(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 105474603 B
(45)授权公告日 2018.12.14

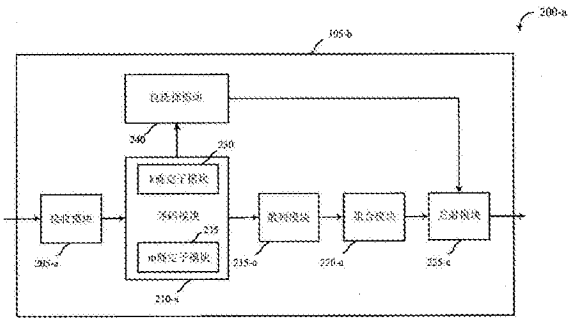
(21)申请号 201480045972.0
(22)申请日 2014.08.11
(65)同一申请的已公布的文献号
申请公布号 CN 105474603 A
(43)申请公布日 2016.04.06
(30)优先权数据
61/869,429 2013.08.23 US
14/148,342 2014.01.06 US
(85)PCT国际申请进入国家阶段日
2016.02.19
(86)PCT国际申请的申请数据
PCT/US2014/050521 2014.08.11
(87)PCT国际申请的公布数据
WO2015/026551 EN 2015.02.26
(73)专利权人 高通股份有限公司
地址 美国加利福尼亚州
(72)发明人 朱班·乔斯 吴新宙
托马斯·J·理查德森
(74)专利代理机构 北京律盟知识产权代理有限责任公司 11287
代理人 宋献涛
(51)Int.Cl.
H04L 9/32(2006.01)
H04L 29/06(2006.01)
H04L 29/08(2006.01)
H04W 4/80(2018.01)
H04W 4/40(2018.01)
H04W 4/46(2018.01)
(56)对比文件
US 2010251067 A1,2010.09.30,
WO 02/101971 A2,2002.12.19,
US 2006235895 A1,2006.10.19,
US 2001053226 A1,2001.12.20,
US 2008235510 A1,2008.09.25,
审查员 陈玲珑
权利要求书4页 说明书14页 附图15页

(54)发明名称

使用预译码包的散列的安全内容传递

(57)摘要

本发明描述用于确保经由通信网络传递的内容安全的方法、系统和装置。所述方法、系统和装置可涉及使用所确定的代码对多个包译码以产生包的译码集(605)。可对包的所述译码集中的多个包进行散列处理以产生多个散列(610)。可经由所述通信网络发射所述多个散列以传递所述安全内容。



CN 105474603 B

1.一种针对无线通信的安全内容分配的方法,其包括:

识别包括待传递内容的多个包;

使用所确定的代码对所述多个包译码以产生包的译码集;

对包的所述译码集中的多个包进行散列处理以产生多个散列;

经由通信网络发射所述多个散列;以及

在发射所述多个散列之后,发射包的所述译码集中的每个包,其中发射包的所述译码集中的每个包包括:

选择包的所述译码集中的至少一个包;

独立于发射所述多个散列,经无线通信网络广播至少一个选定包;以及

重复选择和广播直到包的所述译码集中的每个包被广播。

2.根据权利要求1所述的方法,其中发射所述多个散列包括:

将所述多个散列组合成散列的至少一个包;

以下各者中的至少一者:

使用电子签名对散列的所述至少一个包进行签名,

加密散列的所述至少一个包;以及

经由所述通信网络发射散列的所述至少一个包。

3.根据权利要求1所述的方法,其中选择包的所述译码集中的至少一个包包括:

随机选择包的所述译码集中的至少一个包。

4.根据权利要求1所述的方法,其中使用所确定的代码对所述多个包译码以产生包的译码集包括:

确定在所述多个包中的包的数目(k);以及

使用所述所确定的代码对所述k个包译码以产生包的所述译码集中的包的数目(m),m大于k。

5.根据权利要求4所述的方法,其进一步包括:

确定在包的所述译码集中的包的所述数目(m)以使得具有至少k个包的包的所述译码集的子集足以恢复在所述多个包中的所述k个包。

6.根据权利要求4所述的方法,其进一步包括:

经由所述通信网络发射k、m和所述所确定的代码。

7.根据权利要求4所述的方法,其进一步包括:

至少部分地基于与经由所述通信网络发射所述多个散列相关联的开销,确定在包的所述译码集中的包的所述数目(m)。

8.根据权利要求4所述的方法,其进一步包括:

随机地选择包的所述译码集中的至少一个包;以及

至少部分地基于与所述至少一个所随机选择的包经所述无线通信网络的所述广播相关联的开销,确定在包的所述译码集中的包的所述数目(m)。

9.根据权利要求1所述的方法,其中经由所述通信网络发射所述多个散列包括:

以无线方式发射所述多个散列。

10.根据权利要求1所述的方法,其中经由所述通信网络发射所述多个散列包括:

经由有线回程进行发射。

11.根据权利要求1所述的方法，其中经由所述通信网络发射所述多个散列包括经由专用短程通信DSRC网络发射所述多个散列。

12.根据权利要求1所述的方法，进一步包括：获取由认证机构创建的证书撤销列表，所述证书撤销列表包括待译码的所述多个包。

13.根据权利要求1所述的方法，进一步包括：在发射所述多个散列之前，执行以下各者中的至少一者：使用电子签名对所述多个散列进行签名，以及加密所述多个散列。

14.一种用于针对无线通信的安全内容分配的设备，其包括：

用于识别包括待传递内容的多个包的装置；

用于使用所确定的代码对所述多个包译码以产生包的译码集的装置；

用于对包的所述译码集中的多个包进行散列处理以产生多个散列的装置；

用于经由通信网络发射所述多个散列的装置；以及

用于在发射所述多个散列之后发射包的所述译码集中的每个包的装置，其中用于发射包的所述译码集中的每个包的装置包括：

用于选择包的所述译码集中的至少一个包的装置；

用于独立于发射所述多个散列经无线通信网络广播至少一个选定包的装置；以及

用于重复选择和广播直到包的所述译码集中的每个包被广播的装置。

15.根据权利要求14所述的设备，其中用于发射所述多个散列的装置包括：

用于将所述多个散列组合成散列的至少一个包的装置；

以下各者中的至少一者：

用于使用电子签名对散列的所述至少一个包进行签名的装置，

用于加密散列的所述至少一个包的装置，以及

用于经由所述通信网络发射散列的所述至少一个包的装置。

16.根据权利要求14所述的设备，其中所述用于选择包的所述译码集中的至少一个包的装置包括用于随机地选择包的所述译码集中的至少一个包的装置。

17.根据权利要求14所述的设备，其中所述用于使用所确定的代码对所述多个包译码以产生包的译码集的装置包括：

用于确定在所述多个包中的包的数目(k)的装置；以及

用于使用所述所确定的代码对所述k个包译码以产生包的所述译码集中的包的数目(m)的装置，m大于k。

18.根据权利要求17所述的设备，其中所述用于译码的装置包括：

用于确定在包的所述译码集中的包的所述数目(m)以使得具有至少k个包的包的所述译码集的子集足以恢复在所述多个包中的所述k个包的装置。

19.根据权利要求17所述的设备，其进一步包括：

用于经由所述通信网络发射k、m和所述所确定的代码的装置。

20.根据权利要求17所述的设备，其中所述用于译码的装置包括：

用于至少部分地基于与经由所述通信网络发射所述多个散列相关联的开销，确定在包的所述译码集中的包的所述数目(m)。

21.根据权利要求17所述的设备，其进一步包括：

用于随机地选择包的所述译码集中的至少一个包的装置，

其中所述用于译码的装置包括用于至少部分地基于与所述至少一个所随机选择的包经所述无线通信网络的所述广播相关联的开销，确定在包的所述译码集中的包的所述数目(m)的装置。

22.根据权利要求14所述的设备，其中所述用于经由所述通信网络发射所述多个散列的装置包括用于经由专用短程通信DSRC网络发射所述多个散列的装置。

23.根据权利要求14所述的设备，进一步包括：用于获取由认证机构创建的证书撤销列表的装置，所述证书撤销列表包括待译码的所述多个包。

24.根据权利要求14所述的设备，进一步包括以下各者中的至少一者：用于在发射所述多个散列之前使用电子签名对所述多个散列进行签名的装置，以及用于在发射所述多个散列之前加密所述多个散列的装置。

25.一种经配置以用于无线通信的安全内容分配的装置，其包括：

处理器；

与所述处理器电子通信的存储器；以及

存储于所述存储器中的指令，所述指令可由所述处理器执行以：

识别包括待传递内容的多个包；

使用所确定的代码对多个包译码以产生包的译码集；

对包的所述译码集中的多个包进行散列处理以产生多个散列；

经由通信网络发射所述多个散列；以及

在发射所述多个散列之后，发射包的所述译码集中的每个包，其中发射包的所述译码集中的每个包包括：

选择包的所述译码集中的至少一个包；

独立于发射所述多个散列，经无线通信网络广播至少一个选定包；以及

重复选择和广播直到包的所述译码集中的每个包被广播。

26.一种用于无线通信的安全内容分配的方法，其包括：

接收对应于来自第一装置的待传递内容的包的译码集的多个散列，

独立于接收所述多个散列，经由广播传送来接收待传递内容的包的所述译码集的包；

至少部分基于所接收到的多个散列验证所接收的包；

在至少部分基于所接收到的多个散列验证所述所接收的包之后，解码所述所接收的包；以及

重复接收包的所述译码集的包、验证所接收的包、以及解码所述所接收的包，直到待传递内容被解码。

27.根据权利要求26所述的方法，其中包的所述译码集的所述包是从不同于所述第一装置的第二装置接收的。

28.根据权利要求26所述的方法，进一步包括：

接收与所述多个散列相关联的电子签名；

至少部分地基于所接收到的电子签名，验证所述所接收到的多个散列；以及

转发具有所述所接收到的电子签名的多个散列到另一装置。

29.根据权利要求28所述的方法，其中所述转发具有所述所接收到的电子签名的经验证的多个散列包括：

转发对包的所述译码集译码的代码、经译码以产生包的数目(m)的多个包中的包的数目(k),以及包的所述数目(m)。

30.根据权利要求28所述的方法,其中所述经验证的多个散列与所述所接收到的电子签名经由专用短程通信DSRC网络被转发。

使用预译码包的散列的安全内容传递

[0001] 交叉参考

[0002] 本申请案主张来自共同待决的2014年1月6日申请的标题为“使用预译码包的散列的安全内容传递(Secure Content Delivery Using Hashing of Pre-coded Packets)”的第14/148,342号美国专利申请案;以及2013年8月23日申请的标题为“使用预译码包的散列的安全内容传递(Secure Content Delivery Using Hashing of Pre-coded Packets)”的第61/869,429号美国临时专利申请案的优先权;所述申请案中的每一个皆转让给本受让人。

背景技术

[0003] 以下大体上涉及通信,且更具体地说,涉及经由通信网络提供安全内容传递。广泛部署通信系统以提供各种类型的通信内容,例如话音、视频、包数据、消息传递、广播等。这些系统可为能够通过共享可用系统资源(例如,时间、频率和功率)而支持与多个用户的通信的多址系统。无线多址系统的实例包含码分多址(CDMA)系统、时分多址(TDMA)系统、频分多址(FDMA)系统和正交频分多址(OFDMA)系统。

[0004] 如本文所描述的,专用短距离通信(DSRC)网络可要求向使用DSRC网络的全部车辆进行安全内容传递,(例如)用于分配由认证机构产生的证书撤销列表(CRL)。CRL提供撤销证书的列表以使得车辆可识别出不被信任的接收到的通信。CRL的分发应是安全的,以使得使用DSRC网络的车辆不会转发恶意或不正确包。

发明内容

[0005] 所描述的特征大体上涉及用于确保经由通信网络传递的内容安全的一或多个改进的系统、方法和/或设备。确切地说,所描述的特征涉及经由专用短距离通信(DSRC)网络的安全内容传递。

[0006] 描述确保经由通信网络传递的内容安全的方法。在一个配置中,方法可涉及使用所确定的代码对多个包译码以产生包的译码集,并对包的译码集中的多个包进行散列处理以产生多个散列。

[0007] 在一些实施例中,方法可涉及选择包的译码集中的至少一个包。在此些实施例中,可经无线通信网络广播至少一个选定包。此外,可独立于选定包的广播而发射至少一个经签名和/或经加密的包。在一些实施例中,可随机选择包的译码集中的至少一个包。

[0008] 在一些实施例中,多个包的译码可涉及确定在多个包中的包的数目(k),以及使用所确定的代码对k个包译码以产生在包的译码集中的包的数目(m),其中m大于k。在此些实施例中,可确定在包的译码集中的包的数目(m)以使得具有至少k个包的包的译码集的子集足以恢复在多个包中的k个包。或者或另外,可至少部分地基于与经由通信网络发射多个散列相关联的开销,确定在包的译码集中的包的数目(m)。

[0009] 在一些实施例中,方法可涉及经由通信网络发射多个散列,以及经由所述通信网络发射k、m和所确定的代码。

[0010] 在一些实施例中，方法可涉及随机选择包的译码集中的至少一个包。可经无线通信网络广播至少一个选定包。在此些实施例中，可至少部分地基于与至少一个所随机选择的包经无线通信网络的广播相关联的开销，确定在包的译码集中的包的数目(m)。

[0011] 在一些实施例中，可经由通信网络发射多个散列。在此些实施例中，可无线地发射多个散列。或者或另外，可经由有线回程发射多个散列。

[0012] 在一些实施例中，方法可涉及将多个散列组合成至少一个包。在此些实施例中，可使用电子签名对所述至少一个包进行签名。或者或另外，可加密所述至少一个包。此外，在此些实施例中，方法可涉及经由通信网络发射所述至少一个包。

[0013] 描述用于确保经由通信网络传递的内容安全的设备。在一个配置中，所述设备可包含用于使用所确定的代码对多个包译码以产生包的译码集的装置，以及用于对包的译码集中的多个包进行散列处理以产生多个散列的装置。

[0014] 描述经配置以确保经由通信网络传递的内容安全的装置。在一个配置中，装置可包含处理器和与所述处理器电子通信的存储器。指令可存储于所述存储器中。所述指令可由所述处理器执行以：使用所确定的代码对多个包译码以产生包的译码集；以及对包的译码集中的多个包进行散列处理以产生多个散列。

[0015] 描述用于确保经由通信网络传递的内容安全的计算机程序产品。计算机程序产品可为存储指令的非暂时性计算机可读存储媒体。所述指令可由处理器执行，以使用所确定的代码对多个包译码来产生包的译码集，以及对包的译码集中的多个包进行散列处理来产生多个散列。

[0016] 也描述经由通信网络的安全内容传递的方法。在一个配置中，方法可涉及经由无线通信网络接收对应于包的译码集的多个散列，以及接收与多个散列相关联的电子签名。随后，可至少部分地基于接收到的电子签名来验证接收到的多个散列。

[0017] 描述经由无线通信网络的安全内容传递的另一方法。在一个配置中，方法可涉及经由通信网络接收对应于包的译码集的多个散列，以及经由所述通信网络接收包的译码集中的包。随后，可对接收到的包进行散列处理以产生接收到的包的散列。之后，可比较接收到的包的散列与接收到的多个散列中的对应散列，以验证接收到的包。

[0018] 描述经由通信网络的安全内容传递的又一方法。在一个配置中，方法可涉及经由通信网络接收对应于包的译码集的多个散列，其中对多个散列进行加密。随后，至少部分地基于所述加密，验证接收到的多个散列。

[0019] 描述用于经由通信网络的安全内容传递的设备。设备可包含用于经由通信网络接收对应于包的译码集的多个散列的装置、用于接收与多个散列相关联的电子签名的装置，以及用于至少部分地基于接收到的电子签名来验证接收到的多个散列的装置。

[0020] 描述用于经由通信网络的安全内容传递的装置。装置可包含处理器、与所述处理器电子通信的存储器和存储在所述存储器中的指令。指令可由处理器执行，以经由通信网络接收对应于包的译码集的多个散列，接收与多个散列相关联的电子签名，以及至少部分地基于接收到的电子签名，验证接收到的多个散列。

[0021] 描述用于经由通信网络的安全内容传递的计算机程序产品。计算机程序产品可为存储指令的非暂时性计算机可读存储媒体。指令可由处理器执行，以经由无线通信网络接收对应于包的译码集的多个散列，接收与多个散列相关联的电子签名，以及至少部分地基

于接收到的电子签名，验证接收到的多个散列。

[0022] 描述用于经由通信网络的安全内容传递的另一设备。设备可包含用于经由通信网络接收对应于包的译码集的多个散列的装置、用于经由所述通信网络接收包的译码集中的包的装置、用于对接收到的包进行散列处理以产生接收到的包的散列的装置，以及用于比较接收到的包的散列与接收到的多个散列中的对应散列以验证接收到的包的装置。

[0023] 描述用于经由通信网络的安全内容传递的另一装置。装置可包含处理器、与所述处理器电子通信的存储器和存储在所述存储器中的指令。指令可由所述处理器执行，以经由通信网络接收对应于包的译码集的多个散列，经由所述通信网络接收包的译码集中的包，对接收到的包进行散列处理以产生接收到的包的散列，以及比较接收到的包的散列与接收到的多个散列中的对应散列以验证接收到的包。

[0024] 描述用于经由通信网络的安全内容传递的另一计算机程序产品。计算机程序产品可为存储指令的非暂时性计算机可读存储媒体。指令可由处理器执行，以经由通信网络接收对应于包的译码集的多个散列，经由所述通信网络接收包的译码集中的包，对接收到的包进行散列处理以产生接收到的包的散列，以及比较接收到的包的散列与接收到的多个散列中的对应散列以验证接收到的包。

[0025] 描述用于经由通信网络的安全内容传递的另一设备。设备可包含用于经由通信网络接收对应于包的译码集的多个散列的装置。可对多个散列进行加密。设备可进一步包含用于至少部分地基于加密，验证接收到的多个散列的装置。

[0026] 描述用于经由通信网络的安全内容传递的另一装置。装置可包含处理器、与所述处理器电子通信的存储器和存储在所述存储器中的指令。指令可由所述处理器执行，以经由通信网络接收对应于包的译码集的多个散列。可对多个散列进行加密。指令可进一步由所述处理器执行，以至少部分地基于所述加密，验证接收到的多个散列。

[0027] 描述用于经由通信网络的安全内容传递的另一计算机程序产品。计算机程序产品可为存储指令的非暂时性计算机可读存储媒体。指令可由处理器执行，以经由通信网络接收对应于包的译码集的多个散列。可对多个散列进行加密。指令可进一步由处理器执行，以至少部分地基于所述加密，验证接收到的多个散列。

[0028] 所描述的方法和设备的适用性的进一步范围将从以下详细描述、权利要求书和图式中变得显而易见。由于本说明书的精神和范围内的各种改变和修改对所属领域的技术人员将变得显而易见，所以仅借助于说明给出详细描述和具体实例。

附图说明

[0029] 本发明的本质和优势的进一步理解可参照以下图式实现。在附图中，类似的组件或特征可具有相同的参考标记。此外，可通过在参考标记之后接有在类似组件之间进行区分的破折号和第二标记来区分为相同类型的各种组件。如果本说明书中只使用第一参考标记，那么描述适用于具有相同的第一参考标记的类似组件中的任一者，而与第二参考标签无关。

[0030] 图1展示无线通信系统的框图；

[0031] 图2A展示基站的实例的框图；

[0032] 图2B展示基站的另一实例的框图；

[0033] 图3展示基站的又一实例的框图；

[0034] 图4A展示用户设备(UE)的实例的框图；

[0035] 图4B展示UE的另一实例的框图；

[0036] 图5展示UE的又一实例的框图；

[0037] 图6为在源处实施的确保传递的内容安全的方法的流程图；

[0038] 图7为在源处实施的确保传递的内容安全的另一方法的流程图；

[0039] 图8为在源处实施的安全内容传递的方法的流程图；

[0040] 图9为在UE处实施的安全内容传递的方法的流程图；

[0041] 图10为在UE处实施的安全内容传递的另一方法的流程图；

[0042] 图11为在UE处实施的安全内容传递的又一方法的流程图；

[0043] 图12为在UE处实施的安全内容传递的再一方法的流程图；以及

[0044] 图13为在UE处实施的安全内容传递的方法的最终实例的流程图。

具体实施方式

[0045] 关于专用短距离通信(DSRC)网络作出以下描述。但是应理解，所描述的特征还可大体上适用于其它通信网络，无论其是无线通信网络、有线通信网络或是其组合。尤其是在DSRC网络的情况下，安全内容传递对避免在DSRC网络中的车辆接收和转发恶意和/或不正确信息包来说至关重要。所述车辆中的每一个可更一般地理解为用户设备(UE)。

[0046] DSRC网络的特定目标是证书撤销列表(CRL)的分配。CRL的分配应是安全的以使得在DSRC网络中的车辆可准确地知道哪些信息发送器是无法信任的。因而，描述用于提供安全内容传递的各种技术。在分发CRL的源处，例如在蜂窝式基站或在DSRC网络的路边基站处，一般技术可能是译码和散列。

[0047] 在此方法中，可使用所确定的代码对多个包(在此实例中包括CRL)译码以产生包的译码集。随后，可对包的译码集中的多个包进行散列处理以产生多个散列。以这种方式，可确保用于经由DSRC网络的传递的内容(例如，CRL)的安全。随后，可经由所述网络发射多个散列。为提供额外的安全性，可将多个散列组合成至少一个包，并随后使用电子签名对其进行签名或加密。接收至少一个包的车辆可根据具体情况使用所述电子签名或所述加密来验证包。因为源处使用的代码可能由车辆已知，所以所述车辆可将经验证的包转发到在所述网络中的另一车辆，以及对经验证的包进行解码和转发。

[0048] 另外，所述源可从包的译码集中随机选择包，并随后广播选定包。所述源可继续视需要或以其它所要的方式随机选择和广播包。随后，已经接收所译码和进行散列处理的包的任何车辆可接收所选择和广播的包，然后通过以下操作验证接收到的包：对接收到的包进行散列处理以产生散列，以及比较所产生的散列与先前接收到的散列中的对应散列。

[0049] 以下描述提供实例，且并不限于权利要求书中阐述的范围、适用性或配置。可在不脱离本发明的精神和范围的情况下对元件的功能和布置作出改变。各种实施例可在适当时省略、替换或添加各种程序或组件。举例来说，所描述的方法可以不同于所描述的顺序执行，并且各种步骤可添加、省略或加以组合。另外，相对于某些实施例描述的特征可在其它实施例中加以组合。

[0050] 首先参看图1，图式说明无线通信系统100的实例。系统100包含DSRC基站(例如，路

边基站)105和在DSRC频谱内(例如,在DSRC系统中)操作的DSRC装置(例如,车辆)115-a至115-d。系统100还可包含蜂窝式基站130,其可在U-NII频谱中(例如,在Wi-Fi通信系统中)操作。DSRC基站105中的一者或蜂窝式基站130都可用作所描述的各种实施例中的源。此外,DSRC装置115中的每一个可被称为用户设备(UE),且可被视为用于执行在本文中关于装置/UE所描述的各种功能的装置。

[0051] 可将DSRC装置115分散到整个无线通信系统100,并且每一个DSRC装置115可为静止的或移动的。DSRC装置115可为车辆、交通信号、轨道十字路口、基站、蜂窝式电话和个人数字助理(PDA),等等。DSRC装置115可能能够与DSRC基站105和其它DSRC装置115通信。每一个DSRC基站105可提供用于相应的DSRC地理涵盖区域110的通信涵盖范围。

[0052] FCC一开始分配DSRC频谱用于汽车用途(例如,智能运输系统)。DSRC通信的实例包含车辆的紧急警告、合作自适应巡航控制、合作碰撞警告、交叉口防撞、电子停车支付、车内发信和电子收费,等等。DSRC通信链路120可位于DSRC装置115和DSRC基站105之间或DSRC装置115和另一DSRC装置115之间。在一些情况下,DSRC装置115之间(例如所说明的在DSRC装置115-a和115-b之间)的DSRC通信链路120可出现在DSRC基站105的涵盖区域110外。在一些实施例中,DSRC基站105可经回程链路125彼此直接或间接地通信,回程链路125可为有线或无线通信链路。

[0053] 无线通信系统100也可支持多个载波(具有不同频率的波形信号)上的操作。多载波发射器可在所述多个载波上同时发射调制信号。例如,每一个DSRC通信链路120可为根据各种无线电技术调制的多载波信号。可在不同载波上发送每一个调制信号,且可运载控制信息(例如,参考信号、控制信道,等等)、开销、数据,等等。

[0054] 如上文所指出,DSRC基站105中的一者或蜂窝式基站130可用作源,且可被视为用于执行在本文中关于基站或源所描述的各种功能的装置。就蜂窝式基站130来说,站台130可经配置以用多个包形式从生成机构(generating authority)获取证书撤销列表(CRL)。随后,蜂窝式基站130可通过使用所确定的代码进行译码来处理多个包以产生译码包的集合。随后,站台130可对包的译码集进行散列处理以产生多个散列。此外,蜂窝式基站130可使用电子签名对多个散列进行签名,或可加密多个散列,或两者都可进行。随后,基站130可发射经签名和/或经加密的多个散列。

[0055] 蜂窝式基站130可在适当时或视需要(例如)经由WiFi发射到DSRC基站105中的一者和/或发射到DSRC装置115中的一者,例如DSRC装置115-a。在一些实施例中,限制从蜂窝式基站130到一个或若干接收方的发射可有助于避免与完全依赖于二级无线网络(例如蜂窝式)相关联的相对高的成本。这还可促进用于车辆的DSRC的较早部署。当DSRC装置115-a接收到此发射时,装置115-a可基于电子签名或加密或这两者来验证接收到的多个散列。一经证实,DSRC装置115-a就可将多个散列转发,或解码并转发到在范围内的DSRC装置115的一或多个,例如DSRC装置115-b和115-c。

[0056] 当DSRC基站105从蜂窝式基站130接收到经签名和/或经加密的多个散列的发射时,或当DSRC基站105用作源时,DSRC基站在其涵盖区域110内可将经签名和/或经加密的多个散列发射到DSRC装置115,例如DSRC装置115-d。DSRC基站还可在适当时或按需要将经签名和/或经加密的多个散列发射到另一DSRC基站,所述另一DSRC基站随后可进一步发射所述散列。

[0057] 当DSRC装置115-d接收到此发射时，装置115-d可基于电子签名或加密或这两者来验证接收到的多个散列。一经证实，DSRC装置115-d就可将多个散列转发，或解码并转发到在范围内的DSRC装置115中的一或多个。

[0058] 在任一情况下，从DSRC装置115转发到DSRC装置115可将经验证的多个散列有效地分配到整个DSRC网络。

[0059] 随后，为蜂窝式基站130或DSRC基站105的源可随机选择(例如)译码包的集合中的包，并广播选定包。在已接收经验证的(或已验证接收到的)多个散列的DSRC装置接收到所广播的包后，可验证所广播的包。例如，通过在接收到的散列上执行散列和比较所产生的散列与经验证的多个散列中的对应散列，可验证所广播的包。源可继续随机选择和广播，且DSRC装置可继续验证，以使得可在DSRC装置处接收、验证和解码CRL的包的整个译码集。因此，可将CRL安全和有效地分配到整个DSRC网络。

[0060] 图2A是说明DSRC基站105-a的实例的框图200，DSRC基站105-a可实行如关于图1所论述的本发明的各方面。如上文所论述，应理解，取决于特定的实施方案，图2A(和图2B及3)也可被视为说明蜂窝式基站的实例。DSRC基站105-a可包含经配置以从蜂窝式基站130或DSRC装置115接收通信的接收模块205。确切地说，接收模块205可经配置以用多个包形式从认证机构接收通信(以获取由所述机构产生的证书撤销列表)。因此，接收模块205或接收器可为用于接收的装置和/或用于获取的装置。

[0061] 装置105-a的组件可单独地或共同地由经调适以硬件形式执行适用功能中的一些或全部的一或多个专用集成电路(ASIC)来实施。或者，功能可通过一或多个其它处理单元(或核心)在一或多个集成电路上执行。在其它实施例中，可使用其它类型的集成电路(例如，结构化/平台ASIC、现场可编程门阵列(FPGA)和其它半定制的IC)，其可以所属领域中已知的任何方式编程。每一个单元的功能还可使用指令来完全或部分地实施，所述指令在存储器中体现，经格式化以通过一或多个一般或专用处理器来执行。

[0062] DSRC基站105-a可包含经配置以使用预定义代码对多个包译码以产生译码包的集合的译码模块210。另外，DSRC基站105-a可包含经配置以对包的译码集中的包进行散列处理以产生多个散列的散列模块215。随后，组合模块220可将散列任选地组合成一或多个包。接着，DSRC基站105-a的发射模块225可发射一或多个包。因此，译码模块210或译码器可为用于译码的装置，散列模块215或散列器可为用于进行散列处理的装置，以及发射模块225或发射器可为用于发射的装置。

[0063] 图2B为说明DSRC基站105-b的另一实例的框图200-a，DSRC基站105-b可实行如关于图1所论述的本发明的各方面。如在图2A的实例中，DSRC基站105-b可包含接收模块205-a、散列模块215-a、组合模块220-a和发射模块225-a。这些模块中的每一个可包含如上所述的类似功能性。

[0064] 装置105-b的组件可单独地或共同地由经调适以硬件形式执行适用功能中的一些或全部的一或多个专用集成电路(ASIC)来实施。或者，功能可通过一或多个其它处理单元(或核心)在一或多个集成电路上执行。在其它实施例中，可使用其它类型的集成电路(例如，结构化/平台ASIC、现场可编程门阵列(FPGA)和其它半定制的IC)，其可以所属领域中已知的任何方式编程。每一个单元的功能还可使用指令来完全或部分地实施，所述指令在存储器中体现，经格式化以通过一或多个一般或专用处理器来执行。

[0065] DSRC基站105-b还可包含译码模块210-a。在此实例中，译码模块210-a可包含k确定子模块230和m确定子模块235。k确定子模块230可经配置以确定由接收模块205-a接收的多个包中的包的数目(k)。m确定子模块235可经配置以确定多个包由译码模块210-a译码的包的数目(m)。因此，k确定子模块230或计数器可为用于确定k的装置，且m确定子模块235可为用于确定m的装置。

[0066] 在一些实施例中，可确定m大于所确定的k。在一些实施例中，可确定包的数目(m)以使得具有至少k个包的包的译码集中的子集足以恢复在多个包中的k个包。或者或另外，可至少部分地基于与经由网络发射多个散列相关联的开销，确定包的数目(m)。因此，m确定子模块235可包含经配置以进行此类确定的逻辑。

[0067] 发射模块225-a可进一步经配置以发射k、m和所确定的代码。这可(例如)通过在用于发射多个散列的一或多个包的标头中包含k、m和所确定的代码来实现。

[0068] 如图2B中所展示，DSRC基站105-b还可包含包选择模块240。此模块可经配置以选择将由发射模块225-a广播的译码包的集合中的包中的一者。在此情况下，m确定子模块235可至少部分地基于与所随机选择的包经网络的广播相关联的开销，确定在包的译码集中的包的数目(m)。包选择模块240可继续随机选择译码包的集合中的包，以使得包的译码集中的全部包最终由发射模块225-a发射至少一次(如果没有多次发射的话)。因此，包选择模块240或包选择器可为用于选择的装置。

[0069] 图3为说明DSRC基站105-c的又一实例的框图300，DSRC基站105-c可经配置以提供安全内容传递。DSRC基站105-c可为图1中所描绘的DSRC基站105或蜂窝式基站130的实例。DSRC基站105-c可包含一或多个天线305，天线305经配置以与一或多个收发器模块310合作来接收和发射无线信号。DSRC基站可进一步包含通信管理模块315、路边(DSRC)站台通信模块320(尤其是当DSRC基站105-c为蜂窝式基站130时)、处理器模块325、网络通信模块330和存储器335，其中的每一个可彼此(例如，经一或多个总线)直接或间接地通信。

[0070] 收发器模块310可经配置以在路边(DSRC)站台通信模块320的控制下，经由天线305与(其它)DSRC基站通信。另外，收发器模块310可经配置以在通信管理模块315的控制下，经由天线305与DSRC装置通信。此外，收发器模块310可经配置以在网络通信模块330的控制下，经由天线305与另一网络(例如，蜂窝式)通信(例如)以从生成机构接收CRL。因此，收发器模块310或收发器可为用于单独地或结合模块315、320和/或330，和/或天线来发射、广播和/或获取的装置。

[0071] 存储器335可包含随机存取存储器(RAM)和只读存储器(ROM)。存储器335还可存储含有指令的计算机可读、计算机可执行的软件代码340，所述指令经配置以在执行时使处理器模块325执行本文中所描述的各种功能(例如，译码、散列，等等)。或者，软件代码340可不由处理器模块325直接执行，但可经配置以(例如)当编译和执行时使计算机执行本文中所描述的功能。因此，处理器模块325或处理器可为用于单独地或结合存储器335和软件代码340来译码、散列、组合、签名和/或加密的装置。

[0072] 处理器模块325可包含智能硬件装置，例如中央处理单元(CPU)、微控制器、专用集成电路(ASIC)，等等。收发器模块310可包含调制解调器，其经配置以调制包和向天线305提供调制包以用于发射，以及解调从天线305接收到的包。

[0073] 尽管单独地展示了通信管理模块315，但通信管理模块315的功能性可实施为收发

器模块310的组件，实施为计算机程序产品，和/或实施为处理器模块325的一或多个控制器元件。类似地，路边(DSRC)站台通信模块320和网络通信模块330可实施为收发器模块310的组件，实施为计算机程序产品，和/或实施为处理器模块325的一或多个控制器元件。

[0074] 图4A为说明DSRC装置115-e的实例的框图400，DSRC装置115-e可实行如关于图1所论述的本发明的各方面。DSRC装置115-e可包含经配置以从蜂窝式基站130、DSRC基站105和/或另一DSRC装置115接收通信的接收模块405。因此，接收模块405或接收器可为用于接收的装置。

[0075] DSRC装置115-e的组件可单独地或共同地由经调适以硬件形式执行适用功能中的一些或全部的一或多个专用集成电路(ASIC)来实施。或者，功能可通过一或多个其它处理单元(或核心)在一或多个集成电路上执行。在其它实施例中，可使用其它类型的集成电路(例如，结构化/平台ASIC、现场可编程门阵列(FPGA)和其它半定制的IC)，其可以所属领域中已知的任何方式编程。每一个单元的功能还可使用指令来完全或部分地实施，所述指令在存储器中实施，经格式化以通过一或多个一般或专用处理器来执行。

[0076] DSRC装置115-e还可包含经配置以验证从源接收到的多个散列的验证模块410。如上文所论述，验证可涉及与多个散列一同接收的签名证书或电子签名，或多个散列的加密，或两者都涉及。验证模块410可通过执行以下两种功能验证多个散列：(1)校验证书或签名；以及(2)对随机包进行散列处理，并比较所获取的散列与多个散列中的对应散列(例如，通过匹配来验证)。验证模块410可经配置以将已验证多个散列传达给解码模块415，解码模块415经配置以使用预定义代码来解码译码包的集合。DSRC装置115-e可包含经配置以将包的解码集发射(例如，解码并转发)到另一DSRC装置115的发射模块225。或者或另外，发射模块225可经配置以将经验证的多个散列(其可能具有电子签名和/或加密)发射(例如，转发)到另一DSRC装置115。因此，验证模块410、证书/签名校验器或加密校验器可为用于验证的装置，解码模块415或解码器可为用于解码的装置。类似地，发射模块225或发射器可为用于发射的装置。

[0077] 接收模块405也可经配置以从源接收译码包的集合中所随机选择的包。验证模块410也可经配置以验证这些包。一经证实，这些包就可由解码模块415解码。DSRC装置115-e可进一步包含包装配模块425，其经配置以装配所随机接收到的解码包以获取原始的多个包(例如，证书撤销列表(CRL))。因此，包装配模块425或包装配器可为用于装配的装置。

[0078] 图4B为说明DSRC装置115-f的另一实例的框图400-a，所述DSRC装置115-f可实行如关于图1所论述的本发明的各方面。如在图4A的实例中，DSRC装置115-f可包含接收模块405-a、解码模块415-a、包装配模块425-a和发射模块420-a。这些模块中的每一个可包含如上所述的类似功能性。

[0079] 装置115-f的组件可单独地或共同地由经调适以硬件形式执行适用功能中的一些或全部的一或多个专用集成电路(ASIC)来实施。或者，功能可通过一或多个其它处理单元(或核心)在一或多个集成电路上执行。在其它实施例中，可使用其它类型的集成电路(例如，结构化/平台ASIC、现场可编程门阵列(FPGA)和其它半定制的IC)，其可以所属领域中已知的任何方式编程。每一个单元的功能还可使用指令来完全或部分地实施，所述指令在存储器中实施，经格式化以通过一或多个一般或专用处理器来执行。

[0080] DSRC装置115-f还可包含验证模块410-a。在此实例中，验证模块410-a可包含电子

签名验证子模块430、加密验证子模块435和散列验证模块440。这些子模块可经配置以实行上文中关于图4A所描述的功能，从而分别基于随机包的电子签名、加密和散列来验证多个散列。因此，电子签名验证子模块430或签名验证器、加密验证子模块435或加密验证器和散列验证子模块440或散列验证器可为分别用于验证电子签名、加密和散列的装置。

[0081] 散列验证模块440可经配置以实行上文中关于图4A所描述的功能，从而验证从源接收到的译码包的集合中的所随机选择的包。更确切地说，散列验证模块440可包含散列子模块445和比较子模块450。散列子模块445可经配置以对从源接收到的译码包的集合中的所随机选择的包进行散列处理以产生用于每一个包的散列。比较子模块450可经配置以比较所产生的散列与先前接收到的多个散列中的对应散列。例如，针对给定包的两种散列之间的匹配可验证所述包。因此，散列子模块或散列器和比较子模块450或比较器可分别为用于进行散列处理和比较的装置。如上，一旦包被证实，那么所述包就可由解码模块415-a解码，并可由包装配模块425-a装配以获取原始的多个包(例如，证书撤销列表(CRL))。

[0082] 图5为说明DSRC装置115-g的又一实例的框图500，DSRC装置115-g可经配置以提供安全内容传递。DSRC装置115-g可为图1中所描绘的DSRC装置115的实例。DSRC装置115-g可包含一或多个天线505，其经配置以与一或多个收发器模块510合作来接收和发射无线信号。DSRC装置可进一步包含蜂窝式通信管理模块515、DSRC通信管理模块520、处理器模块525和存储器530，其中的每一个可彼此(例如，经一或多个总线)直接或间接地通信。

[0083] 收发器模块510可经配置以在DSRC通信管理模块520的控制下，经由天线505与其它DSRC装置115和DSRC基站105通信。另外，收发器模块510可经配置以在蜂窝式通信管理模块515的控制下，经由天线505与其它蜂窝式基站130通信。因此，收发器模块510或收发器可为用于单独地或结合模块515和/或520和/或天线来发射、广播和/或获取的装置。

[0084] 存储器530可包含随机存取存储器(RAM)和只读存储器(ROM)。存储器530还可存储含有指令的计算机可读、计算机可执行的软件代码535，所述指令经配置以在执行时使处理器模块525执行本文中所描述的各种功能(例如，验证、解码，等等)。或者，软件代码535可不由处理器模块525直接执行，但可经配置以(例如)当编译和执行时使计算机执行本文中所描述的功能。因此，处理器模块525或处理器可为用于单独地或结合存储器530和软件代码535来译码、散列、组合、签名和/或加密的装置。

[0085] 处理器模块525可包含智能硬件装置，例如中央处理单元(CPU)、微控制器、专用集成电路(ASIC)，等等。收发器模块510可包含调制解调器，其经配置以调制包和向天线505提供调制包以用于发射，以及解调从天线505接收到的包。

[0086] 尽管单独地展示了蜂窝式通信管理模块515，但蜂窝式通信管理模块515的功能性可实施为收发器模块510的组件，实施为计算机程序产品，和/或实施为处理器模块525的一或多个控制器元件。类似地，DSRC通信管理模块520可实施为收发器模块510的组件，实施为计算机程序产品，和/或实施为处理器模块525的一或多个控制器元件。

[0087] 图6为说明方法600的一个实施例的流程图，方法600用于确保经由通信网络传递的内容安全。为了清楚起见，下文参照DSRC基站105中的一或多个的各方面描述方法600，DSRC基站105参照图1、2A、2B和/或3描述。在一个实施方案中，参照图3所描述的处理器模块325可执行一或多个代码集，以控制DSRC基站105的功能元件执行下文所述的功能。

[0088] 在框605处，可操作DSRC基站105对多个包译码以产生包的译码集。这可使用所确

定的代码完成。可如上所述确定代码。确切地说，译码可涉及确定在多个包中的包的数目(k)，以及使用所确定的代码对k个包译码以产生在包的译码集中的包的数目(m)。在一些实施例中，m可大于k。可确定在包的译码集中的包的数目(m)以使得具有至少k个包的包的译码集的子集足以恢复在多个包中的的k个包。此外，可至少部分地基于与多个散列经由无线通信网络的发射相关联的开销，确定在包的译码集中的包的数目(m)。

[0089] 在框610处，可操作DSRC基站105对包的译码集中的多个包进行散列处理。可按需要使用任何合适的散列算法来执行散列。以此方式，可确保用于传递的多个包的内容安全。尽管未说明，但可经由通信网络发射多个散列。因此，可通过有效方式执行在源处的译码和散列以提供用于传递的安全内容。

[0090] 图7为说明方法700的另一实施例的流程图，方法700用于确保经由通信网络传递的内容安全。为了清楚起见，下文参照DSRC基站105中的一或多个的各方面描述方法700，DSRC基站105参照图1、2A、2B和/或3描述。在一个实施方案中，参照图3所描述的处理器模块325可执行一或多个代码集，以控制DSRC基站105的功能元件执行下文所述的功能。

[0091] 在框705处，可操作DSRC基站105以从认证机构获取CRL。这可(例如)通过DSRC基站105从认证机构经由任何合适的装置接收发射来实现。

[0092] 在框710处，DSRC基站105可对包括CRL的多个包译码以产生包的译码集。如上，这可使用所确定的代码完成。

[0093] 在框715处，可操作DSRC基站105对包的译码集中的多个包进行散列处理。同样，可按需要使用任何合适的散列算法来执行散列。以此方式，可确保用于传递的内容(CRL)安全。

[0094] 在框720处，可操作DSRC基站105将多个散列组合成至少一个包。随后，在框725处，可操作DSRC基站105使用电子签名对至少一个包进行签名。或者或另外，在框730处，可操作DSRC基站105加密至少一个包。最后，在框735处，可发射至少一个经签名和/或经加密的包。根据此实施例，可通过有效方式执行在源处的译码和散列以确保用于传递的内容安全。此外，使用电子签名进行签名或加密可为发射的接收方提供验证至少一个包的有效机制。

[0095] 图8为说明方法800的实施例的流程图，方法800用于经由通信网络的安全内容传递。为了清楚起见，下文参照DSRC基站105中的一或多个的各方面描述方法800，DSRC基站105参照图1、2A、2B和/或3描述。在一个实施方案中，参照图3所描述的处理器模块325可执行一或多个代码集，以控制DSRC基站105的功能元件执行下文所述的功能。

[0096] 在框805处，可操作DSRC基站105对多个包译码以产生包的译码集。如上，这可使用所确定的代码完成。

[0097] 在框810处，可操作DSRC基站105对包的译码集中的多个包进行散列处理。同样，可按需要使用任何合适的散列算法来执行散列。以此方式，可确保用于传递的内容(CRL)安全。

[0098] 在框815处，可操作DSRC基站105发射经散列处理的多个包。随后，在框820处，可操作DSRC基站105选择包的译码集中的至少一个包。这可随机进行。最后，在框825处，可操作DSRC基站105广播至少一个选定包。根据此实施例，可通过有效方式执行在源处的译码和散列以确保用于传递的内容安全。此外，选择和广播包的译码集中的包可提供用于遍及网络传递原始多个包的安全内容的有效机制。

[0099] 图9为说明方法900的一个实施例的流程图，方法900用于在无线通信网络中的安全内容传递。为了清楚起见，下文参照DSRC装置115中的一或多个的各方面描述方法900，DSRC装置115参照图1、4A、4B和/或5描述。在一个实施方案中，参照图5所描述的处理器模块525可执行一或多个译码集，以控制DSRC装置115的功能元件执行下文所述的功能。

[0100] 在框905处，可操作DSRC装置115接收对应于包的译码集的多个散列。例如，这可通过接收在图6的框615中或在图7的框735中的发射来执行。

[0101] 在框910处，可操作DSRC装置115接收与多个散列相关联的电子签名。例如，这可通过接收在图7的框735中的发射来执行。

[0102] 随后，在框915处，可操作DSRC装置115以至少部分地基于接收到的电子签名来验证接收到的多个散列。根据此实施例，可通过有效方式执行接收在源处已经译码和进行散列处理的数据以传递安全内容。此外，可基于电子签名有效地验证数据。

[0103] 图10为说明方法1000的另一实施例的流程图，方法1000用于经由通信网络的安全内容传递。为了清楚起见，下文参照DSRC装置115中的一或多个的各方面描述方法1000，DSRC装置115参照图1、4A、4B和/或5描述。在一个实施方案中，参照图5所描述的处理器模块525可执行一或多个代码集，以控制DSRC装置115的功能元件执行下文所述的功能。

[0104] 在框1005处，可操作DSRC装置115以接收对应于包的译码集的多个散列。例如，这可通过接收在图6的框615中或在图7的框735中的发射来执行。

[0105] 在框1010处，可操作DSRC装置115以接收与多个散列相关联的电子签名。例如，这可通过接收在图7的框735中的发射来执行。

[0106] 随后，在框1015处，可操作DSRC装置115以至少部分地基于接收到的电子签名来验证接收到的多个散列。

[0107] 在框1020处，可操作DSRC装置115以将具有电子签名的经验证的多个散列转发到一或多个其它DSRC装置115。此外，在框1025处，可操作DSRC装置115以转发对包的译码集译码的代码、经译码以产生包的数目(m)的多个包中的包的数目(k)，以及包的数目(m)。如上文所论述，这可通过在(例如)所转发的散列的标头中包含代码、k和m来实现。根据此实施例，可通过有效方式执行接收在源处已经译码和进行散列处理的数据以传递安全内容。另外，可基于电子签名有效地验证数据。此外，可将经验证的数据转发到其它DSRC装置115，以提供遍及网络的安全内容传递。

[0108] 图11为说明方法1100的另一实施例的流程图，方法1100用于经由通信网络的安全内容传递。为了清楚起见，下文参照DSRC装置115中的一或多个的各方面描述方法1100，DSRC装置115参照图1、4A、4B和/或5描述。在一个实施方案中，参照图5所描述的处理器模块525可执行一或多个代码集，以控制DSRC装置115的功能元件执行下文所述的功能。

[0109] 在框1105处，可操作DSRC装置115以接收对应于包的译码集的多个加密散列。例如，这可通过接收在图7的框735中的发射来执行。

[0110] 随后，在框1110处，可操作DSRC装置115以至少部分地基于加密来验证接收到的多个散列。根据此实施例，可通过有效方式执行接收在源处已经译码和进行散列处理的数据以传递安全内容。此外，可基于加密有效地验证数据。

[0111] 图12为说明方法1200的另一实施例的流程图，方法1200用于经由通信网络的安全内容传递。为了清楚起见，下文参照DSRC装置115中的一或多个的各方面描述方法1200，

DSRC装置115参照图1、4A、4B和/或5描述。在一个实施方案中，参照图5所描述的处理器模块525可执行一或多个译码集，以控制DSRC装置115的功能元件执行下文所述的功能。

[0112] 在框1205处，可操作DSRC装置115接收对应于包的译码集的多个加密散列。例如，这可通过接收在图7的框735中的发射来执行。

[0113] 然后，在框1210处，可操作DSRC装置115以至少部分地基于加密来验证接收到的多个散列。在框1215处，可操作DSRC装置115将经验证的多个加密散列转发到一或多个其它DSRC装置115。此外，在框1220处，可操作DSRC装置115转发对包的译码集译码的代码、经译码以产生包的数目(m)的多个包中的包的数目(k)，以及包的数目(m)。如上文所论述，这可通过在(例如)所转发的散列的标头中包含代码、k和m来实现。根据此实施例，可通过有效方式执行接收在源处已经译码和进行散列处理的数据以传递安全内容。另外，可基于加密有效地验证数据。此外，可将经验证的数据转发到其它DSRC装置115，以提供遍及网络的安全内容传递。

[0114] 图13为说明方法1300的另一实施例的流程图，方法1300用于经由通信网络的安全内容传递。为了清楚起见，下文参照DSRC装置115中的一或多个的各方面描述方法1300，DSRC装置115参照图1、4A、4B和/或5描述。在一个实施方案中，参照图5所描述的处理器模块525可执行一或多个译码集，以控制DSRC装置115的功能元件执行下文所述的功能。

[0115] 在框1305处，可操作DSRC装置115接收对应于包的译码集的多个散列。例如，这可通过接收在图6的框615中或在图7的框735中的发射来执行。

[0116] 在框1310处，可操作DSRC装置115接收包的译码集中的包。例如，这可通过接收在图8的框825中的广播来执行。

[0117] 随后，在框1315处，可操作DSRC装置115对接收到的包进行散列处理以产生接收到的包的散列。

[0118] 在框1320处，可操作DSRC装置115比较接收到的包的散列与接收到的多个散列中的对应散列以验证接收到的包。根据此实施例，可通过有效方式执行接收在源处已经译码和进行散列处理的数据以传递安全内容。另外，可基于接收到的多个散列中的对应散列，通过在接收到的包上仅执行散列来有效地验证接收到的包。

[0119] 以上结合附图阐述的详细描述描述了例示性实施例，但并不表示是可实施的仅有实施例或权利要求书范围内的仅有实施例。贯穿本说明书使用的术语“例示性”意味着“充当实例、例子或说明”，而不是“优选的”或“优于其它实施例的”。为了提供所描述的技术的理解，详细描述包含具体细节。但是，这些技术可在没有这些具体细节的情况下实践。在一些例子中，以框图的形式展示众所周知的结构和装置以免混淆所描述的实施例的概念。

[0120] 本文中所描述的技术可用于各种无线通信系统，例如CDMA、TDMA、FDMA、OFDMA、SC-FDMA和其它系统。术语“系统”和“网络”通常可互换地使用。CDMA系统可实施例如CDMA2000、全球陆地无线接入(UTRA)等等的无线电技术。CDMA2000涵盖IS-2000、IS-95和IS-856标准。IS-2000版本0和A通常被称为CDMA20001X、1X，等等。IS-856(TIA-856)通常被称为CDMA20001xEV-DO、高速包数据网络(HRPD)，等等。UTRA包含宽带CDMA(WCDMA)和CDMA的其它变化形式。TDMA系统可实施例如全球移动通信系统(GSM)的无线电技术。OFDMA系统可实施例如超移动宽带(UMB)、演进型UTRA(E-UTRA)、IEEE 802.11(Wi-Fi)、IEEE 802.16(WiMAX)、IEEE 802.20、快闪OFDM等等的无线电技术。UTRA和E-UTRA是全球移动电信系统(UMTS)的部

分。3GPP长期演进(LTE)及LTE高级(LTE-A)是使用E-UTRA的UMTS的新版本。UTRA、E-UTRA、UMTS、LTE、LTE-A和GSM描述于来自名为“第三代合作伙伴计划”(3GPP)的组织的文献中。CDMA2000和UMB描述于来自名为“第三代合作伙伴计划2”(3GPP2)的组织的文献中。本文中所描述的技术可用于以上所提及的系统和无线电技术,以及其它系统和无线电技术。但是,出于实例的目的,以上描述描述了LTE系统,且LTE术语用于以上描述中的多处,但所述技术可适用于LTE应用之外的应用。

[0121] 因此,以下描述提供实例,且并不限于在权利要求书中阐述的范围、适用性或配置。可在不脱离本发明的精神和范围的情况下对元件的功能和布置作出改变。各种实施例可在适当时省略、替换或添加各种程序或组件。举例来说,所描述的方法可以不同于所描述的顺序执行,并且各种步骤可添加、省略或加以组合。另外,相对于某些实施例描述的特征可在其它实施例中加以组合。

[0122] 以上结合附图阐述的详细描述描述了例示性实施例,但并不表示是可实施的仅有实施例或权利要求书范围内的仅有实施例。贯穿本说明书使用的术语“例示性”意味着“充当实例、例子或说明”,而不是“优选的”或“优于其它实施例的”。为了提供所描述的技术的理解,详细描述包含具体细节。但是,这些技术可在没有这些具体细节的情况下实践。在一些例子中,以框图的形式展示众所周知的结构和装置以免混淆所描述的实施例的概念。

[0123] 可使用多种不同技术及技艺中的任一个来表示信息和信号。例如,可由电压、电流、电磁波、磁场或磁粒子、光场或光粒子或其任何组合来表示可在整个以上描述中参考的数据、指令、命令、信息、信号、位、符号和码片。

[0124] 可使用通用处理器、数字信号处理器(DSP)、专用集成电路(ASIC)、现场可编程门阵列信号(FPGA)或其它可编程逻辑装置、离散门或晶体管逻辑、离散硬件组件或经设计以进行本文所描述的功能的任何组合来实施或执行结合本发明所描述的各种说明性方框和模块。通用处理器可为微处理器,但在替代方案中,处理器可为任何常规处理器、控制器、微控制器或状态机。处理器还可实施为计算装置的组合,例如DSP和微处理器、多个微处理器、结合DSP核心的一或多个微处理器或任何其它此类配置的组合。

[0125] 本文中所描述的功能可以由处理器、固件或其任何组合执行的硬件、软件的形式实施。如果以由处理器执行的软件的形式实施,那么可将功能作为一或多个指令或代码存储于计算机可读媒体上或经由计算机可读媒体发射。其它实例和实施方案在本发明及所附权利要求书的范围和精神内。例如,由于软件的性质,所以上文所描述的功能可使用由处理器、硬件、固件、硬连线或这些中的任一者的组合执行的软件来实施。实施功能的特征还可物理地位于各种位置处,包含经分配以使得在不同物理位置处实施功能的部分。另外,如本文(包含权利要求书)中所使用,在以“至少一个”为结束的项列表中所使用的“或”表明分离性列表,以使得(例如)“A、B或C中的至少一个”意味A或B或C或AB或AC或BC或ABC(即,A和B和C)。

[0126] 计算机可读媒体包含计算机存储媒体与包含促进计算机程序从一处传送到另一处的任何媒体的通信媒体两者。存储媒体可以是可由通用或专用计算机存取的任何可用媒体。借助于实例而非限制,计算机可读媒体可包括RAM、ROM、EEPROM、CD-ROM或其它光盘存储装置、磁盘存储装置或其它磁性存储装置,或可用于以指令或数据结构的形式运载或存储所要的程序代码装置并且可由通用或专用计算机或通用或专用处理器存取的任何其它媒

体。另外，将任何连接恰当地称为计算机可读媒体。例如，如果使用同轴电缆、光纤电缆、双绞线、数字订户线(DSL)或无线技术(例如，红外线、无线电和微波)从网站、服务器或其它远程源发射软件，那么所述同轴电缆、光纤电缆、双绞线、DSL或无线技术(例如，红外线、无线电和微波)包含在媒体的定义中。如本文所使用，磁盘和光盘包含压缩光盘(CD)、激光光盘、光学光盘、数字多功能光盘(DVD)、软性磁盘和蓝光光盘，其中磁盘通常以磁性方式再生数据，而光盘使用激光以光学方式再生数据。上述项的组合也可包含在计算机可读媒体的范围内。

[0127] 提供对本发明的先前描述以使得所属领域的技术人员能够制作或使用本发明。对本发明的各种修改对所属领域的技术人员来说将容易显而易见，且在不脱离本发明的精神或范围的情况下，本文中定义的一般原理可应用于其它变化形式。贯穿本发明的术语“实例”或“例示性”表明实例或例子，但并不暗示或需要对所提到的实例的任何偏好。因此，本发明不限于本文中所描述的实例和设计，而应符合与本文中所揭示的原理和新颖特征相一致的最广范围。

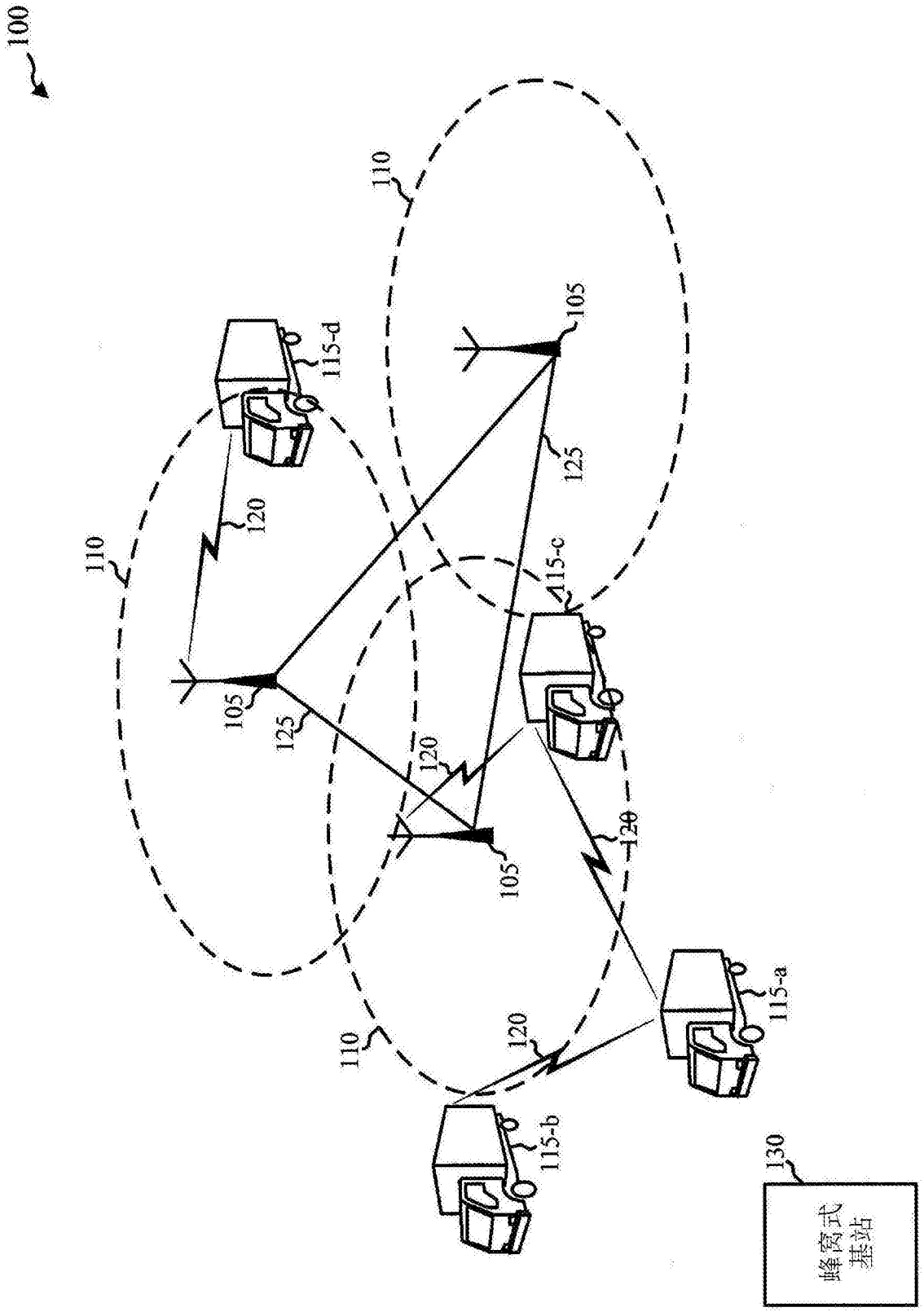

100
110
105
115-d
125
120
110
115-c
105
125
120
105
120
115-a
110
120
115-b
130
蜂窝式基站

图1

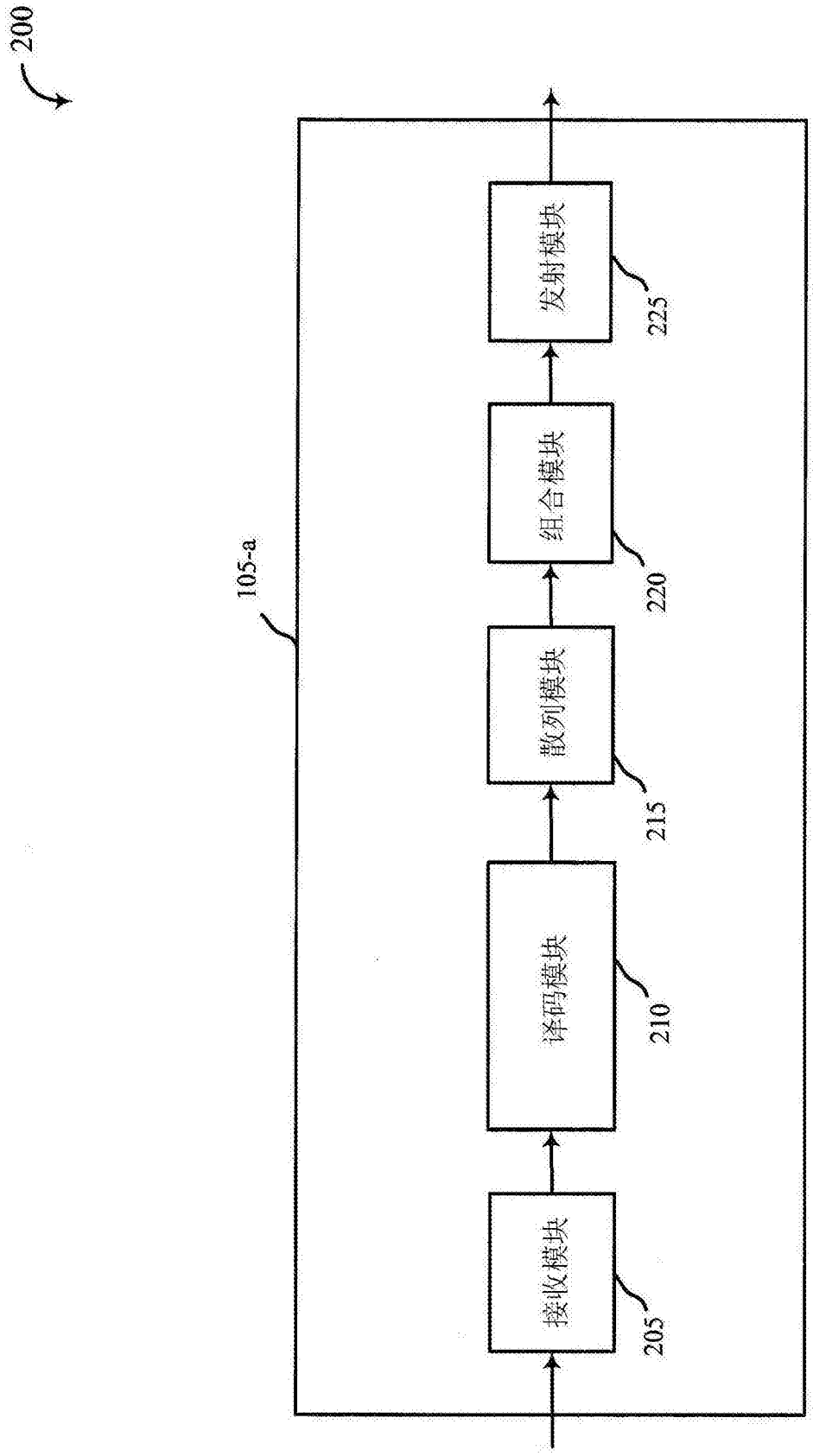


图2A

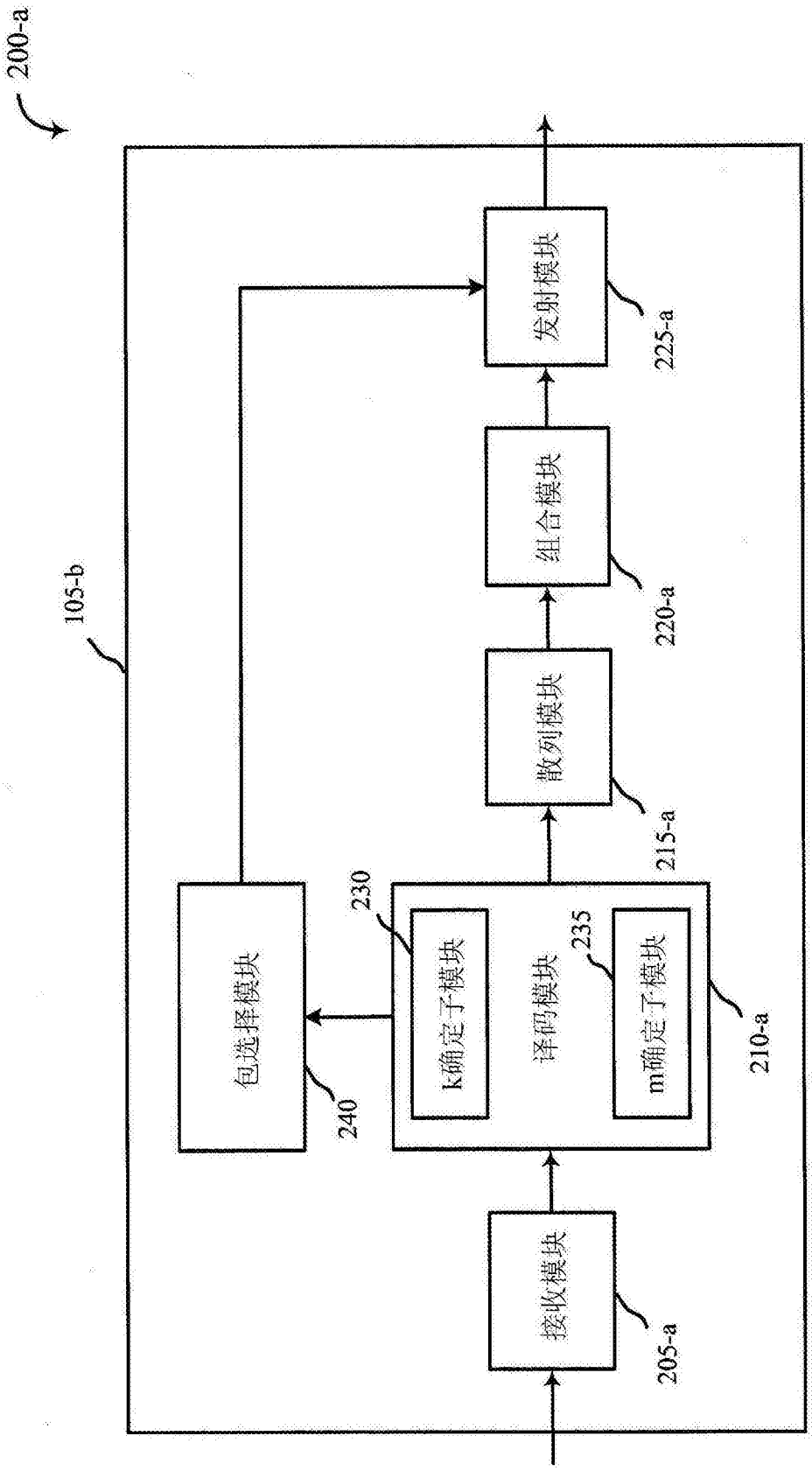

200-a
105-b
接收模块
205-a
译码模块
210-a
k确定子模块
230
m确定子模块
235
散列模块
215-a
组合模块
220-a
发射模块
225-a
包选择模块
240

图2B

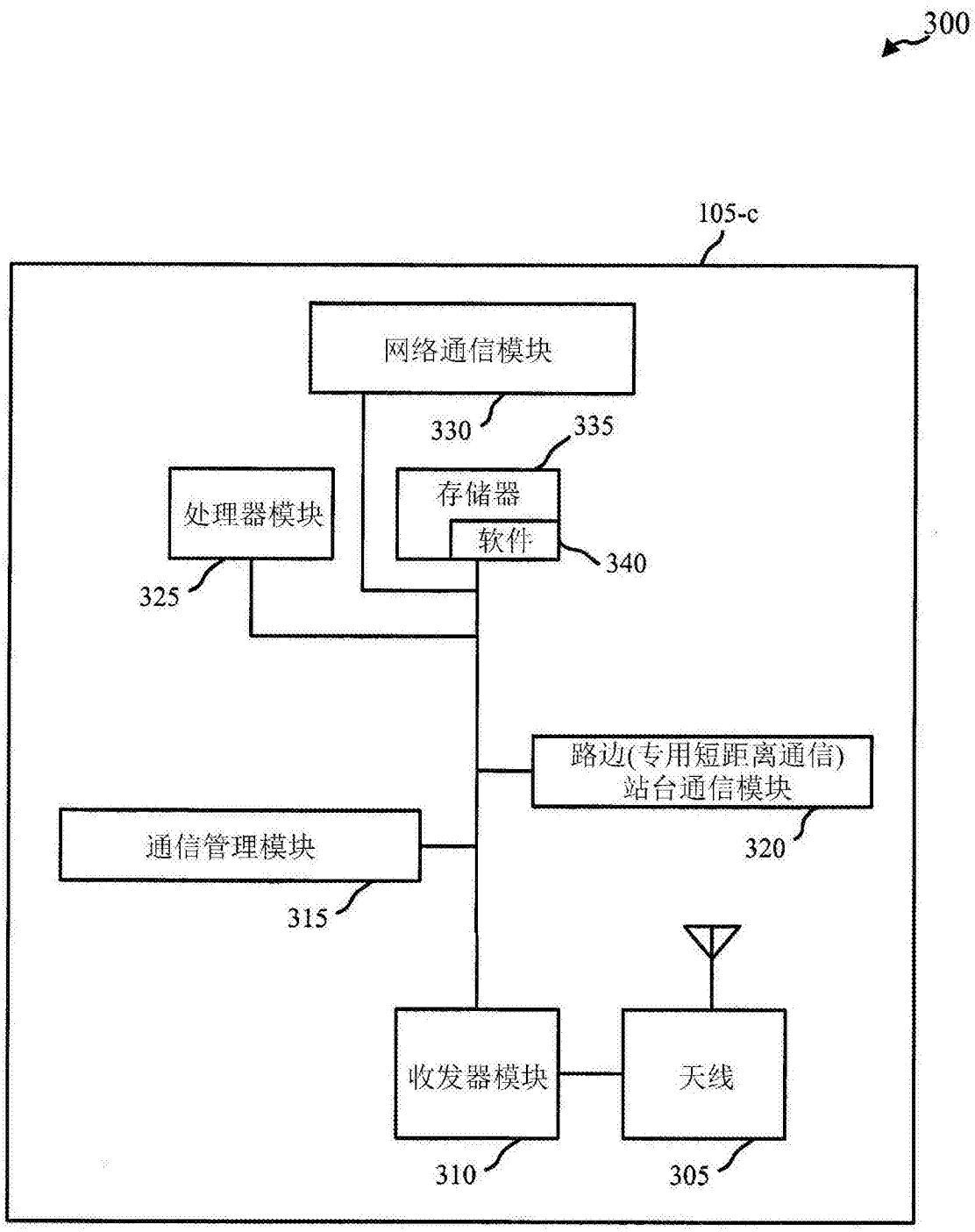

300
105-c
网络通信模块
330
335
存储器
软件
340
处理器模块
325
路边(专用短距离通信)
站台通信模块
320
通信管理模块
315
收发器模块
天线
310
305

图3

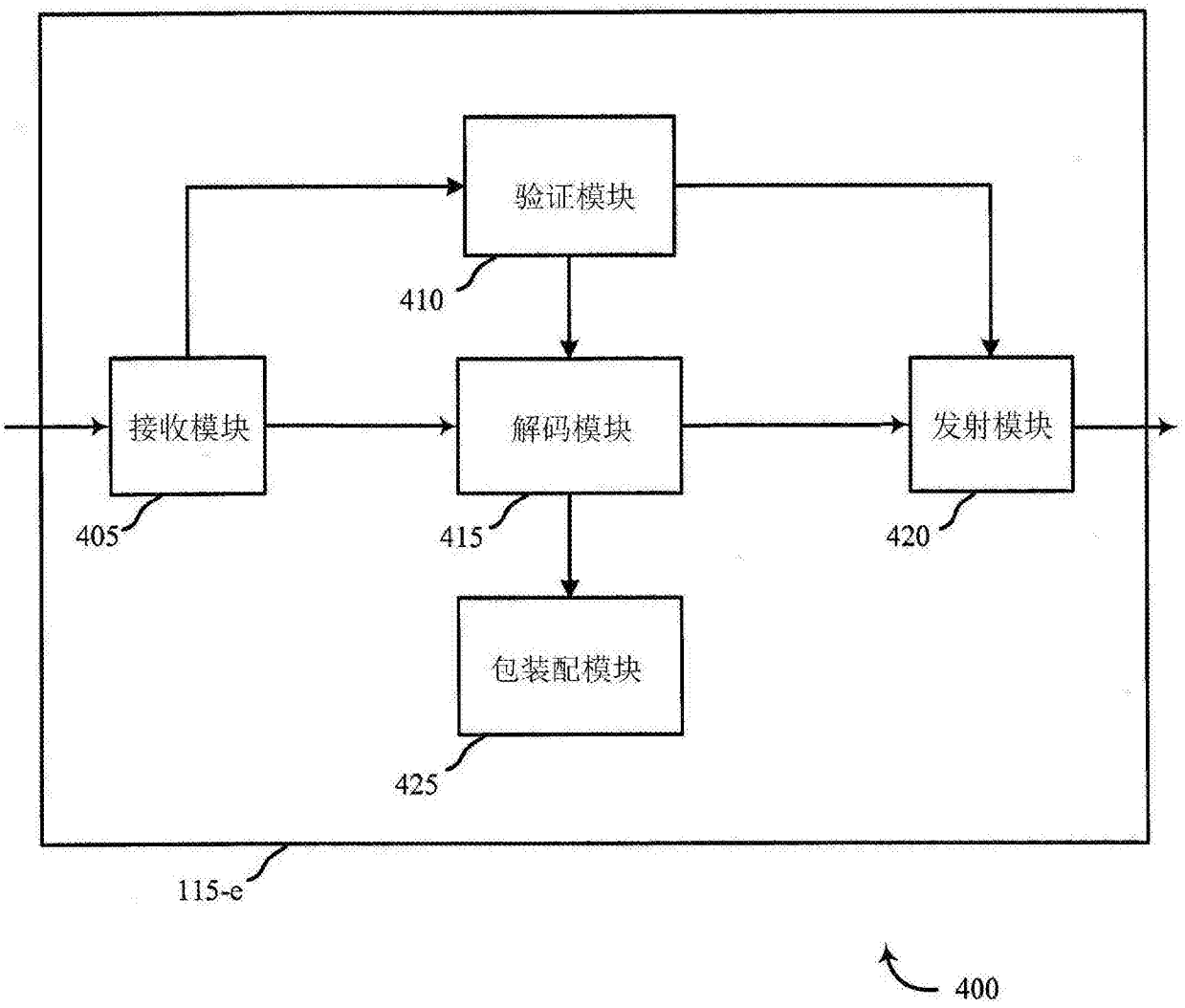


图4A

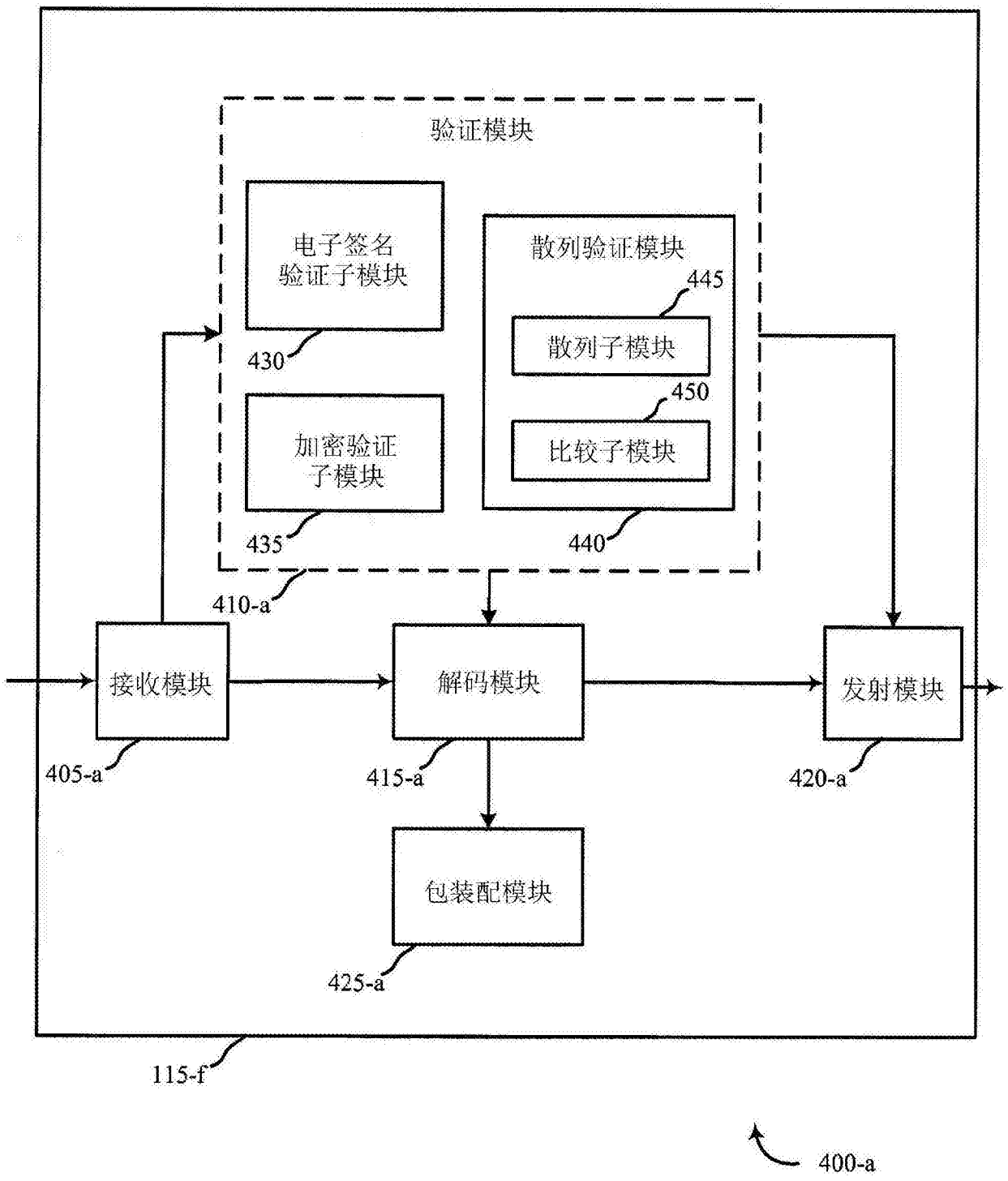

验证模块
电子签名
验证子模块
430
散列验证模块
445
散列子模块
450
比较子模块
加密验证
子模块
435
440
410-a
接收模块
解码模块
发射模块
405-a
415-a
420-a
包装配模块
425-a
115-f
400-a

图4B

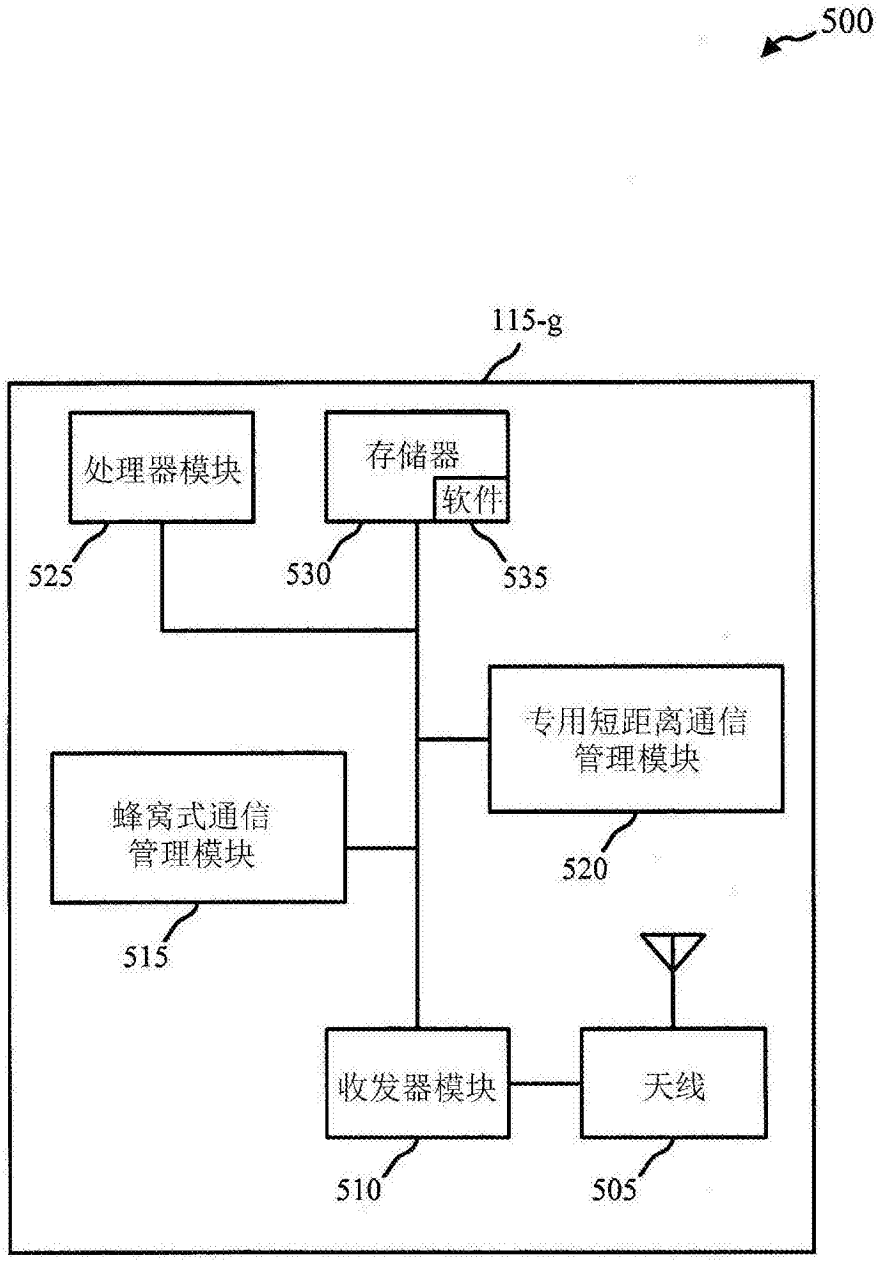

500
115-g
处理器模块
存储器
软件
525
530
535
专用短距离通信
管理模块
520
蜂窝式通信
管理模块
515
收发器模块
天线
510
505

图5

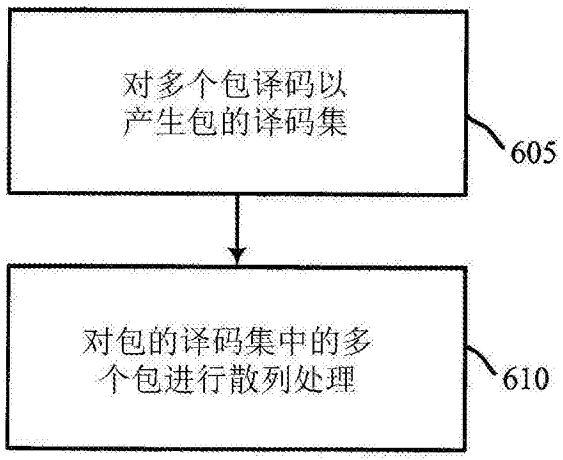


图6

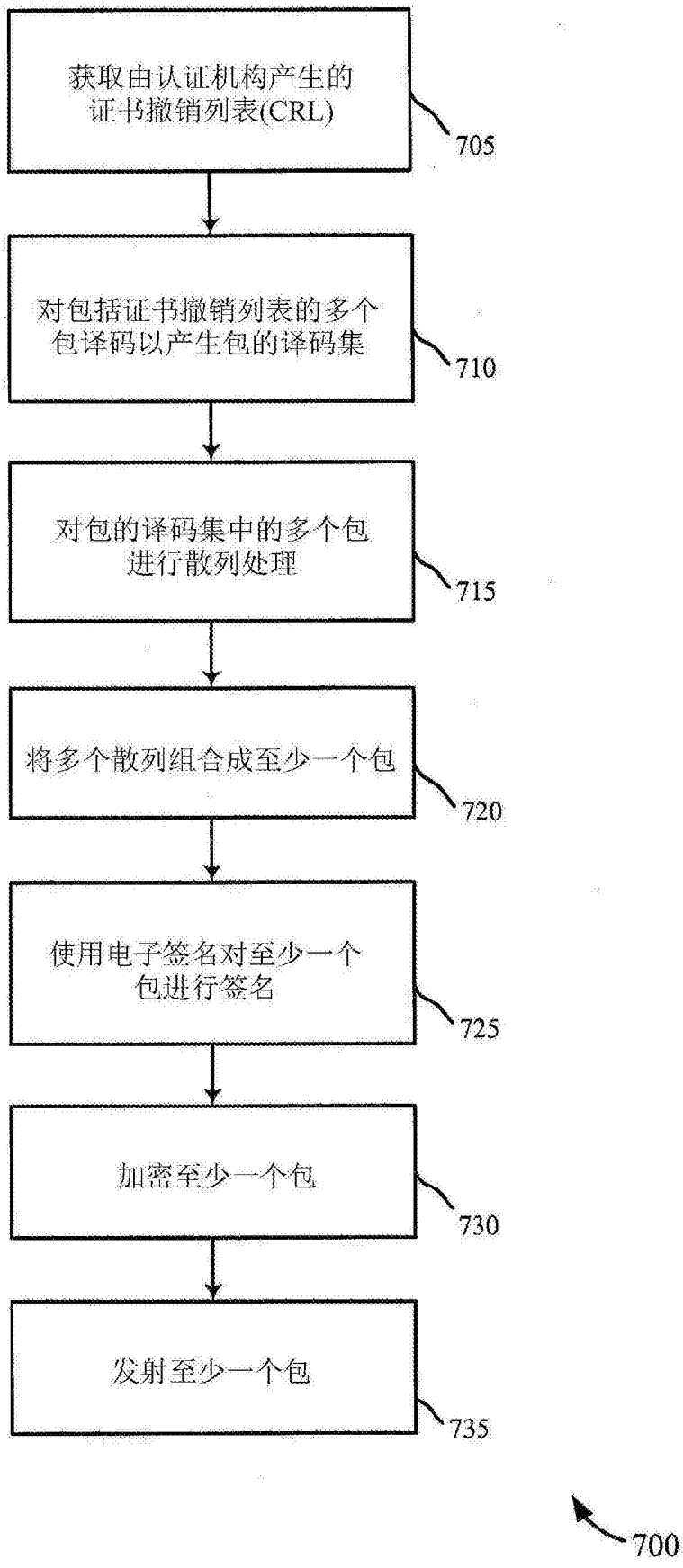

获取由认证机构产生的证书撤销列表(CRL)
705
对包括证书撤销列表的多个包译码以产生包的译码集
710
对包的译码集中的多个包进行散列处理
715
将多个散列组合成至少一个包
720
使用电子签名对至少一个包进行签名
725
加密至少一个包
730
发射至少一个包
735
700

图7

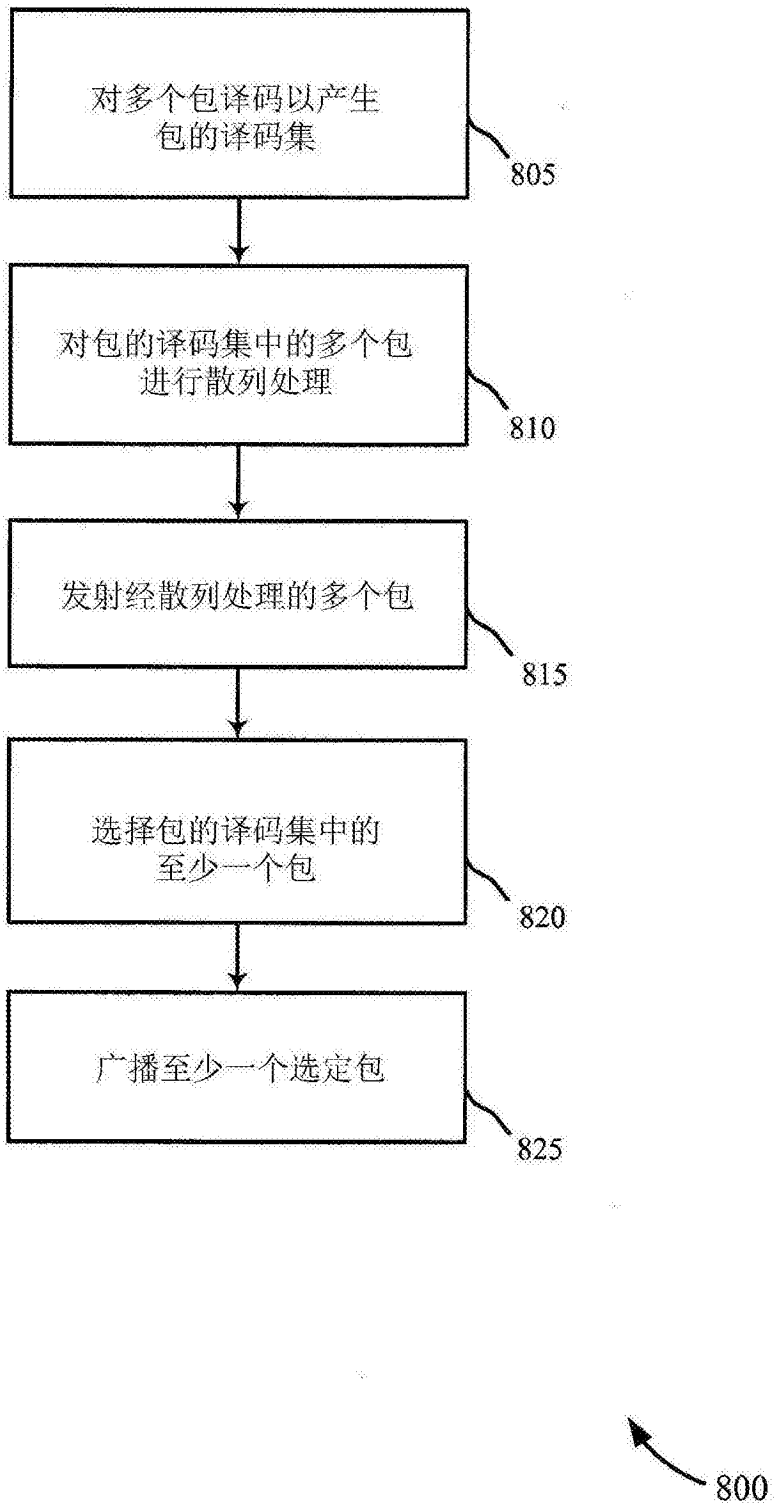

对多个包译码以产生包的译码集
805
对包的译码集中的多个包进行散列处理
810
发射经散列处理的多个包
815
选择包的译码集中的至少一个包
820
广播至少一个选定包
825
800

图8

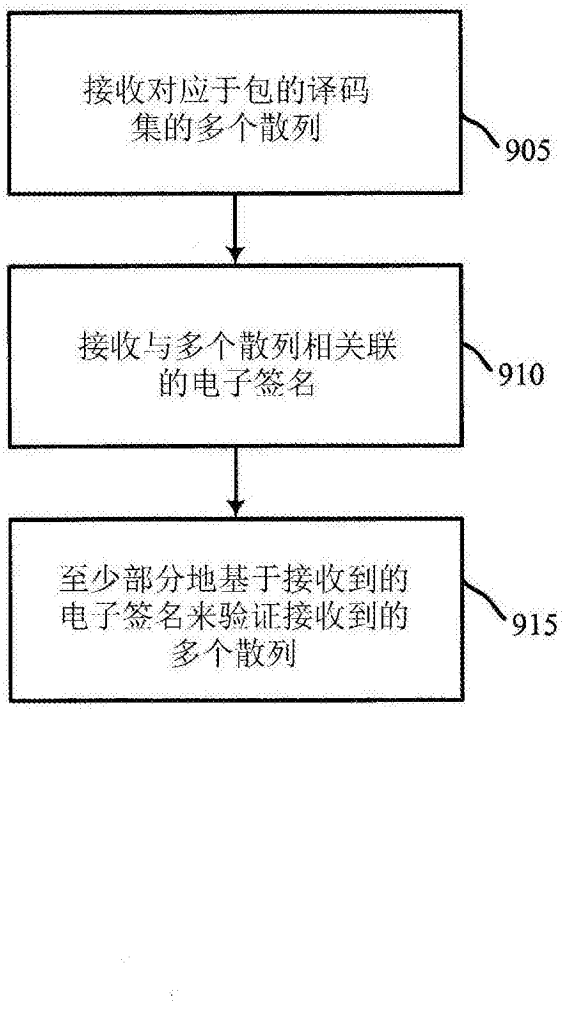

接收对应于包的译码集的多个散列
905
接收与多个散列相关联的电子签名
910
至少部分地基于接收到的电子签名来验证接收到的多个散列
915
900

图9

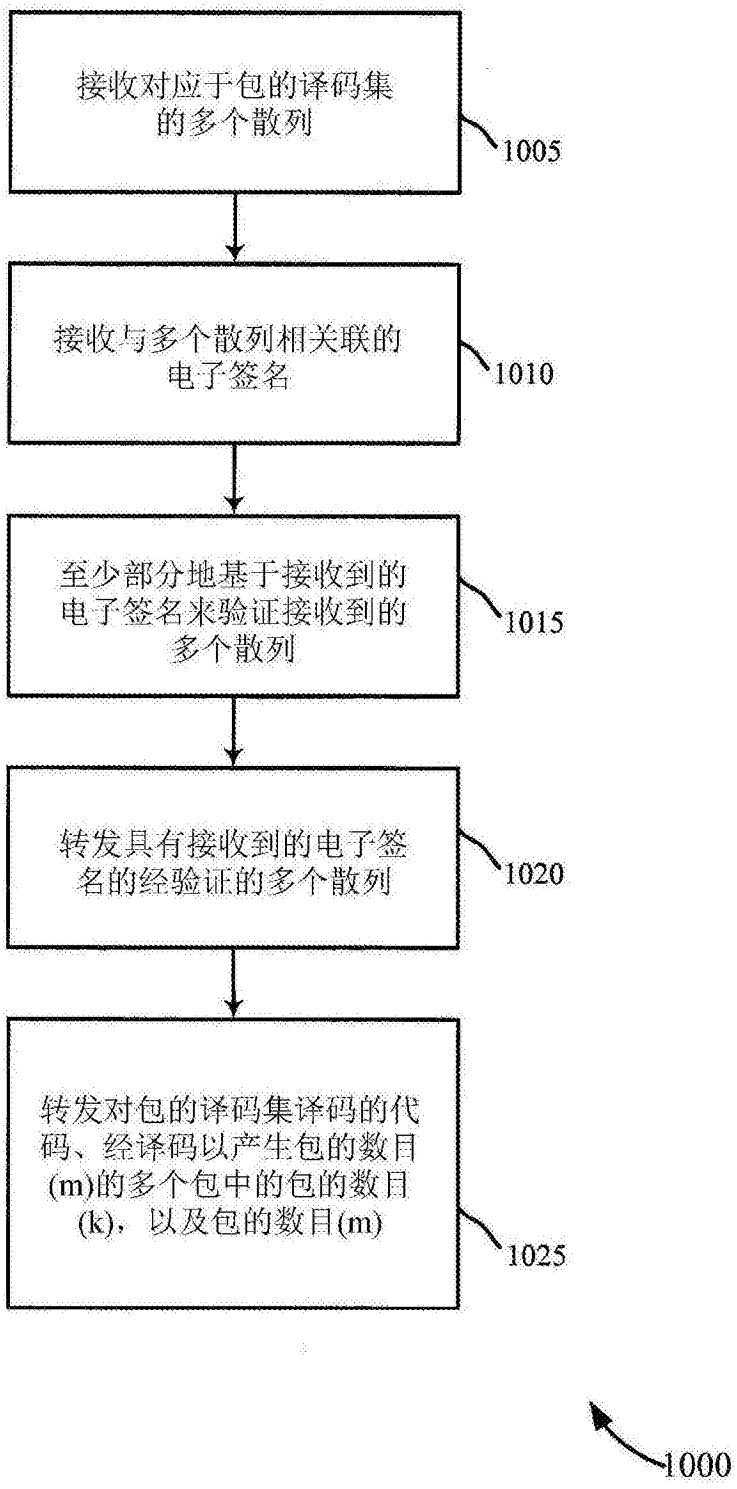

接收对应于包的译码集的多个散列
1005
接收与多个散列相关联的电子签名
1010
至少部分地基于接收到的电子签名来验证接收到的多个散列
1015
转发具有接收到的电子签名的经验证的多个散列
1020
转发对包的译码集译码的代码、经译码以产生包的数目(m)的多个包中的包的数目(k)，以及包的数目(m)
1025
1000

图10

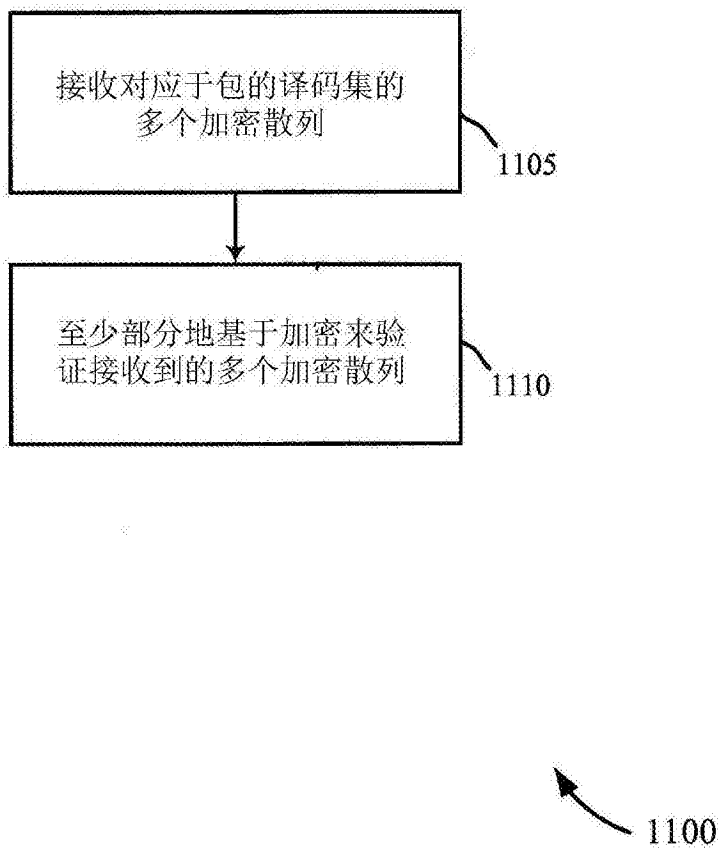

接收对应于包的译码集的多个加密散列
1105
至少部分地基于加密来验证接收到的多个加密散列
1110
1100

图11

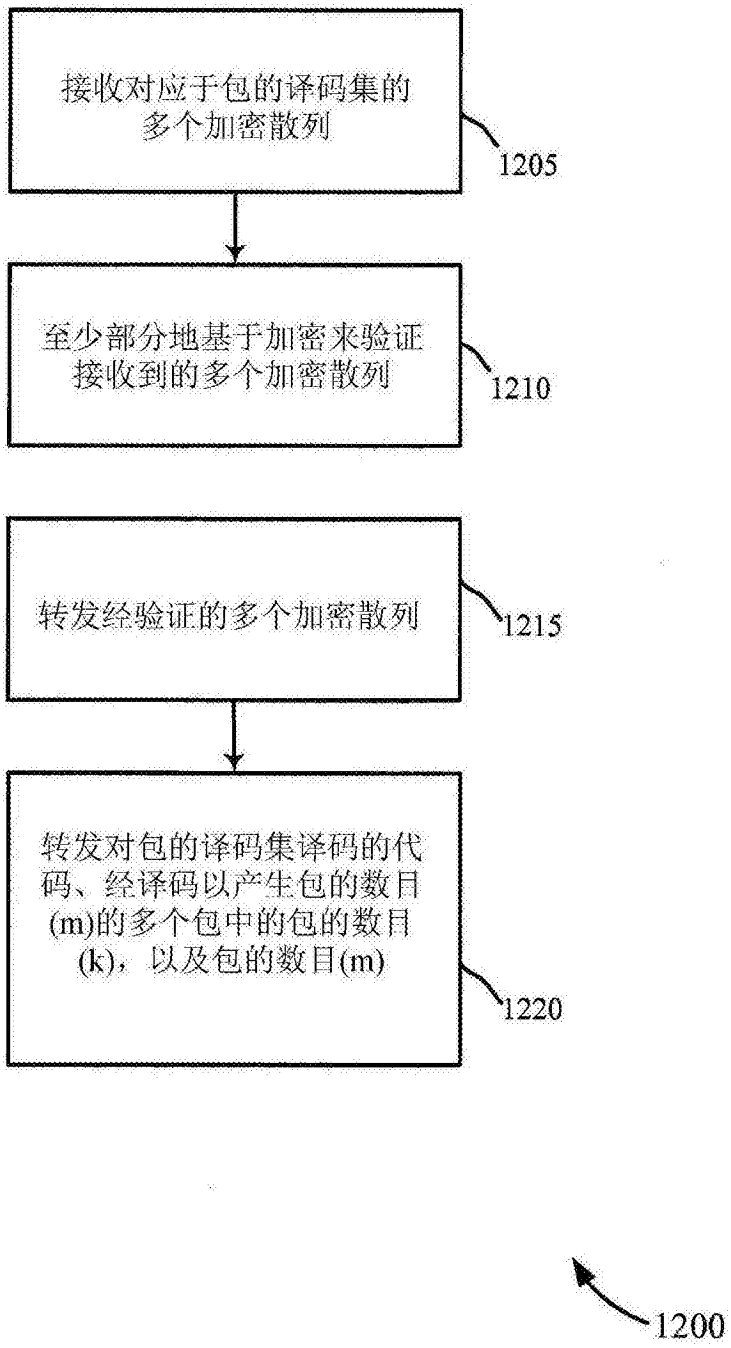

接收对应于包的译码集的多个加密散列
1205
至少部分地基于加密来验证接收到的多个加密散列
1210
转发经验证的多个加密散列
1215
转发对包的译码集译码的代码、经译码以产生包的数目(m)的多个包中的包的数目(k)，以及包的数目(m)
1220
1200

图12

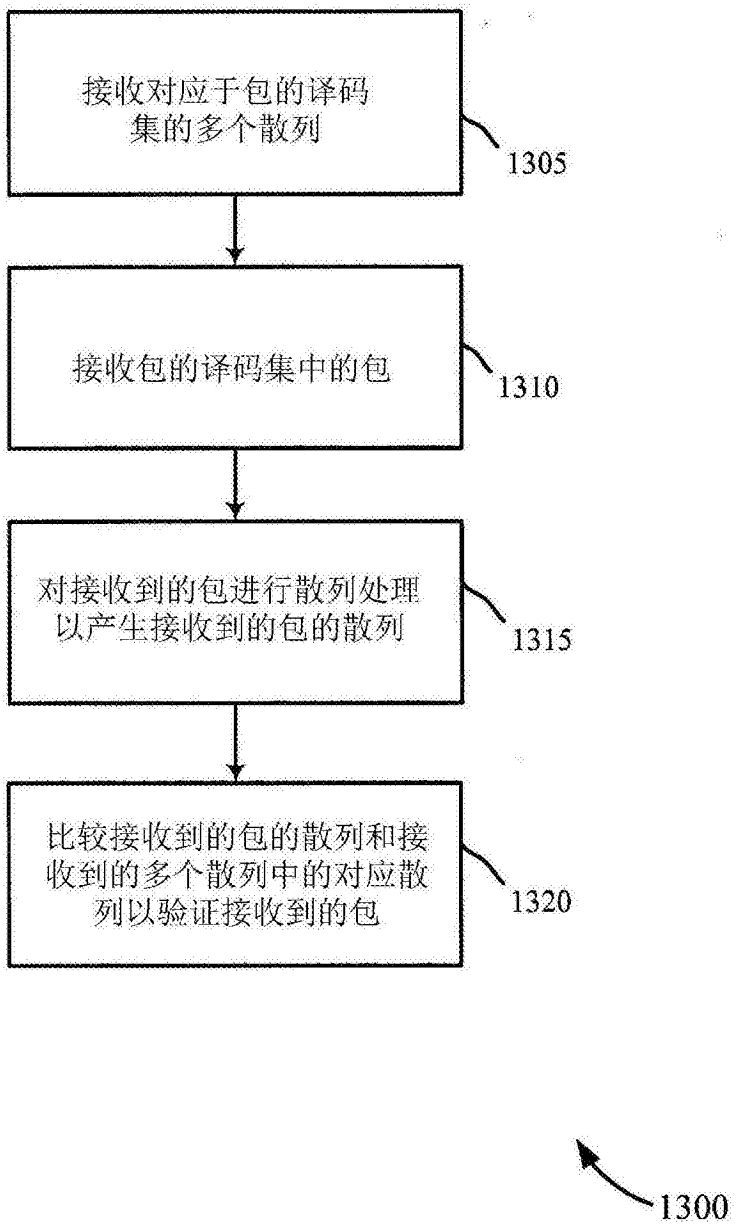

接收对应于包的译码集的多个散列
1305
接收包的译码集中的包
1310
对接收到的包进行散列处理以产生接收到的包的散列
1315
比较接收到的包的散列和接收到的多个散列中的对应散列以验证接收到的包
1320
1300

图13