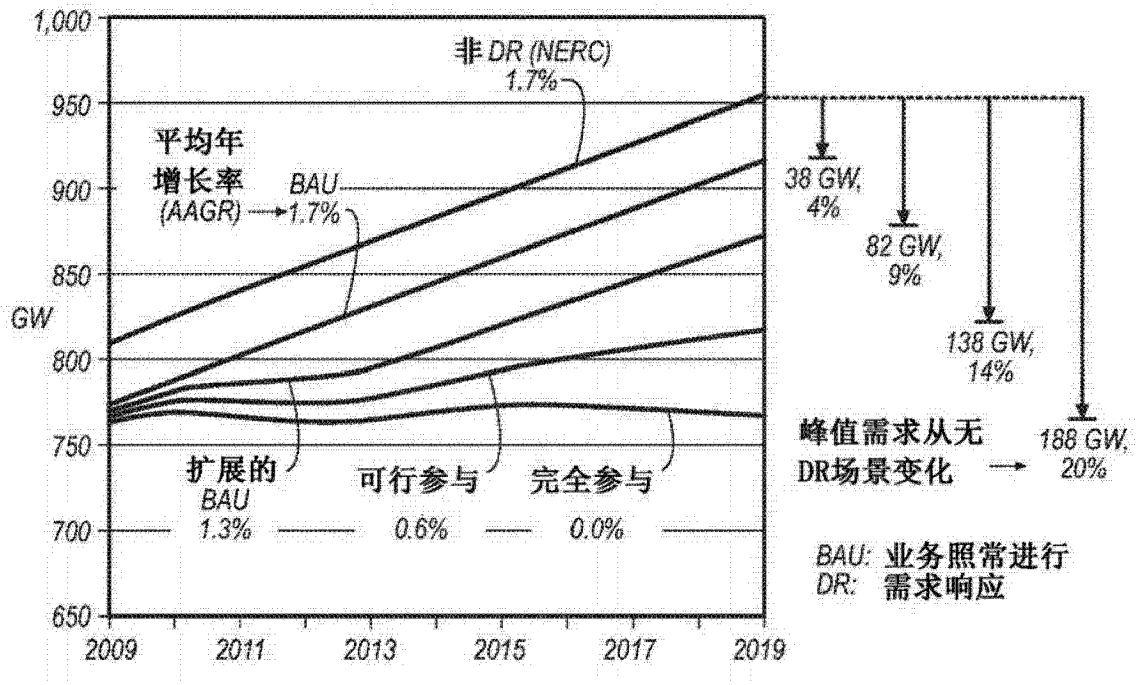

1,000
950
900
850
800
750
700
650
GW
非 DR (NERC)
1.7%
平均年
增长率
(AAGR)
BAU
1.7%
扩展的
BAU
1.3%
可行参与
0.6%
完全参与
0.0%
38 GW,
4%
82 GW,
9%
138 GW,
14%
188 GW,
20%
峰值需求从无
DR场景变化
BAU: 业务照常进行
DR: 需求响应
2009
2011
2013
2015
2017
2019

图 5


假设
业务照常
扩展的BAU
可行参与
完全参与
AMI部署
部分部署
部分部署
完全部署
完全部署
动态定价参与（符合条件的）
当日级别
自愿(选择加入) 5%
默认(选择退出) 60%至75%
通用(强制) 100%
符合条件的客户被提供了授权技术
没有
没有
95%
100%
符合条件的的客户接受授权技术
没有
没有
60%
100%
以未定价参与率为基础
当日级别
"最佳实施"预测
"最佳实施"预测
"最佳实施"预测

图 6

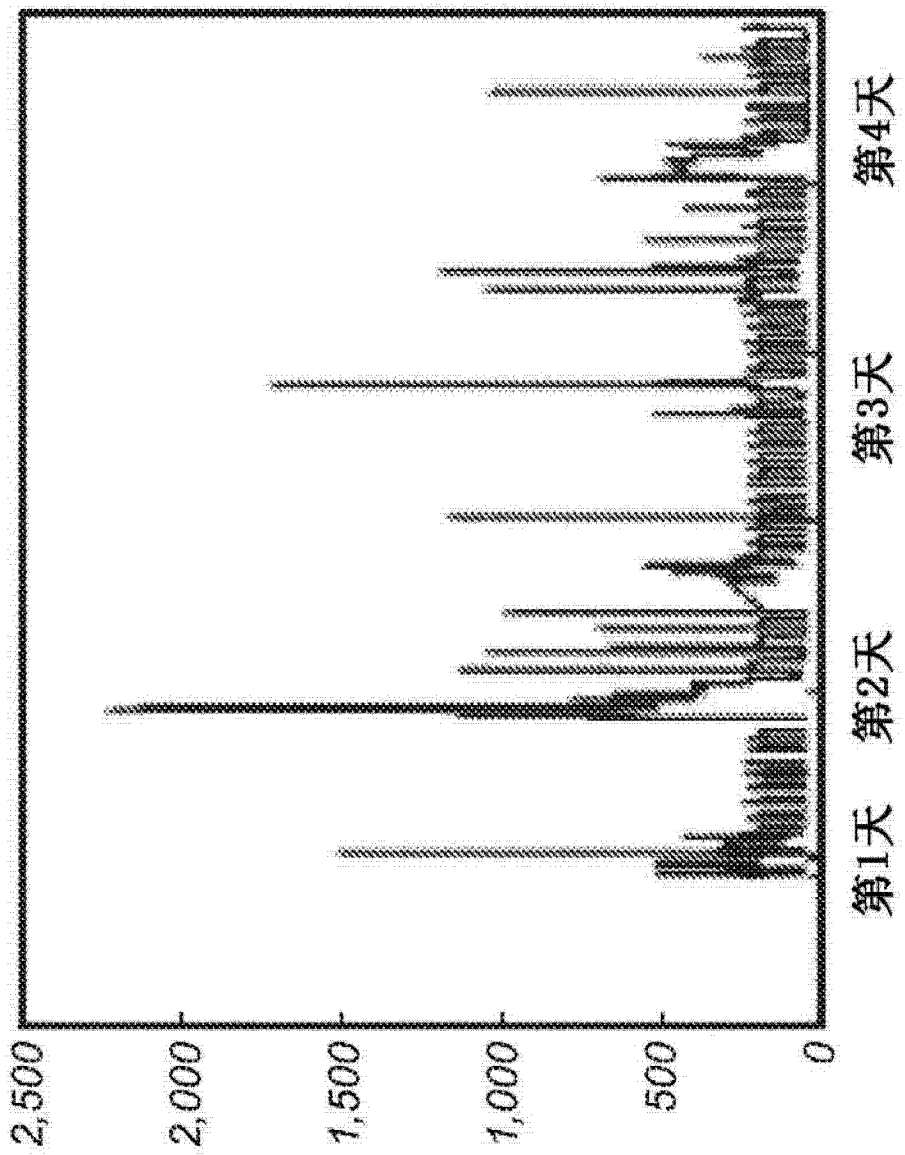


图 7(a)

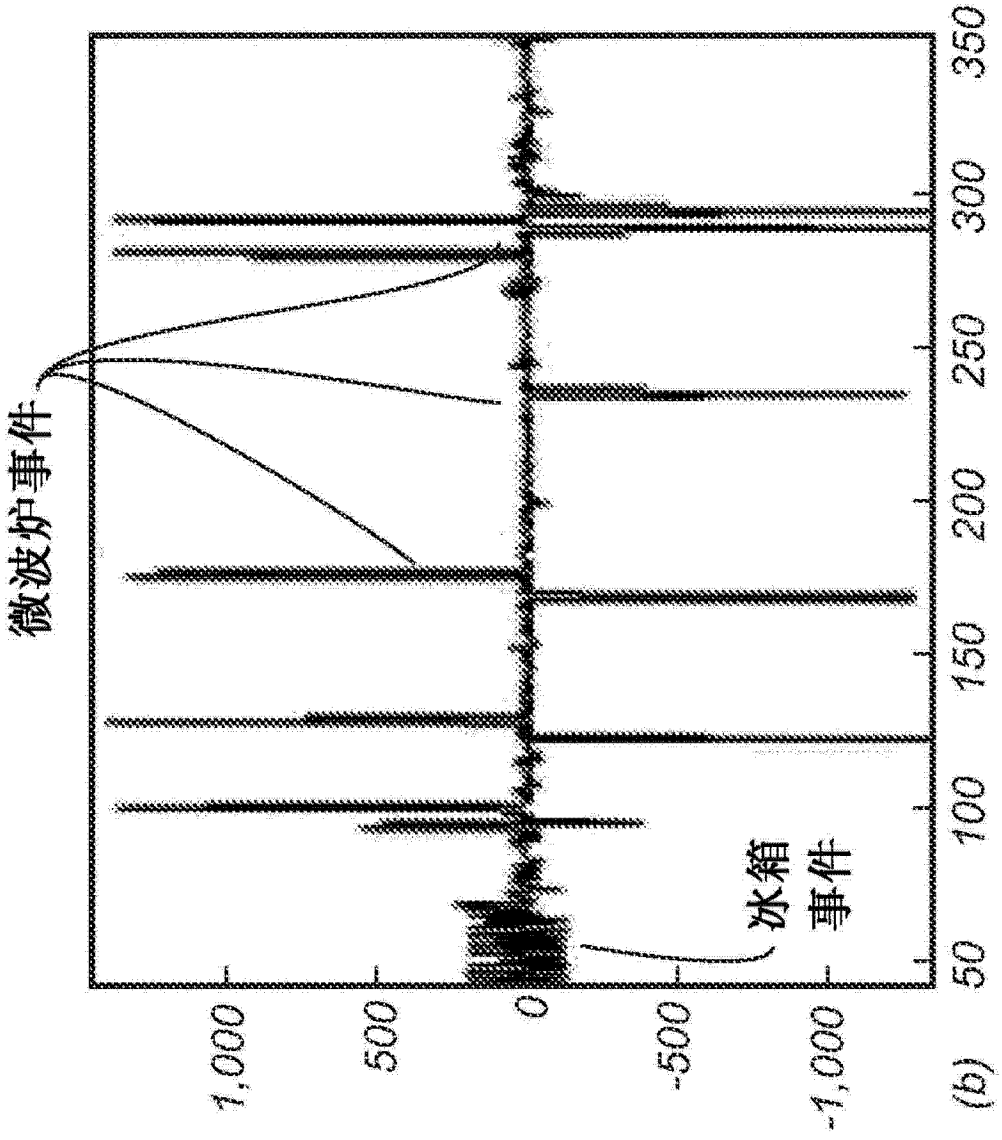


图 7(b)

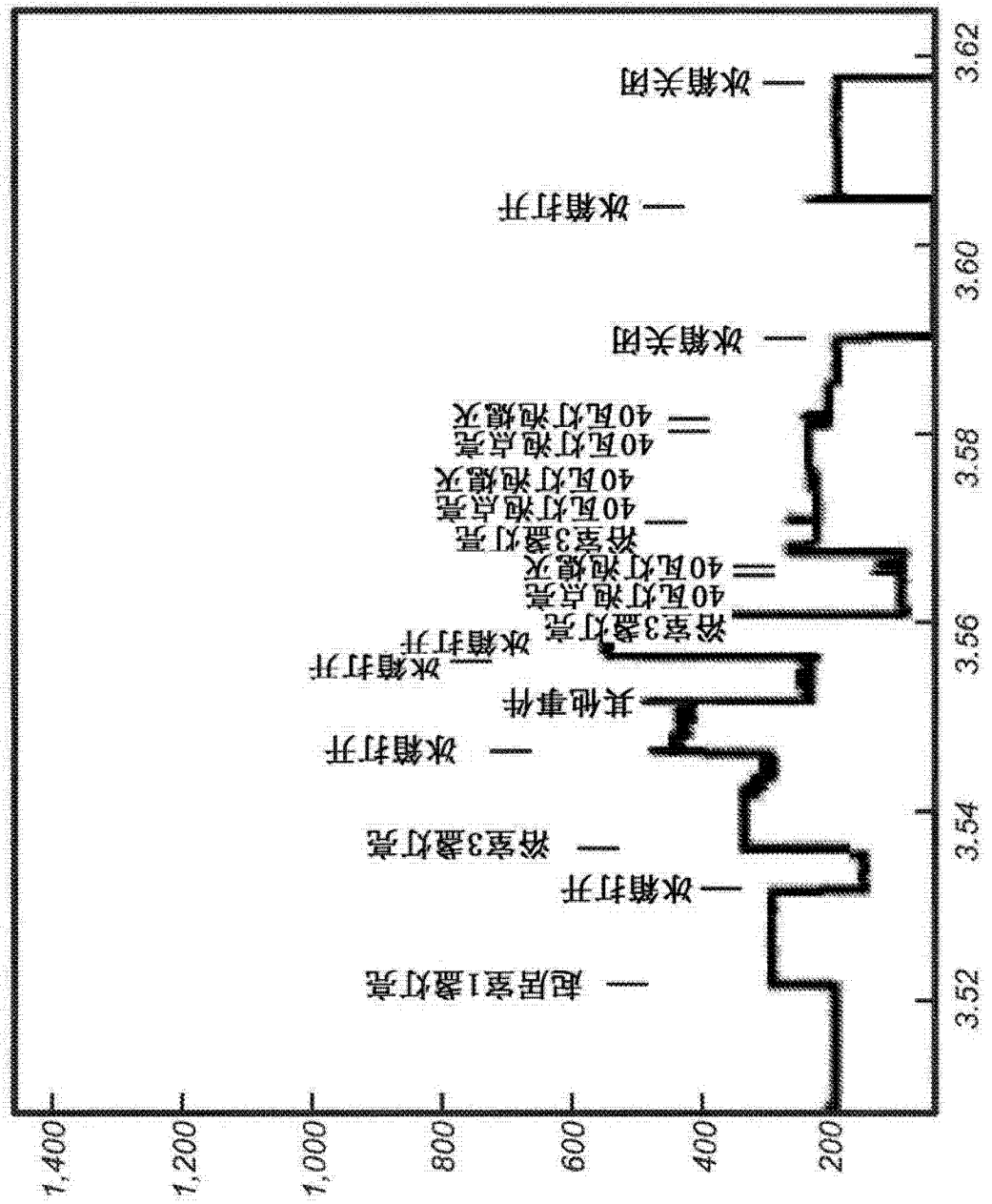

起居室1盏灯亮
冰箱打开
浴室3盏灯亮
冰箱打开
其他事件
冰箱打开
浴室3盏灯亮
冰箱打开
40瓦灯泡点亮
40瓦灯泡熄灭
浴室3盏灯亮
40瓦灯泡点亮
40瓦灯泡熄灭
40瓦灯泡点亮
40瓦灯泡熄灭
冰箱关闭
冰箱打开
冰箱关闭
1,400
1,200
1,000
800
600
400
200
3.52
3.54
3.56
3.58
3.60
3.62

图 7(c)

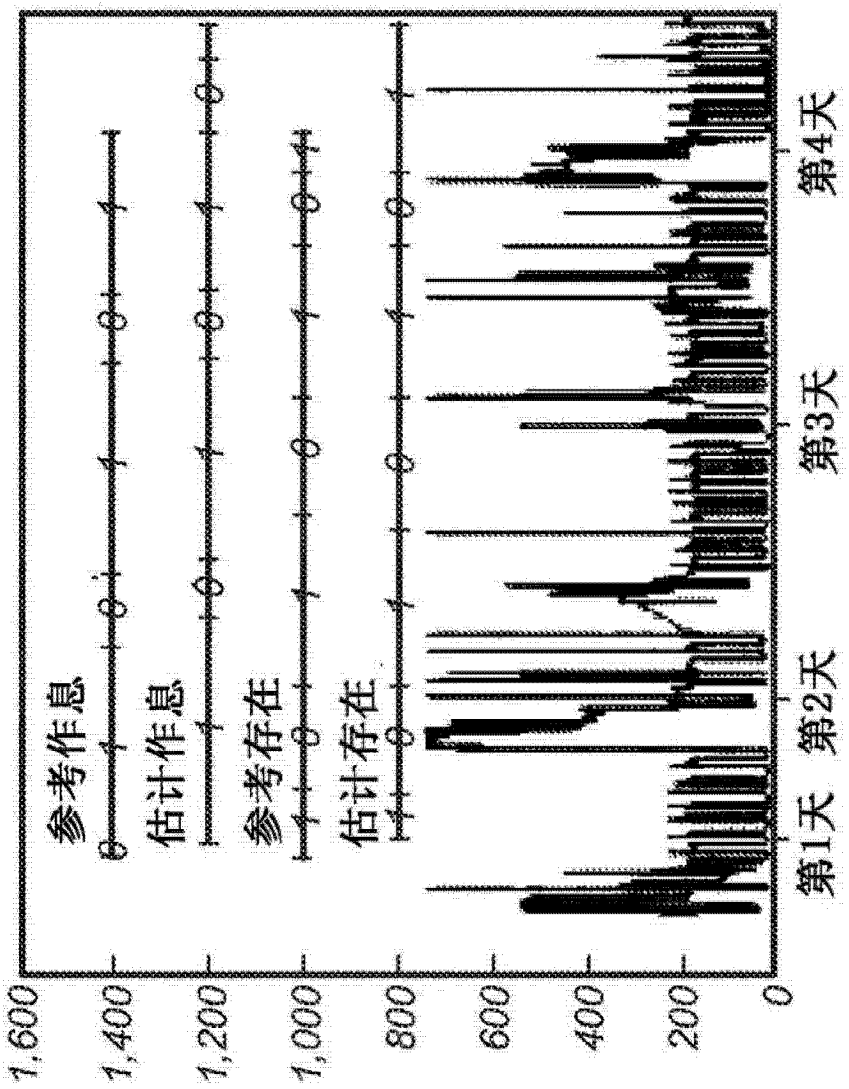

参考作息
估计作息
参考存在
估计存在
1,600
1,400
1,200
1,000
800
600
400
200
0
第1天
第2天
第3天
第4天

图 7(d)

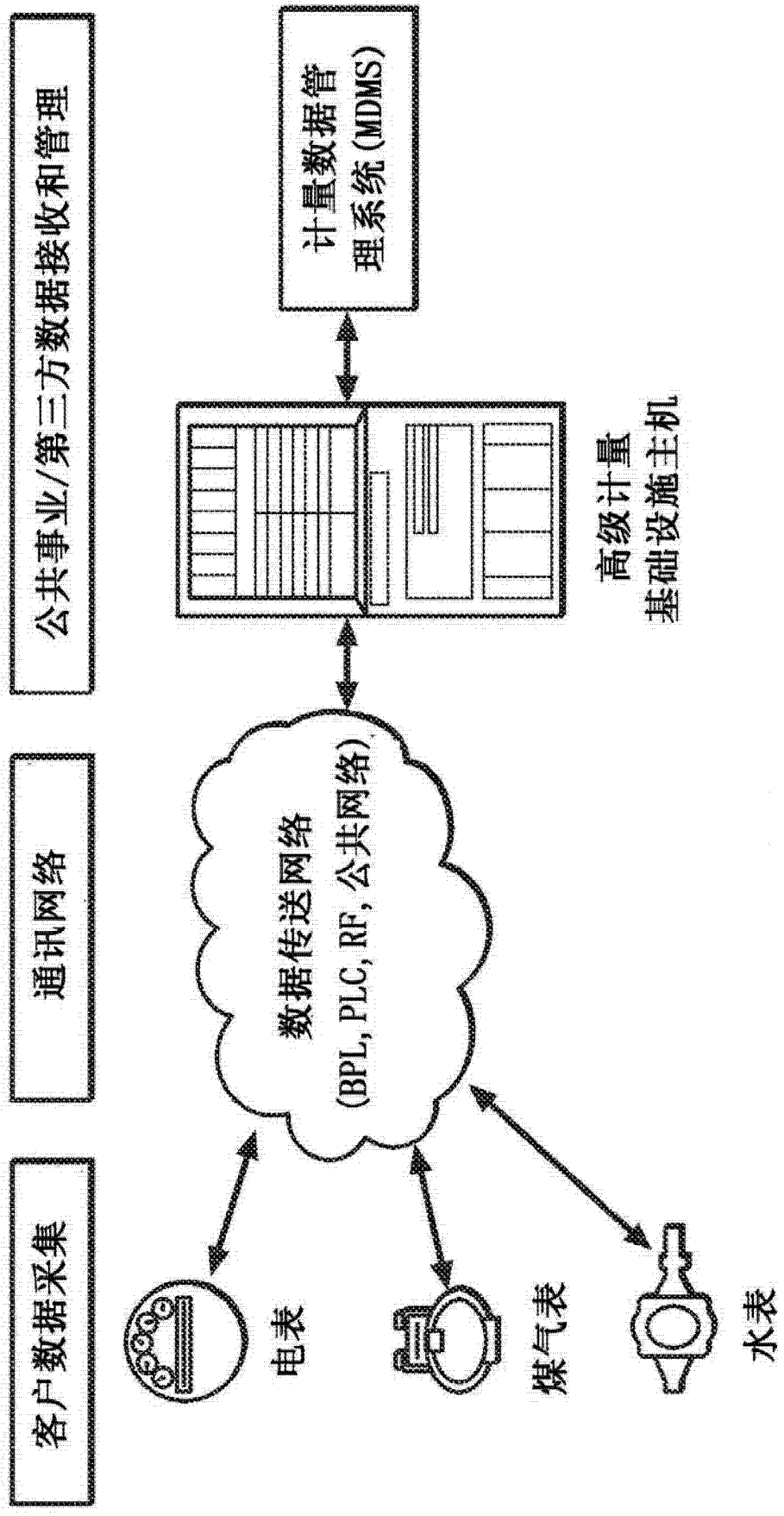

客户数据采集
通讯网络
公共事业/第三方数据接收和管理
计量数据管理系统(MDMS)
高级计量基础设施主机
数据传送网络
(BPL, PLC, RF, 公共网络)
电表
煤气表
水表

图 8

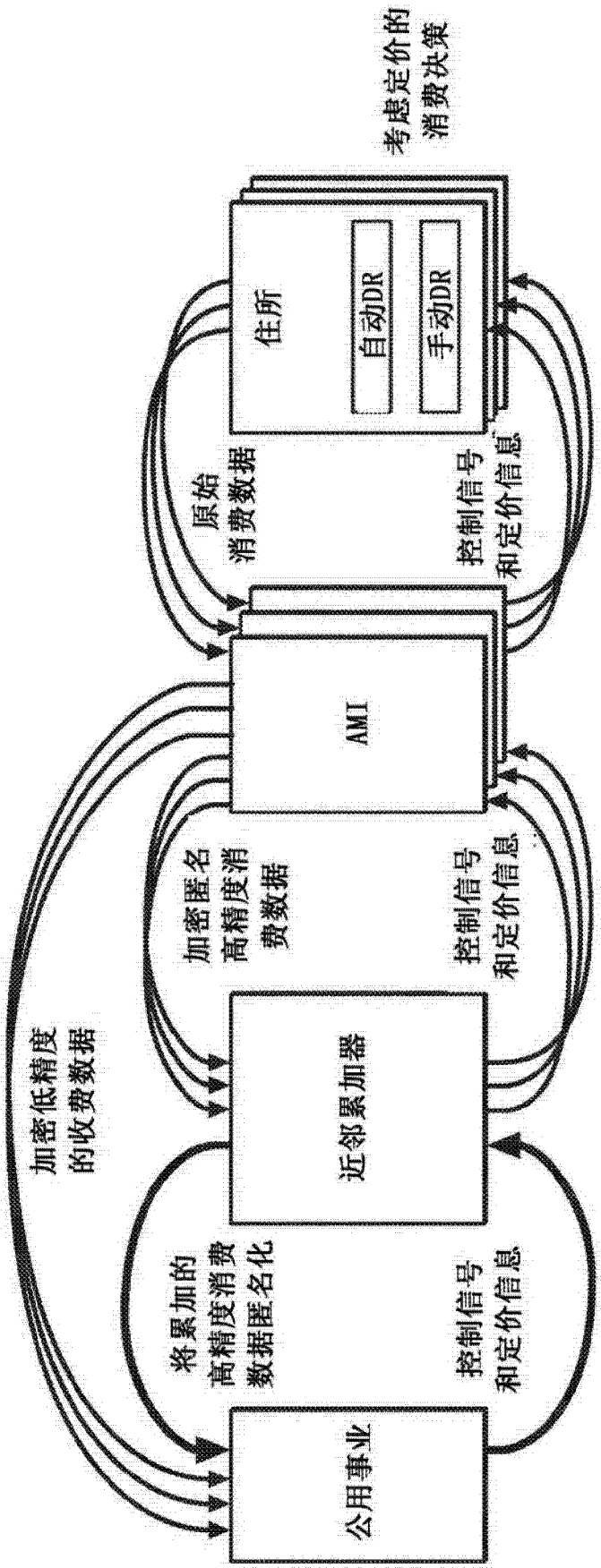

考虑定价的
消费决策
住所
自动DR
手动DR
原始
消费数据
控制信号
和定价信息
AMI
加密匿名
高精度消
费数据
控制信号
和定价信息
加密低精度
的收费数据
近邻累加器
将累加的
高精度消费
数据匿名化
控制信号
和定价信息
公用事业

图 9