

[19] 中华人民共和国国家知识产权局



[12] 发明专利申请公开说明书

[21] 申请号 02815759.1

[51] Int. Cl.

C06Q 10/00 (2006.01)

H04L 29/06 (2006.01)

H04L 9/32 (2006.01)

H04L 12/58 (2006.01)

[43] 公开日 2006 年 1 月 4 日

[11] 公开号 CN 1717697A

[22] 申请日 2002.6.12 [21] 申请号 02815759.1

[30] 优先权

[32] 2001.6.12 [33] US [31] 60/297,681

[32] 2002.3.20 [33] US [31] 60/365,535

[86] 国际申请 PCT/CA2002/000889 2002.6.12

[87] 国际公布 WO2002/101605 英 2002.12.19

[85] 进入国家阶段日期 2004.2.11

[71] 申请人 捷讯研究有限公司

地址 加拿大安大略省沃特卢市

[72] 发明人 詹姆斯·A·戈弗雷

赫伯特·A·利特尔

迈克尔·K·布朗

尼尔·P·亚当斯 卡尔·L·彻丽

蒂莫西·R·泰赫斯特

迈克尔·S·布朗

[74] 专利代理机构 中科专利商标代理有限责任公司

代理人 朱进桂

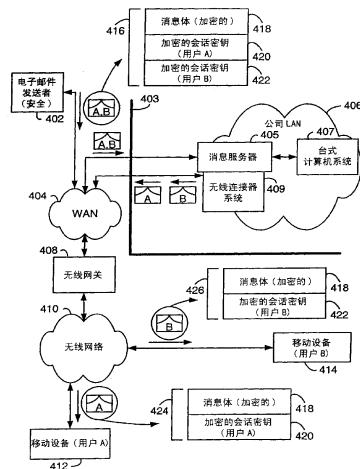
权利要求书 12 页 说明书 48 页 附图 22 页

[54] 发明名称

压缩安全电子邮件用于与移动通信设备交换的系统和方法

[57] 摘要

提供了一种在消息传送到无线移动通信设备之前在主系统预处理加密和/或签名的消息的系统和方法。在主系统从消息发送者接收消息。确定是否任何一个消息接收者具有相应的无线移动通信设备。对于具有相应的无线移动通信设备的每个消息接收者，处理消息以便针对加密和/或验证情况修改消息。处理的消息被传送到相应的无线移动通信设备。系统和方法可包括从无线移动通信设备发送到远程系统的后处理消息。对消息执行验证和/或加密消息。然后所处理的消息通过远程系统发送到一个或多个接收者。



1. 一种在消息发送到无线移动通信设备之前在主系统减少加密消息的尺寸的方法，该方法包括步骤：
 - (a) 在主系统从消息发送者接收寻址到第一和第二消息接收者的加密的消息，该加密的消息包括加密的消息体和用于每个消息接收者的加密的会话密钥；
 - (b) 在主系统产生包含加密的消息体和用于第一消息接收者的加密的会话密钥的第一减少尺寸的加密消息，所述第一减少尺寸的加密消息不包括用于第二消息接收者的加密的会话密钥； 和
 - (c) 将第一减少尺寸的加密消息传送到对应于所述第一消息接收者的无线移动通信设备。
2. 如权利要求1所述的方法，其特征在于产生第一减少尺寸的加密消息的步骤包括步骤：去除除了用于第一消息接收者的加密的会话密钥之外的加密的会话密钥以形成第一减少尺寸的加密的消息。
3. 如权利要求1所述的方法，其特征在于产生第一减少尺寸的加密消息的步骤包括步骤：去除除了用于第一消息接收者的加密的会话密钥之外的所有加密的会话密钥以形成第一减少尺寸的加密的消息。
4. 如权利要求3所述的方法，其特征在于产生第一减少尺寸的加密消息的步骤包括步骤：去除将每个加密的会话密钥映射到消息接收者的消息的消息接收者信息字段。
5. 如权利要求1所述的方法，其特征在于，所述接收步骤 (a) 包括步骤：在主系统从消息发送者接收寻址到多个消息接收者的加密的消息，该加密的消息包括加密的消息体和用于每个消息接收者的加密的会话密钥；该方法进一步包括步骤：确定是否任何一个消息接收者具有一相应的无线移动通信设备；所述产生步骤 (b) 包括步骤：对于具有一相应无线移动设备的每个消息接收者，产生包含加密的消息体和仅用于该消息接收者的加密的会话密钥。

密钥的减少尺寸的加密消息；和

所述传送步骤(c)包括步骤：将减少尺寸的加密消息传送到无线移动通信设备。

6. 如权利要求5所述的方法，其特征在于单个地址由消息接收者和相应的
5 无线移动通信设备共享。

7. 如权利要求5所述的方法，其特征在于每个加密的会话密钥使用消息接收者的公钥加密，并且消息接收者和相应的无线移动通信设备共享公钥和相关私钥。

8. 如权利要求1所述的方法，其特征在于所述加密的消息是已经被签名然
10 后加密的消息，并且进一步包括加密的数字签名；和

产生第一减少尺寸的加密的消息的步骤包括步骤：产生包含加密的消息体，加密的数字签名和用于第一消息接收者的加密的会话密钥的减少尺寸的加密的消息。

9. 如权利要求8所述的方法，其特征在于，
15 加密的消息进一步包括加密的签名相关信息；和

产生第一减少尺寸的加密的消息的步骤包括步骤：产生包含加密的消息体，加密的数字签名，加密的签名相关信息和用于第一消息接收者的加密的会话密钥的减少尺寸的加密的消息。

10. 如权利要求1所述的方法，其特征在于，所述加密的消息是安全多用
20 途互联网邮件扩展(S/MIME)电子邮件消息。

11. 如权利要求1所述的方法，其特征在于，所述加密的消息按照极好保密性(Pretty Good Privacy,PGP)加密。

12. 一种按照权利要求1的方法产生的第一减少尺寸的加密消息。

13. 一种减少加密消息的尺寸以传送到无线移动设备的系统，该系统包括：

25 主系统，被配置用于接收来自消息发送者并且寻址到消息接收者的加密消息，该加密消息包括加密消息体和用于每个消息接收者的加密会话密钥；和

无线连接器系统，与主系统相关联，并且被配置以确定是否任何一个消息接收者具有相应的无线移动设备，并且如果是，对于具有相应无线移动通信设备的每个消息接收者，产生包含消息体和仅用于消息接收者的加

密会话密钥的减少尺寸的加密的消息，并且将减少尺寸的加密的消息传递到无线移动设备。

14. 如权利要求13所述的系统，其特征在于所述主系统包括消息服务器系统。

5 15. 如权利要求14所述的系统，其特征在于消息服务器系统在网络安全防火墙后面的安全网络中实现。

16. 如权利要求13所述的系统，其特征在于所述主系统包括台式计算机系统或膝上计算机系统。

17. 如权利要求13所述的系统，其特征在于网络运营者基础设施实现主系统和无线移动通信设备之间的无线信息交换。

18. 一种在消息发送到无线移动通信设备之前在主系统减少加密消息的尺寸的系统，该系统包括：

接收装置，用于在主系统从消息发送者接收寻址到第一和第二消息接收者的加密的消息，该加密的消息包括加密的消息体和用于每个消息接收者的加密的会话密钥；

产生装置，用于在主系统产生包含加密的消息体和用于第一消息接收者的加密的会话密钥的第一减少尺寸的加密消息，所述第一减少尺寸的加密消息不包括用于第二消息接收者的加密的会话密钥；和

传送装置，用于将第一减少尺寸的加密消息传送到对应于所述第一消息接收者的无线移动通信设备。

19. 一种无线设备，包括存储第一减少尺寸的加密消息的存储器，其中，第一减少尺寸的加密消息由远程系统基于从消息发送者提供到远程系统的加密消息产生，所述来自消息发送者的所述加密消息已经含有到第一和第二消息接收者的地址，所述发送者的加密消息包括加密的消息体和用于每个消息接收者的加密的会话密钥，

其中，所述第一减少尺寸的加密消息包含加密的消息体和用于第一消息接收者的加密的会话密钥，由远程系统发送到无线设备的所述第一减少尺寸的加密消息不包括用于第二消息接收者的加密的会话密钥。

20. 如权利要求19所述的无线设备，其特征在于所述无线设备具有与第一消息接收者的关联，所述关联指示无线设备将接收发送到第一消息接收者

的消息。

21. 如权利要求19所述的无线设备，其特征在于所述远程系统包括主系统装置。

22. 如权利要求19所述的无线设备，其特征在于所述主系统包括无线连接
5 系统装置。

23. 一种在包括第一减少尺寸的加密消息的载波中包含的计算机数据信号，其中，第一减少尺寸的加密消息由远程系统基于从消息发送者提供到远程系统的加密消息产生，所述来自消息发送者的所述加密消息已经含有到第一和第二消息接收者的地址，所述发送者的加密消息包括加密的消息体和用于每个消息接收者的加密的会话密钥，
10

其中，所述第一减少尺寸的加密消息包含加密的消息体和用于第一消息接收者的加密的会话密钥，由远程系统发送到无线设备的所述第一减少尺寸的加密消息不包括用于第二消息接收者的加密的会话密钥。

24. 一种在消息发送到无线移动通信设备之前在主系统重新安排签名的消息的方法，该方法包括步骤：
15

在主系统从消息发送者接收寻址到消息接收者的签名消息，该签名消息具有数字签名和签名的消息体；

确定是否任何消息接收者具有相应的无线移动通信设备；

如果任何消息接收者具有相应的无线移动通信设备，然后：

20 重新安排所述接收的签名消息以便产生包括由数字签名跟随的签名消息体的重新安排的消息； 和

将所述重新安排的消息传送到每个相应的无线移动通信设备。

25. 如权利要求24所述的方法，其特征在于所接收的签名消息还包括签名相关信息，该方法还包括步骤：

如果一个或多个消息接收者具有相应的无线移动通信设备，那么执行
25 步骤包括：

在主系统存储签名相关信息； 和

仅响应于来自无线移动通信设备的请求将签名相关信息传送到任何一个无线移动通信设备。

30 26. 如权利要求24所述的方法，其特征在于所述接收的签名消息还包括签

名相关信息；和

重新安排接收的签名消息的步骤包括：重新安排接收的签名消息以产生包括由数字签名和签名相关信息跟随的签名消息体的重新安排的消息。

27. 如权利要求24所述的方法，其特征在于所接收的签名消息还包括签名
5 相关信息，

所述方法还包括步骤：如果一个或多个消息接收者具有相应的无线移动通信设备，确定签名相关信息是否存储在每个相应的无线移动通信设备上；

重新安排接收的签名消息的步骤包括步骤：

10 对于签名相关信息存储在其上的每个无线移动通信设备，重新安排接收的签名消息以产生包括由数字签名跟随的签名消息体的第一重新安排的消息；和

15 对于签名相关信息不存储在其上的每个无线移动通信设备，重新安排接收的签名消息以产生包括由数字签名和签名相关信息跟随的签名消息体的第二重新安排的消息；和

传送重新安排的消息到每个相应的无线移动通信设备的步骤包括步骤：

将第一重新安排的消息传送到签名相关信息存储在其上的每个相应无线移动通信设备；和

20 将第二重新安排的消息传送到签名相关信息不存储在其上的每个相应无线移动通信设备。

28. 如权利要求27所述的方法，其特征在于，传送第二重新安排的消息的步骤包括步骤：

将第二重新安排的消息的签名的消息体和数字签名传送到签名相关信息不存储在其上的每个相应无线移动通信设备；

25 将签名相关信息存储在主系统上；和

将签名相关信息传送到仅响应于来自无线移动通信设备的请求而不将签名相关信息存储在其上的任何一个无线移动通信设备。

29. 如权利要求25所述的方法，其特征在于所述签名相关信息包括一个或多个消息发送者证书、包括一个或多个链证书的证书链和用于证书和任何链证书的证书注销表。

30. 如权利要求27所述的方法，其特征在于所述签名相关信息包括一个或多个消息发送者证书、包括一个或多个链证书的证书链和用于证书和任何链证书的证书注销表。

31. 如权利要求27所述的方法，其特征在于确定签名相关信息是否存储在

5 每个相应的无线移动通信设备上的步骤包括：访问存储在主系统上用于每个相应无线移动通信设备的用户的用户配置文件。

32. 如权利要求24所述的方法，其特征在于所述签名消息是已经加密然后
签名的消息，并且还包括用于每个消息接收者的加密的会话密钥，这样消息体被加密并且加密的消息体和加密的会话密钥二者被签名；和

10 该重新安排的消息包括加密的消息体和由数字签名跟随的加密的会话密钥。

33. 如权利要求25所述的方法，其特征在于所述签名消息是已经加密然后
签名的消息，并且还包括用于每个消息接收者的加密的会话密钥，这样消息体被加密并且加密的消息体和加密的会话密钥二者被签名；和

15 该重新安排的消息包括加密的消息体和由数字签名跟随的加密的会话密钥。

34. 如权利要求27所述的方法，其特征在于，所述签名消息是已经加密然后
签名的消息，并且还包括用于每个消息接收者的加密的会话密钥，这样消息体被加密并且加密的消息体和加密的会话密钥二者被签名；和

20 其中第一重新安排的消息包括加密的消息体和由数字签名跟随的加密的会话密钥；和

其中第二重新安排的消息包括加密的消息体和由数字签名和签名相关信息跟随的加密的会话密钥。

35. 如权利要求24所述的方法，其特征在于：

25 所述加密的消息是已经签名然后加密的消息，并且还包括加密的数字
签名；和

该重新安排接收的签名消息的步骤包括步骤：产生用于具有相应的无线移动通信设备的每个消息接收者的减少尺寸的加密的消息，包含加密的消息体，加密的数字签名和用于消息接收者的加密的会话密钥。

30 36. 一种在消息发送到无线移动通信设备之前在主系统预处理加密消息的

方法，该方法包括步骤：

在主系统从消息发送者接收寻址到消息接收者的加密的消息，该加密的消息包括加密的消息体和用于每个消息接收者的加密的会话密钥；

- 确定是否任何一个消息接收者具有相应的无线移动通信设备； 和
5 对于具有相应的无线移动通信设备的每个消息接收者，

解密加密的消息体以恢复原始消息； 和

将原始消息传送到相应的无线移动通信设备。

37.如权利要求36所述的方法，其特征在于解密加密的消息体的步骤包括
10 步骤：

对于具有相应的无线移动通信设备的每个消息接收者，执行步骤包
括：

产生包括用于消息接收者的加密的会话密钥的第二消息；

将第二消息到传送无线移动通信设备；

15 从无线移动设备接收解密的会话密钥，加密的会话密钥使用关于
无线移动通信设备上的私钥被解密； 和

使用解密的会话密钥解密加密的消息体。

38. 如权利要求36所述的方法，其特征在于解密加密的消息体的步骤包括
步骤：

20 对于具有相应的无线移动通信设备的每个消息接收者，执行步骤包
括：

检索与相应的无线移动设备相关并且存储在主系统处的私钥；

使用私钥解密用于消息接收者的加密的会话密钥； 和

使用解密的会话密钥解密加密的消息体。

25 39. 如权利要求36所述的方法，其特征在于传送的步骤包括：按照在主系
统和无线移动通信设备之间实现的安全方案重新加密原始的消息。

40. 如权利要求39所述的方法，其特征在于所述安全机制是三重数据加密
标准（Triple Data Encryption Standard）。

41. 如权利要求39所述的方法，其特征在于传送的步骤还包括压缩原始消
30 息。

42. 如权利要求37所述的方法，其特征在于还包括步骤：

在无线移动通信设备处，执行步骤包括：

从主系统接收第二消息；

使用关于无线移动通信设备的私钥解密加密的会话密钥；

5 按照在主系统和无线移动通信设备之间实现的安全方案重新加密解密的会话密钥；和

传送该重新加密的会话密钥到主系统，和

在主系统处，

解密该重新加密的会话密钥。

10

43. 如权利要求36所述的方法，其特征在于解密加密的消息体的步骤仅被执行一次，以恢复原始消息。

44. 如权利要求37所述的方法，其特征在于产生第二消息和传送第二消息的步骤针对每个相应的无线移动通信设备重复，并且解密加密的消息体的

15 步骤仅当从任何一个相应的无线移动通信设备接收解密的会话密钥时被执行一次。

45. 如权利要求36所述的方法，其特征在于：

加密的消息是已经被签名然后加密的消息，并且还包括加密的数字签名；

20 该方法还包括，在解密步骤之后，执行验证操作以检验数字签名的步骤；和

传送的步骤包括将原始消息和验证操作结果的指示传送到每个相应的无线移动通信设备。

46. 如权利要求45所述的方法，其特征在于：

25 传送的步骤包括将原始消息，验证操作结果的指示和原始消息被加密的指示传送到每个相应的无线移动通信设备；和

该方法还包括步骤：在传送步骤之前，按照在主系统和每个无线移动通信设备之间实现的安全方案，加密原始消息、验证操作的结果的指示和原始消息被加密的指示。

30 47. 一种在将消息发送到无线移动通信设备之前在主系统预处理签名的消

息的方法，该方法包括步骤：

在主系统从消息发送者接收签名的消息，该签名的消息被寻址到一个或多个消息接收者，并且具有数字签名和签名的消息体；

确定是否任何一个消息接收者具有相应的无线移动通信设备；和
如果一个或多个消息接收者具有相应的无线移动通信设备，那么，

执行验证操作以检验数字签名；和

将消息体和验证操作的结果的指示传送到每个相应的无线移动通信设备。

10 48. 如权利要求47所述的方法，其特征在于数字签名包括消息体摘要和摘要的签名，其中所述验证操作包括步骤：

产生消息体的摘要；

从数字签名提取摘要；

使用消息发送者的公钥检验摘要的签名；和

15 比较产生的摘要和提取的摘要，

其中当摘要的签名被验证并且产生的摘要和提取的摘要匹配时验证数字签名。

49. 如权利要求47所述的方法，其特征在于消息体和指示按照在主系统和无线移动通信系统之间实现的安全方案被加密。

20 50. 如权利要求48所述的方法，其特征在于：

签名消息还包括签名相关信息；

验证操作包括检验签名相关信息以确定是否数字签名被信任；和

仅当签名被信任时验证数字签名。

51. 如权利要求47所述的方法，其特征在于：

25 所述签名消息是已经加密然后签名的消息，并且还包括用于每个消息接收者的加密的会话密钥，这样消息体被加密并且加密的消息体和加密的会话密钥二者被签名；

该方法还包括，在执行验证操作步骤之后，解密加密的消息体以恢复原始消息的步骤；和

30 传送的步骤包括：将原始消息和验证操作结果的指示传送到每个

相应的无线移动通信设备。

52. 如权利要求51所述的方法，其特征在于传送步骤包括：将原始消息，验证操作结果的指示和原始消息被加密的指示传送到每个相应的无线移动通信设备。

5 53. 如权利要求52所述的方法，其特征在于还包括步骤：在传送步骤之前，按照在主系统和每个无线移动通信设备之间实现的安全方案，加密原始消息、验证操作的结果的指示和原始消息被加密的指示。

54. 一种在消息被转发到消息接收者之前在主系统后处理签名的消息的方法，该方法包括步骤：

10 从无线移动通信设备接收寻址到一个或多个消息接收者的签名消息，并且签名消息包括消息体、数字签名和签名相关信息指示；

从签名消息中去除签名相关信息指示；

将签名相关信息指示中标识的签名相关信息附加到签名的消息；
和

15 将带有附加的签名相关信息的签名消息转发到消息接收者。

55. 如权利要求54所述的方法，其特征在于所述签名信息包括一个或多个无线移动通信设备的证书、包括一个或多个链证书的证书链和用于证书和任何链证书的证书注销表。

56. 如权利要求54所述的方法，其特征在于所述签名的消息是已经加密然后签名的消息，从而使得签名的消息体被加密，并且签名的消息还包括用于每个消息接收者的加密的会话密钥。

57. 一种在消息前送到消息接收者之前在主系统后处理加密的消息的方法，该方法包括步骤：

从无线移动通信设备接收寻址到一个或多个消息接收者的加密消息，并且加密消息包括加密的消息体和会话密钥；

从加密消息中去除会话密钥；

检索每个消息接收者的公共加密密钥；

使用每个消息接收者的公钥加密会话密钥以产生多个会话密钥，包括用于每个消息接收者的一个会话密钥；

30 将多个加密的会话密钥附加到加密的消息体； 和

将加密的消息体和附加的加密的会话密钥转发到每个消息接收者。

58. 如权利要求57所述的方法，其特征在于：

5 加密的消息在被发送到主系统之前按照无线移动通信设备和主系统之间实现的安全方案由无线移动通信设备加密；和

该方法还包括步骤：在主系统解密消息以恢复加密的消息体和会话密钥。

59. 如权利要求57所述的方法，其特征在于加密的消息是已经签名然后加密的消息并且还包括加密的数字签名。

10 60. 一种在消息被转发到消息接收者之前在主系统后处理消息的方法，包括步骤：

在主系统从无线移动通信设备接收被寻址到一个或多个消息接收者的消息，所述消息按照在主系统和无线移动通信设备之间实现的安全方案被加密，并且包括消息体和至少签名指示、签名相关信息指示、加密指示和会话密钥之一；

在主系统解密接收的消息；

基于签名指示，确定是否消息将被签名，并且如果是，然后

产生代表无线移动通信设备的消息体的数字签名并且将数字签名附加到消息体；和

20 基于签名相关信息指示，确定是否签名相关信息将附加到消息，并且如果是，然后将签名相关信息附加到消息体；

基于加密指示，确定消息是否将被加密，并且如果是，然后

确定接收的消息是否包括会话密钥；

如果接收的消息包括会话密钥，则使用会话密钥加密消息体；

25 如果接收的消息不包括会话密钥，则产生会话密钥并且使用产生的会话密钥加密消息体；

使用每个消息接收者的公钥，加密用于加密接收的消息的会话密钥；和

将每个加密的会话密钥附加到加密的消息体；和

30 将消息体和任何附加的信息转发到每个消息接收者。

61. 如权利要求60所述的方法，其特征在于，在消息转发到消息接收者之前，主系统可以签名消息，加密消息，首先签名然后通过加密消息体、数字签名和任何附加的签名相关信息来加密消息，或者首先加密，然后通过基于加密的消息体和加密的会话密钥产生数字签名并且如果任何签名相关信息被包括在接收的消息中，附加在签名相关信息指示中标识的任何签名相关信息来签名消息。
5

62. 一种在消息传送到无线移动通信设备之前在主系统处理编码的消息的方法，该方法包括步骤：

10 在主系统从消息发送者接收寻址到多个消息接收者的编码的消息；
确定是否任何消息接收者具有相应的无线移动通信设备； 和
对于具有相应的无线移动通信设备的每个消息接收者：

处理消息以便针对编码情况修改消息，所述编码情况是从由编码情况、验证情况和它们的组合的组中选择的； 和
将所述处理的消息传送到相应的无线移动通信设备。

压缩安全电子邮件用于与移动通信设备交换的系统和方法

5

与相关申请的交叉参考

该申请要求美国临时申请 2001 年 6 月 12 日提交的 S/N 60/297,681 和 2002 年 3 月 20 日提交的 S/N 60/365,535 的优先权。这些临时申请的每一个的全部公开包括附图被引用包含在该申请中。

10 发明背景

发明领域

本发明一般涉及安全电子消息，并且特别涉及通过运行移动设备的无线通信网络在主系统和移动通信设备（“移动设备”）之间交换安全电子邮件消息的高级系统和方法。

15 相关技术描述

有很多已知的用于主系统和移动设备之间交换信息的方案。然而，这些系统趋于遵循简单的编码方法，用于将原始消息缩短的版本传递给移动设备，尤其当处理验证和/或加密时。这限制了移动设备在处理这类消息中的使用。

20 简述

按照在此提供的教导，提供了一种系统和方法，用于在消息传送到无线移动通信设备之前，预处理加密和/或签名的消息。在主系统处从消息发送者接收消息。判断任何消息接收者是否具有一个相应的无线移动通信设备。对于具有一个相应无线移动通信设备的每个消息接收器，处理所述消息以便针对加密和/或验证修改消息。被处理的消息传送到对应于消息接收者的无线移动通信设备。该系统和方法可包括从无线移动通信设备发送到远程系统的后处理消息。对消息执行验证和/或加密消息处理。然后所处理的消息通过远程系统发送到一个或多个接收器。

附图的简单描述

30 图 1 是表示可使用移动设备的环境的概观的方框图。

图 2 描述了目前通常在互联网中使用的电子邮件交换的主要类型。

图 3 是支持安全和非安全电子邮件交换二者的系统的主要组件的方框图。

图 4 是表示接收的加密消息尺寸减小的方框图。

5 图 5 是表示接收的签名消息尺寸减小的方框图。

图 6 是根据存储在移动设备处的信息减少签名的消息尺寸的系统方框图。

图 7 是用于已经加密然后签名的接收消息的安全消息尺寸减少的方框图。

10 图 8 是用于已经签名然后加密的接收消息的安全消息尺寸减少的方框图。

图 9 是表示加密消息预处理系统的方框图。

图 10 是签名消息预处理系统的方框图。

15 图 11 是用于已经加密然后签名的接收消息的安全消息预处理的方框图。

图 12 是用于已经签名然后加密的接收消息的安全消息预处理的方框图。

图 13 和 14 示出了对签名、加密或签名并加密的消息在将它们发送到移动设备之前进行预处理的方法流程图。

20 图 15 是用于后处理从移动设备发送的签名或加密然后签名的消息的方法流程图。

图 16 是用于后处理从移动设备发送的加密或签名然后加密的消息的方法流程图。

25 图 17 是能够使用在此描述的系统和方法的示范的无线通信设备的方框图。

图 18 和 19 是涉及移动设备的消息处理的方框图。

图 20 是表示通信系统例子的方框图。

图 21 是另一通信系统例子的方框图。

图 22 是另一可选的通信系统的方框图。

30 详细描述

对于访问存储在或与公司企业计算机系统相关的数据的移动设备的公司用户来说，更丰富以及安全的电子邮件经历需要在无线环境中支持 S/MIME, PGP 和其它电子邮件安全的方法。在此描述的系统和方法允许例如在公司用户和移动设备之间使用安全消息传送方法。已经由 2001 年 4 月 4 日发布的相关美国专利 6, 219, 694 使得这种公司电子邮件信箱到移动设备的扩展成为可能，该专利题名“从主系统到具有共享电子地址的移动数据通信设备推进信息的系统和方法（System and Method for Pushing Information from a Host System to a Mobile Data Communication Device Having a Shared Electronic Address”（在此称为“694 专利”），该专利被全部包含于此用作参考。通过使用这种如在‘694 专利’中描述的系统，可‘互联网’通信或格式化的电子邮件可以被发送或推送移动设备，由此提供更丰富和更远到达的安全，扩展了在今天移动通信行业可利用的技术。在先前的无线电子邮件方案中，不能合适地支持不同公司之间的安全。随着公司和私人用户二者之间安全电子邮件的增长，希望用于这种安全电子邮件方法的移动设备支持如 S/MIME 和 PGP 标准。

正如在该申请中使用的，术语“主系统”指在无线通信连接器系统（在此称为“无线连接器”）处运行或具有无线通信连接器系统或与其相关的一个或多个计算机。在一个实施例中，主系统是运行于操作在至少一个安全防火墙之后且被保护的公司网络环境内的服务器计算机。主系统实现无线连接器系统作为相关的无线通信使能组件，其通常是构建的软件程序/应用程序/组件，以便与至少一个或多个消息服务器一起工作，所述服务器诸如 MicrosoftTM 交换或 Lotus DominoTM。使用无线连接器系统或软件程序通过无线网络往移动设备发送和接收用户选择的信息。或者，主系统能够是一用户桌上或膝上 PC，并且也运行在连接到局域网（LAN）的公司环境内，或者是能够与用户 PC 通信的任何其它系统。于是，无线连接器系统或软件程序可以是基于服务器或基于 PC 的，这样，主系统可以是一服务器计算机，桌上计算机或膝上计算机。

一旦检测到已经发生了一个或多个触发事件，操作在主系统上的无线连接器系统使移动设备的用户能够通过无线网络从主系统向用户移动设备发送或映射用户选择的数据项或数据项的部分。在发送数据项到用户移

动设备的过程中，有启动 S/MIME 或 PGP 加密消息的支持执行的特殊处理。对于在 S/MIME 领域的技术人员，已知当 S/MIME 算法应用到消息时，原始电子邮件消息的尺寸猛烈增加。通过对消息使用高级滤波、重组织和预处理，用户仍然能够在移动设备上接收这些数据项。在某些情况下，
5 用户能够拥有对 S/MIME 处理阶段的完全控制，并且能够引导主系统应该对消息执行哪些程序。

当在主系统已经激活对公司数据的无线访问以用于移动设备时，例如当主系统检测到一触发事件发生，主系统以对移动设备透明的方式重新打包接收的消息，使得发送到并由移动设备接收的消息类似于存储在主系统
10 并且在主系统可访问的消息。触发事件包括但不限于一个或多个下列事件：从移动设备或另一计算机发送到主系统以开始发送存储在主系统处的一个或多个消息的命令，在主系统或与主系统相关的计算机上的屏幕保护应用程序的激活等。除了重新打包信息本身外，重新打包也可以提供关于消息的信息，例如消息是否已经被签名并且是否已经验证签名。一个优选
15 的重新打包的方法包括将要通过无线网络发送的接收的消息包装在对应于移动设备的无线网络地址的电子信封中。或者，另一重新打包的方法能够用于该系统，诸如特殊用途传输控制协议/互联网协议（TCP/IP）包装技术。这种重新打包最好还导致从移动设备发送的电子邮件消息似乎来自主系统即使它们是在移动设备处被起动（例如被编辑并且从移动设备发
20 送），于是使得移动设备用户对其消息的预定接收者来说似乎使用和具有一个单个电子邮件地址。

在可选的系统和方法中，无线连接器系统与网络服务器一起工作，并且编程服务器以从通过局域网（LAN）连接到服务器的多个用户计算机（诸如桌上和笔记本计算机）检测网络上的多个事件触发。服务器能够通过网络从每个用户台式计算机检测内部事件触发，并且也能检测外部事件触发，诸如来自用户移动设备的消息或命令。为了响应检测这些触发之一，服务器向合适的移动设备发送接收的消息。用于特定移动设备的消息和寻址信息能够存储在位于服务器上、连接到服务器上或与服务器相关的存储器设备上，或存储在位于、连接到或相关于连接到 LAN 的用户台式或笔记
30 本计算机处的存储器设备上。使用该可选的配置，一个无线连接器系统

能够服务多个用户。该可选配置也能包括互联网或基于内部网的系统，其能够通过安全网页或其它用户接口可访问。无线连接器系统也能位于互联网服务提供商（ISP）系统上并且单独可访问或也通过互联网接口访问。

在另一配置中，无线连接器系统运行于主系统和用户移动设备上。然
5 后，用户移动设备类似于主系统操作，并且以类似的方式配置，一旦检测
到移动设备处的触发事件将某些用户选择的数据项从移动设备发送到主
系统（或可能到某些其它目的地）。该配置提供主系统和移动设备之间信
息的双向发送。

图 1 是可使用移动设备的环境的概观的方框图。本领域技术人员能够
10 理解，能够有很多不同的结构，但是图 1 所示帮助展示系统和方法如何可
被实现。

在图 1 中，所示的安全防火墙 22 后面的公司 LAN 30 作为中央基于
服务器的主系统（在此典型地称为公司 LAN 或主场所）的例子。然而，
这个不限于是分部办公室、家庭办公室或交换电子邮件消息的其它场所的
15 主场所。如上所述，主系统可改为是台式或膝上计算机。还示出了电子邮
件发送者 10，其能够例如是使用 ISP 帐户的个人、另一公司内的人员、同一
公司内另一分部办公室内的人员或 ASP（应用服务提供商）用户。

公司 LAN 30 内是消息服务器 40，其运行于公司防火墙后的计算机上，
充当公司与通常是互联网的 WAN 20 交换电子邮件、日历数据、语音信件、
20 电子文档和其它个人信息管理（PIM）数据的主接口。两个最普通的消息
服务器 40 是 Microsoft Exchange 和 Lotus Domino 服务器产品。这些服务
器通常与互联网邮件路由器结合使用，互联网路由器典型地使用基于
UNIX 发送邮件协议来路由和传递电子邮件。这些中间步骤和计算机将取
决于通过其进行电子邮件消息交换的消息传递机构和网络的特定类型，但
25 是在图 1 中没有示出，因为它们在所描述的系统和方法的操作中不直接起
主要作用。消息服务器 40 不仅可以扩展到电子邮件发送和接收，而且提
供这些功能如已经预定义数据库格式用于象日历、待办事件表、任务表、
电子邮件和文档的数据的动态数据库存储引擎。

在该典型的公司环境内，如上简单描述的无线连接器系统 45 可以与
30 消息服务器 40 一起工作。无线连接器系统 45 可以驻留在与消息服务器 40

相同的计算机上，但这不是必须的。无线连接器系统 45 和消息服务器 40 被设计合作并且交互，以允许信息推移动设备 100。在这样的安装中，最好配置无线连接器系统 45 以借助无线网络通过公司防火墙 22 向用户的移动设备 100 为发送保密和非保密公司信息，所述发送是针对具有移动设备 5 100 的每个用户的。无线连接器系统 45 最好采用‘基于推送(push-based)’技术、‘基于拉回(pull-based)’技术或它们的某些组合，使得能够扩展包括消息服务器 40 的任何电子邮件系统。由此，用户移动设备 100 能够访问消息服务器的存储的消息。尽管该系统没有单独针对‘基于推送’技术，这种重定向系统的更详细描述可发现于上述引用的‘694’专利和下列 10 共同待审和共同拥有的美国专利申请中，所有这些涉及‘694’专利：美国专利申请 S/N 09/401,868, S/N 09/545,963, S/N 09/528, 495, S/N 09/545, 962, 和 S/N 09/649,755。每一个这些专利的全部公开包括附图和权利要求由此被包含于该申请中被引用。该推送技术使用一个无线友好编码(wireless friendly encoding)、压缩和加密技术将所有信息传递到移动设备 15，这样将公司防火墙 22 有效地扩展到包括移动设备 100。

如图 1 所示，有很多可选路径用于从公司网络 30 到移动设备 100 获得信息。在该部分后面将讨论的一个到移动设备 100 的可能的获取信息的路径是使用接口或连接器 65 通过物理连接器 50 诸如串行口。该路径例如对在系统启动时经常执行的、或当移动设备 100 的用户工作在具有 LAN 30 20 的台式计算机系统诸如主计算机系统 35 时周期执行的大批信息更新时有用的。尽管在图 1 中仅示出了一个台式计算机系统 35，本领域技术人员将理解 LAN 将典型地包含很多台式、笔记本和膝上计算机系统。

另一种用于与移动设备 100 数据交换的方法是使用无线网络的无线方法。如图 1 所示，这能够涉及无线虚拟专用网络(VPN)路由器 75 (如果在网络 30 中可用的话)，或通过与提供到一个或多个无线网络诸如 105 和 110 接口的无线网关 85 的传统广域网(WAN)连接。无线 VPN 路由器 75 的概念在无线行业是新的，并且意味着 VPN 连接能够直接通过到无线设备 100 的特定无线网络 110 建立。使用无线 VPN 路由器的可能性仅是最近可行的，并且能够与静态寻址方案一起使用。例如，无线网络诸如 30 110 能够是基于 IP 的无线网络，其中新 IP 版本 6 (IPV6) 将提供足够的

IP 地址，以将一个 IP 地址专用于每个移动设备 100，并且这使得能够在任何时候将信息推送到移动设备 100。使用无线 VPN 路由器 75 的主要的优点是它能够是一个不需要单独的无线网关 85 的现成的 VPN 组件。VPN 连接最可能使用 TCP/IP 或用户数据报协议（UDP）/IP 连接将消息直接传递到移动设备 100。

如果无线 VPN 不可用，那么通常是互联网的到 WAN 20 的链路通常被用作连接机构。对于无线网络领域的技术人员，传递无线数据报到移动设备 100 的路径是公知的。为了处理移动设备 100 的寻址和任何其他需要的接口功能，最好使用无线网关 85。无线网关 85 也能确定最可能的网络 10 用于定位一给定的用户和当用户在国家或网络之间漫游时跟踪用户。在无线网络诸如 110 和 105 中，消息通常通过基站（未示出）和移动设备 100 之间的 RF 传输传递到移动设备 100 或从移动设备 100 传递。

图 1 还示出了一个离开电子邮件发送者 10 的编辑的电子邮件消息 15，位于 WAN 20 上的某个地方。该消息 15 完全是普通文字的，并且可使用 15 传统简单邮件传输协议（SMTP），RCF822 报头和 MIME 主体部分定义邮件消息的格式。这些技术对于本领域人员是公知的。在该环境中，消息 15 到达消息服务器 40 并且由无线连接器系统 45 转发到移动设备 100。当上述发生时，消息被重新封装到信封里如 80 指示的，并且对原始消息 15 应用压缩和加密算法。这样，在移动设备 100 上读到的消息与在台式计算机系统 35 上读到的一样安全。最好，系统 45 和移动设备 100 之间交换的所有消息最好使用该消息重打包技术。该外部信封（尽管不需要）的另一个目标是保持原始消息 15 的至少某些寻址信息。这允许答复消息到达合适的目的地，并且其允许“from（来自）”字段在其台式计算机系统 35 上反映移动设备用户的电子信箱帐户的电子邮件地址。使用用户的台式计算机系统，来自移动设备 100 的电子邮件地址允许接收的信息以似乎发自其桌上计算机系统 35 而不是移动设备 100 上的用户电子信箱帐户的消息出现。

回到与移动设备 100 的物理连接 50，该连接路径提供了很多优点，以实现一次多项数据交换。对于个人数字助理（PDA）和数据同步领域的 30 技术人员，个人信息管理（PIM）数据通常通过这样的连接进行交换，例

如串行端口，连接到合适的接口或连接器 65 诸如移动设备可放入或放上的一个支架。当第一次交换时，PIM 数据量趋于相对较大，并且需要大的带宽用于传送到移动设备 100。该物理连接 50 也能够用于其它用途，包括从用户桌上计算机系统 35 到用户移动设备 100 传送私有安全密钥（在此称为“私钥”）诸如在处理 S/MIME 消息中使用的移动设备用户私钥，用户数字证书（Cert）和任何链证书，及 CRL。例如，私钥可通过在用户移动连接到机算机系统 35 的鼠标或其它输入设备时收集光标位置信息来产生。然后私钥可通过物理连接 50 和接口或连接器 65 装到移动设备 100 上。

私钥交换允许用户桌上计算机系统 35 和移动设备 100 共享至少一个个性和方法用于访问所有加密的信件。用户桌上计算机系统 35 和移动设备 100 也能由此共享私钥，于是主系统 35 或移动设备 100 能够处理寻址到用户电子信箱帐户或桌上计算机系统 35 的安全消息。可能需要经过该物理连接 50 的证书和 CRL 的传送，因为它们代表用于 S/MIME、PGP 和其它公钥安全方法移动设备 100 需要的大量数据。证书经常是证书链的一部分，证书链包括用户证书和其它可能的证书以验证用户证书是可信的。在验证被签名消息上的签名时，消息接收者还将典型地获得用于消息的签名证书的证书链并且验证在该链中由链中的下个证书所签名的每个证书，直到发现证书由信任源、或许来自与证书权威（CA）诸如 VerisignTM 或 EntrustTM 例如在公钥密码术领域的两个著名公司相关的大型公钥服务器（PKS）的根证书签名。一旦发现这种根证书，签名应该被信任，因为发送者和接收者信任根证书源。

应理解，用户的自身证书或证书链以及那些用于其它用户的，可以从用户台式机算机系统装载到移动设备 100 上。如果用户证书或证书链是在移动设备 100 上，那么它能够连同在移动设备 100 上编辑的任何安全消息一起发送到接收者，以便每个接收者能够验证证书的信任状态。装载其它用户证书并且到移动设备 100 上的目的是允许移动设备用户选择其它实体或用户，他们可以与其交换安全消息，并且通过物理连接而不是无线将较大信息预装载到移动设备 100 上，这样当从这些其它用户接收安全消息或发送到这些其它用户安全消息时，节省时间和无线带宽。较大信息一般

是具有大字节尺寸的任何电子数据。装载 CRL 到移动设备也可以允许移动设备确定接收证书的状态。

再参照图 1，通常有到无线网络 110 和 105 的一系列连接。正如本领域技术人员将理解的，这些连接能够包括例如综合业务数字网络 (ISDN)，
5 帧中继或使用整个互联网中使用的 TCP/IP 协议的 T1 连接。这些网络能够代表不同的、唯一的和不相关的网络，或者它们能够代表在不同国家中的相同的网络。术语“无线网络”意指包括不同类型的网络，包括但不限于

(1) 数据为核心的无线网络，(2) 语音为核心的无线网络和(3) 能够支持在相同或类似物理基站上语音和数据通信二者的双模式网络。最新的这些网络包括但不限于(1) 码分多址 (CDMA) 网络，(2) 分组特殊移动或全球移动通信系统 (GSM) 和通用分组无线业务 (GPRS)，两者由
10 CEPT 标准委员会开发，和(3) 第三代 (3G) 网络象全球发展的增进型数据比率 (EDGE) 和通用移动电信系统 (UMTS)。GPRS 是在很普通的 GSM 无线网络的顶部的数据叠加，实际上运行于欧洲每个国家。某些老的数据为核心的网络包括但不限于：(1) Mobitex™ 无线网络 (“Mobitex”) 和(2) DataTAC™ 无线网络 (“DataTAC”)。老的语音为核心的数据
15 网络的例子包括个人通信系统 (PCS) 网络象 CDMA、GSM、时分多址 (TDMA) 系统。

现在回到图 2，示出了当前在互联网中通常使用的电子邮件交换的主要类型。我们首先具有电子邮件消息的正常交换 (方法 1)。在该情形中，
20 使用 RFC822、RFC821 和 MIME 技术创建电子邮件，并且使用标准 SMTP 电子邮件交换协议传递，如在 120 示出的。然后，接收电子邮件和给寻址用户，如 125 指示的。这种正常的电子邮件交换通常在位于安全防火墙
22 后面的公司或 LAN 诸如 30 内，但不在单机用户和/或不同网络上的用户之间是安全的。

另外通常使用的是 VPN 连接，用于办公室间消息交换 (方法 2)，
例如同一公司的分部办公室之间、某些时候一起工作很近的不同公司之间。使用该方法，低层安全称为 IP 安全 (IPSec) 可用于加密在两个 VPN 场所之间的交换的所有数据，如 130 指示的。当在相应的 VPN 系统处接

收到一个加密的电子邮件时，在 135 处它被解密成明文并且路由到寻址用户。

已经采用私用安全方案的不同公司或用户之间的电子邮件交换在图 2 中示为方法 3。在该情形中，在 140 处，诸如 PGP、OpenPGP 或某些其它 5 较少使用的协议的协议在电子邮件发送之前用于加密电子邮件。一旦被接收，在 145 处，相应的邮件代理解密电子邮件并且将明文呈现给接收者。

示于图 2 中的方法 4, 5, 6 和 7 涉及 S/MIME。这些方法是 S/MIME 的所有不同的变形。在方法 4 中，发送者提取电子邮件消息的摘要，并且使用发送者私钥签名摘要，如 150 处示出的。摘要例如可以通过对消息执行校验和、循环冗余校验 (CRC) 或某些其它优选的非可逆运算诸如散列，然后通过发送者使用发送者私钥签名。被签名的摘要很可能与发送者证书，并且可能任何链证书和 CRL 一起被附加到输出消息中。该签名消息的接收者还提取消息的摘要，将该摘要与附加到消息的摘要比较，通常通过从发送者证书中提取公钥检索发送者公钥，并且验证在附加的摘要上的 10 签名。这些操作是图 2 中在 155 处指示的签名验证部分。如果消息内容由于由发送者签名已经被改变，然后，摘要将不同或摘要上的签名将不合适地验证。这不防止任何人看到消息的内容，但是保证消息没有由于由发送者签名被篡改，并且消息由在消息的“From(来自)”字段上指示的人签名。 15 证书、证书链和 CRL 由接收者使用以保证发送者证书有效的，即，证书没有被注销、过期，并且是可信任的。在发送者处产生的摘要与在摘要上的签名的组合通常称为数字签名。此后，对数字签名的引用相应地应解释为包括摘要和摘要签名。

方法 5 代表 S/MIME 加密消息的交换。在该方法中，产生一次会话密钥，并且用来加密消息主体（典型地用对称密码如三倍数据加密标准 25 （3DES））。然后，在 160，使用消息的每个预计接收者的公钥加密会话密钥。会话密钥加密通常使用公钥加密算法诸如 Rivest Shamir Adelman(RSA)完成。S/MIME 消息包括加密的消息和会话密钥的所有加密版本被发送到每个接收者。然后每个接收者必须通常基于附加到消息的接收者的接收信息概要，查找其相应的加密会话密钥，并且使用其私钥解密 30 特别编码的会话密钥，如在 165 处指示的。一旦会话密钥被解密，其被用

于解密消息体。S/MIME 消息也可指定必须被用于解密消息的加密算法。该信息通常放置在 S/MIME 消息的首标中。

已经被加密然后签名的消息的交换在图 2 中作为方法 6 示出。按照该方案，发送者首先产生一次会话密钥，加密消息体，然后使用每个接收者的公钥加密会话密钥，如上所述。然后，在 170 处，发送者取消消息的摘要，包括加密的会话密钥，并且使用其私钥签名摘要，以产生数字签名。每个接收者取消消息的摘要，比较该摘要与附加到消息的数字签名中的摘要，检索发送者的公钥，并且验证摘要上的签名，如上所述。然后，找到正确的会话密钥，并且用接收者私钥解密，然后允许消息体被解密。按照该方法的签名验证和消息解密在图 2 的 175 处被示出。

图 2 中的方法 7 示出了已经签名然后加密的交换消息。在 180 处，基本上如上所述由发送者产生数字签名。该数字签名以及可能的发送者证书、证书链和 CRL 均附加到输出消息。然后，产生会话密钥，并且用来加密消息体，数字签名，和任何证书和 CRL。用每个接收者的公钥加密会话密钥。产生的 S/MIME 消息包括会话密钥的加密版本，被发送到接收者。当接收者接收到这样的消息时，如在 185 处所示，它必须首先用其私钥解密其相应的加密的会话密钥。然后使用该解密的会话密钥解密消息体，数字签名和消息发送者的任何证书和 CRL。然后，数字签名能够被验证，如上所述。

图 3 是支持安全和非安全电子邮件交换的系统组件方框图，用于与标准典型的非安全消息诸如基于互联网的电子邮件对比展示安全消息的某些一般特性和功能。在图 3 中，示例的公司网络 30a 和 30b 是位于各自的安全防火墙 22a 和 22b 后面的安全网络。尽管作为台式计算机系统 35a 和 35b 示出的网络 30a 和 30b 上的用户最好被启动用于与在下面进一步详细描述的网络之一上的其它用户系统安全消息传送，这样的用户系统通常也能与非安全系统诸如电子邮件发送者系统 12 通信。

当电子邮件发送者 12 发送电子邮件消息 15 到 LAN 30a 上的用户时，消息 15 通过 WAN 20(可以是最常用的互联网)，并且由在 LAN 30a 中的消息服务器 40a 接收。由于电子邮件消息发送者 12 是非安全的，电子邮件消息 15 将未被加密地正常传送到 LAN 30a 上的消息服务器 40。

在 LAN 30a 和 30b 上的用户之间的消息传递有些不同地进行，因为两个网络能够用于安全电子邮件通信。从 LAN 30a 到 LAN 30b 上的一个或多个用户发送电子邮件的用户假定他们能够使用 S/MIME 安全其电子邮件。电子邮件消息的发送者，例如使用台式计算机系统 35a，最好从多个编码方法中选择一个编码方法，为了便于示出，假定被签名的然后加密的 S/MIME。台式计算机系统 35a 或可能的消息服务器 40a 或更可能的在台式系统或服务器上执行的软件将产生用于电子邮件消息的数字签名，并且包括在输出消息中用于发送者的数字签名及可能的证书和 CRL。台式计算机系统 35a 或服务器 40a 然后将产生会话密钥，加密整个消息，从例如 PKS 600 中取出（或检索）用于每个接收者的公钥的复印件，并且加密用于每个接收者的会话密钥。PKS 600 最好是正常与 CA 相关的服务器，从 CA 可得到包括实体公钥的一个实体的证书。对本领域技术人员明显的是，PKS 能够驻留在公司防火墙 22a, 22b 或 WAN 20、互联网或其它网络（通过它消息发送者和接收者可以与 PKS 建立通信）上的任何地方。还应该明显的是，消息发送者不须总是取出或检索计划接收者的公钥，例如，接收者证书或公钥已经存储在发送者系统处的存储设备上。

在图 3 中作为 200 示出的经 WAN 20 传送到消息服务器 40b 的产生消息具有加密的涉及签名的信息组件 202，其可包括发送者证书、证书链、CRL 和数字签名、对应于在台式系统 35a 中编辑的原始电子邮件消息的加密消息体部分 204、和一个或多个加密的会话密钥 206。组件 202 和 204 使用会话密钥加密，其中，每个接收者的公钥用于加密会话密钥，如上所述。根据在 LAN 30a 和 30b 之间的特定安全消息方案，安全消息可包含与图 3 中所示出的不同的或附加的组件，或按不同顺序的相同或类似组件。当然，安全消息 200 还将包括至少一个目的地址和可能其它首标信息，该信息必须未被加密地留着，以提供到接收者的消息的路由。这种附加和/或不同的消息字段对本领域技术人员是明显的，它们在附图中没有明显显示出。

图 4 是表示接收的加密消息尺寸缩小的方框图。减少消息尺寸改善通过无线网络到移动设备的公钥加密消息的处理和传送。图 4 所示的系统包括能够用于安全电子邮件消息传送的电子邮件消息发送者 402，WAN 404

(其大部分情况下是互联网)，作为主场所例子的公司 LAN 406，无线网关 408，无线网络 410，和移动设备 412 和 414。图 4 中范例主场所是位于安全防火墙 403 后面的 LAN 406，并且包括：消息服务器 405，台式计算机系统 407，和运行在消息服务器 405 上或与其一起运行或作为消息服务器 405 的集成模块的无线连接器系统 409。下面将通过例子详细描述图 4 所示的系统的操作，其中，电子邮件消息在安全电子邮件发送者 402 处编辑并且发送到用户 A 和 B，每个用户是移动设备 412 或 414 及主场所处即 LAN 406 上的主台式计算机系统 407 的用户，只示出了他们中的一个。

如图 4 所示，电子邮件发送者 402 编辑电子邮件消息，该消息至少包括指向用户 A 和 B 的目的地址和电子文本。在该例中，基本如上所述，电子邮件消息使用由电子邮件发送者 402 选择的一次会话密钥加密电子邮件消息。电子邮件发送者 402 然后使用每个电子邮件接收者即用户 A 和 B 的公钥，加密会话密钥。也如同以上所述的，公钥可以从本地存储区、配置电子邮件发送器系统 402 运行的网络（未示出）内的 PKS 驻留、或 WAN 404 或电子邮件发送者 402 可与其通信的其它网络上的 PKS 驻留中检索。在该例子中，PKS 的位置和公钥的位置不重要。该系统不依赖于在电子邮件消息发送者诸如 402 处的任何特定密钥管理方案。

安全消息 416，包括加密消息 418 和所有接收者的会话密钥 420、422 的加密版本，通过 WAN 404 发送到消息服务器 405 上的接收者地址。应理解，在 416 示出的消息组件表示直接涉及系统的那些组件。由电子邮件消息发送者诸如 402 发送的消息可包括附加的组件，或可以与所示出的不同次序包括在 416 示出的组件，不影响与系统的该方面相关的操作。

当可能通过主场所并且连到 WAN 404 的一个或多个其它计算机系统（未示出）在消息服务器 405 接收到消息时，无线连接器系统 409 检测安全和加密的消息。系统 409 还确定用户 A 和 B 具有相关的移动设备 412、414，接收的安全消息应该通过无线网络发送到移动设备 412、414。

按照该方面，系统 409 通过去除（remove）每个个别的用户移动设备 100 不需要的任何加密的会话密钥减少消息的尺寸。例如 S/MIME 消息包括接收者信息列表，该列表提供关于哪个加密的会话密钥对应于在消息的

To, Cc 或 Bcc 字段中的每个接收者的图。因此，系统 409 可以咨询接收者信息列表，以确定哪些加密的会话密钥应该发送到每个接收者。

如图 4 所示，系统 409 检测寻址到用户 A 和用户 B 二者的接收的消息 416，并且将消息 416 的修改的复制件发送到每个用户的移动设备。发送到用户 A 的移动设备 412 的消息更详细地示于 424，并且包括加密的消息体 418，和使用用户 A 的公钥加密的仅一个加密会话密钥 420。不能由用户 A 使用的用户 B 的加密会话密钥 422 由系统 409 从发送到移动设备 412 的消息去除。类似地，系统 409 从接收的加密消息中去除计划用于用户 A 的加密会话密钥 420，并且发送到移动设备 404 一个产生的消息，该消息包括加密消息体 418 和用于用户 B 的加密会话密钥，如 426 示出的。

由于每个用户接收其相应的加密会话密钥作为安全消息的部分，安全消息能够在每个设备 412, 414 得到处理，即使由电子邮件发送者 402 发送的原始安全消息 416 中的其它信息已经由系统 409 除去。加密的会话密钥能够使用驻留在移动设备上的每个用户的各自的私钥在每个移动设备 412, 414 上得到解密，并且然后用于解密消息体。如上所述，用户私钥例如可以从用户台式计算机系统诸如 407 通过物理连接(在图 4 中未示出)传送到用户移动设备。在解密消息体之后，移动设备 上的用户接口能够在设备的显示器上呈现未加密的消息。通过如上所述重新组织原始的消息，会话密钥的所有不必要的加密版本从原始消息中去除，由此减少了通过无线网络发送到移动设备的消息的尺寸。对于 S/MIME 消息，由于移动设备只接收其会话密钥的相应的加密版本，接收信息列表不需要，并且也可以去除，进一步减少了消息尺寸。由于会话密钥的加密版本的数目和接收信息列表的尺寸随着原始消息中接收者的数目增加，对于具有大量接收者的原始消息来说消息尺寸减少能够是特别有效的。

尽管图 4 中所示的范例系统包括安全防火墙 403 之后的公司 LAN 406 内的消息服务器 405 和系统 409，该系统还可应用于其它类型的系统，例如移动设备用户具有直接或例如通过 ISP 连接到互联网的计算机系统。在该情况下，台式计算机系统实现无线连接器系统，最好作为用运行在台式计算机系统上的电子消息程序运行的无线连接器系统的台式版本。电子消息程序的例子包括，但不限于，MS Outlook, Lotus Notes, 和 Eudora。这

些程序可以通过包括 POP 的一个或多个装置访问存储在第一数据存储设备（不位于台式机算机上）上的邮件。带有电子消息程序的基于台式的无线连接器通过无线网络 410 发送接收的消息到用户移动设备，并且执行上述的消息尺寸减少操作。

5 图 5 是接收签名的消息尺寸减少的方框图。图 5 中所示的整个系统类似于图 4 的系统，在图 5 中的系统组件基本上与图 4 中类似标出的组件相同，尽管其操作稍微不同，如下面将描述的。

为了图示，假定从系统 502 发送电子邮件消息到用户 A 和 B 二者的用户要签名消息，使得用户 A 和 B 可以确认发送者是消息的真正发送者，
10 并且所接收的是由发送者发送的。为了允许消息接收者确认发送者签名是可信任的，电子邮件发送者 502 正常附加它们的证书、在证书链中的任何其他证书，和可能当前的 CRL。从电子邮件发送者 502 发送的安全消息于是可以具有如 516 示出的形式，包括发送者证书、证书链、CRL 和数字签名 518 和消息体 520。在 S/MIME 中，证书、链、CRL 和签名通常放置在
15 消息体的开始，如图 5 所示。按照其它安全消息方案的消息可以以如所示出的不同的次序放置消息组件，或包括附加和/或不同的组件。

安全消息诸如 516 将通常通过 WAN 504 诸如互联网被发送到寻址的接收者。在图 5 中，消息被寻址到仅两个接收者，两个接收者中的每个具有与相同的消息服务器 505 相关的电子信箱帐户，尽管该系统不限于此。
20 图 5 中的范例系统仅是一个系统例子，并且打算仅用于展示。

一旦被消息服务器 505 接收，安全消息就被路由到在服务器 505 上的每个接收者电子邮件帐户。无线连接器系统 509 检测新消息，并且还确定是否该消息应该通过无线网络发送到任何接收者的移动设备。如果这样，然后系统 509 重新组织消息：首先放置消息体，随后是数字签名，然后是证书、证书链和 CRL。然后证书、证书链和 CRL 最好由主系统的系统 509 存储。包括至少消息体和数字签名的消息然后通过无线网络发送到接收者用户 A 和 B 的移动设备 512 和 514，如在 522 和 526 示出的。数字签名 524，
25 528 有效地是原始消息、证书、证书链和 CRL 组件 518 的截取形式。尽管在消息 522 和 526 中不同地标出，签名 524 和 528 实际上是由电子邮件发送者 502 产生的相同的签名。证书、证书链和 CRL 不与消息体和签名一

起初始发送到移动设备 512, 514, 这基于假定证书和 CRL 例如使用到用户台式计算机系统 511, 513 的物理连接 515, 517 可以已经预装载到所述设备的存储设备上。发送者证书和证书链可以已经附加到通过无线网络发送到移动设备 512, 514 并且随后存储在移动设备上的先前安全消息，这 5 也是可能的。最新的 CRL 可以类似地已经在移动设备 512, 514 上存在。在这些情况下，证书、证书链和 CRL 将在移动设备 512, 514 上不被使用即使它们被发送。如果需要这些任何信息但在移动设备 512, 514 上没有，然后可以从无线连接器系统 509 请求。

如上所述，用户可以看签名消息的内容不用首先验证签名。证书、证书链和 CRL 仅当移动设备用户例如用户 A 希望验证来自电子邮件发送者 502 的消息上的签名 524 时需要。如果这些部分在移动设备 512 上存在，那么可以完成签名验证操作不用移动设备 512 和 LAN 506 之间的进一步通信。然而，如果这些证书和 CRL 信息对于从其接收签名消息的消息发送者不有效，那么按照系统的另一方面，用户然后给系统 509 提交一个请求：发送原始消息的剩余部分，特别地在消息由系统 509 通过无线网络 510 发送到移动设备并且存储在主场所（LAN 506）之前去除的任何证书和 CRL。一旦在移动设备 512 处接收到证书和 CRL 就允许签名被全部检验和验证。

相对较大的（即大字节尺寸的电子数据）证书和 CRL 在被发送到移动设备之前从接收的签名消息中的去除能够大大减少通过无线网络 510 发送的签名消息的尺寸，由此保留了无线网络资源，减少了需要发送签名消息到移动设备需要的带宽和时间。

在系统的该方面的另一实施例中，用户主系统 511, 513 包括图 6 中进一步详细示出的证书同步系统，图 6 是基于存储在移动设备上的信息减少签名消息尺寸的系统的方框图。在图 6 中，由于避免附图中的拥挤，无线连接器系统运行的主系统场所外的系统组件没有被示出。为了清楚，消息服务器和主计算机系统之间的连接也已经被省去。然而，明显的是，图 6 中所示的系统可以包括如在消息系统公共的那些组件和连接。

图 6 中的范例系统包括：消息服务器 602，无线连接器系统 604 和两个台式计算机系统 606, 614。每个台式计算机系统包括物理连接 608, 616，

通过该连接，证书、CRL 和可能其它相对较大的信息可被传送到用户移动设备（未示出）。按照系统的该实施例，每个台式计算机系统 606, 614 包括证书同步（sync）系统 610, 618，其在大部分方案中将是一软件应用程序。证书同步系统 610, 618 与在主计算机系统 606, 614 上的物理连接 608, 616 和数据存储器 612, 620 连接。如本领域技术人员将理解的，数据存储器 612, 620 能够是任何存储介质，例如包括本地硬盘驱动器和其它存储器单元。也期望是公共信息的证书和 CRL 能够在例如网络内的计算机系统之间共享，这样存储器 612, 620 实际是例如在网络文件服务器上的相同的数据存储器。

10 使用证书同步系统 610，当移动设备通过连接 608 连接到台式计算机系统时，用户 A 最好选择并传送证书和可能的 CRL（如果需要的话）到他或她的移动设备。然而，由于 CRL 趋向于较大，于是需要相当大的存储器资源用于存储，用户将最可能经常只传送证书到移动设备。然后证书同步系统被配置以咨询一相应的 CRL，保证在证书被传送到移动设备之前，证书没有被注销，或可选的从用于下载的证书列表中去除任何注销的证书。在一个设备中，证书能够被存储到数据存储器诸如随机访问存储器（RAM）、快闪存储器或数据可以被写到移动设备上的其它这些存储器组件。

如图 6 所示，每个证书同步系统 610, 618 也能够用于与无线连接器系统 604 通信。这允许证书同步系统告诉无线连接器系统哪些证书已经装到用户移动设备上。这例如通过每次使用证书同步系统执行任何设备相关的操作传送在设备上所有证书的全部最新列表或证书添加和删除列表来完成。任何时候当移动设备连接到其台式计算机系统时，由证书同步系统在移动设备上检测新证书时，证书更新也能够被发送到无线连接器系统 604。尽管证书同步系统对于装载移动设备用户希望从其接收签名的消息的实体的特别证书是有用的，可能有这种情形，移动设备用户从其它源诸如 CA 获得证书。在该情况下，也能配置证书同步系统确定自从使用证书同步系统的最后证书传送时起，是否任何证书已经装载到移动设备上，并且，如果这样，传送设备证书更新到无线连接器系统 604。

当从台式计算机系统 606, 614 接收到这样的设备证书更新时，在数据存储器 622 中由无线连接器系统 604 为特定用户保持的用户配置文件 (profile) 被更新。尽管用户配置文件 624, 626 可包括这些信息诸如用户姓名、控制哪些信息经无线网络发送的配置设定、移动设备标识信息和可能进一步的用户配置或移动设备相关信息，无线连接器系统 604 最好还存储在用户移动设备上的证书列表。在图 6 所示的例子中，用户 A 的移动设备在其移动设备上存储实体 X 的证书，如由[证书 X]表示的，而用户 B 在其移动设备上已经存储了实体 Y 的证书，[证书 Y]。在用户配置文件 624, 626 中示出的单个证书仅用于示出；移动设备最好具有足够的存储器资源以存储多个证书。

当包括证书、证书链 CRL 和数字签名组件 630 和消息体 632 的签名消息 628 到达消息服务器 602 时，如上所述由无线连接器系统 604 检测。然后，重新安排原始消息，以便首先放置消息体，随后为数字签名和签名相关的信息。按照系统的该实施例，然后无线连接器系统 604 通过咨询用于每个寻址的移动设备用户的用户配置文件确定消息将被发送到的每个移动设备是否需要签名相关的信息。由于发送者的证书，证书 X 已经存储到用户 A 的移动设备，仅包括消息体 632 和数字签名 636 的重新安排的消息 634 发送到用户 A 的移动设备。尽管实体 Y 的证书已经存储到用户 B 的移动设备上，用于原始消息 628 的发送者的证书 X 在用户 B 的移动设备上无效，这样，给用户 B 移动设备的重新安排的信息包括消息体 632 和签名相关信息以及数字签名组件 630。如上，无线连接器系统 604 可改为存储签名相关信息用于后面传送到用户 B 的移动设备，并且初始只发送消息体和数字签名。

证书同步系统 610, 618 和对无线连接器系统 604 的设备签名相关信息的使用允许无线连接器系统 604 确定特定的移动设备需要的信息，并且从发送到移动设备的消息去除任何不必要的信息。代替假定移动设备可能已经存储一个证书如在前面的实施例中，无线连接器系统 604 能够确定是否设备已经存储了证书。用户配置文件也可能用于指定其它配置设定，例如指示 CRL 应从来没有发送到用户移动设备或仅当被请求签名相关信息应仅被发送到用户移动设备。

现在参考图 7 和 8，首先执行消息签名或加密以产生签名和加密的消息的作用将被讨论。当首先加密然后签名一个消息时，能够应用一套重新组织和/或消息缩小方案。当消息首先被签名然后加密时，其它重新组织和尺寸缩小的技术是可用的。正如将明显的，只有消息系统的主场所部分 5 (消息服务器和无线连接器系统) 示于图 7 和 8 的每一个中。

图 7 是用于已经加密然后签名的接收消息的安全消息尺寸缩小的方框图。这样一个消息 706 将典型包括使用发送者建立的一次会话密钥加密的消息体 710。使用每个所需消息接收者的公钥加密会话密钥，在该例子 10 中是用户 A 和 B，以产生用于每个用户的加密会话密钥 712, 714。加密的消息体 710 和加密的会话密钥 712, 714 然后基本如上所述被签名。尽管在加密之后执行签名，除了数字签名带有证书、可能证书链和一个或多个 CRL 的消息组件 708 例如可以在安全消息的开始，正如在 S/MIME 中。

带有会话密钥 712, 714 和数字签名和签名相关信息 708 的该加密和签名消息 706 由消息服务器 702 接收，该服务器处理该消息并且将其放在 15 用于用户 A 和 B 的合适的信箱。无线连接器系统 704 检测新消息并且开始该处理以便发送消息到具有移动设备的每个接收者。在消息发送到移动设备之前，消息的数字签名和证书部分 708 最好至少重新安排，使得数字签名和签名相关信息移到消息末端。由于加密的消息体 710 和会话密钥 712, 714 均被签名，只有签名和签名相关信息能够被重新排列或从消息 20 中去除。如果无线连接器系统 704 在发送消息到移动设备之前，处理消息 706 以重新安排或去除任何被签名的组件，签名验证将在移动设备失败。

如上所述，无线连接器系统 704 可以去除证书、以及任何证书链和 CRL (如果包括在消息 706 中)，并且存储这些部分以便后面传送到移动设备。无线连接器系统 704 能够确定哪些证书在寻址的接收者移动设备上 25 是存在的，仅当在移动设备上没有时，证书能够被发送。在图 7 中所示的例子中，只有数字签名 718 和原始消息 706 的签名组件 710, 712, 714 被发送在消息 716 中给以用户 A。这将发生在当在一接收消息被发送之前所有签名相关信息被去除，或当无线连接器系统 704 检测到在原始消息 706 中的发送者证书已经装到用户 A 的移动设备上时。在用户 B 的情况下， 30 例如如果无线连接器系统 704 确定原始消息 706 中的证书还没有装载到用

户 B 的移动设备，证书和数字签名 722 二者连同在消息 720 中的签名组件 710, 712, 714 发送到用户 B 的移动设备。

因此，当一安全消息被加密然后签名时，数字签名和任何签名相关信息可被重新安排到消息的末端，并且某些或所有签名相关信息可以从消息中被去除。
5

图 8 是用于已经签名然后加密的接收消息的安全消息尺寸减少的方框图。在该情况下，发送者产生用于编辑的消息的数字签名并且将数字签名、证书和可能的证书链和 CRL 附加到消息的起始处。对于 S/MIME 消息，数字签名、证书和任何成链的证书和 CRL 被附加到消息的开始。如 10 上所述，然后使用一次会话密钥加密全部签名的消息，并且使用每个接收者的公钥为在消息中寻址的每个接收者加密会话密钥。产生的消息在 806 处示出，其包括数字签名和签名相关信息 808 以及消息体 810，二者使用会话密钥加密，后面跟随用于每个接收者的会话密钥 812, 814 的加密版本。

15 当消息服务器 802 接收了签名并加密的消息 806 并且放进用户 A 和 B 的合适的信箱时，无线连接器系统 804 检测该新消息，并且确定是否任何寻址的消息接收者具有一移动设备（未示出）以及是否消息将发送到移动设备。如果这样，那么准备消息用于发送到每个移动设备，该消息包括原始接收消息的加密部分和对应于移动设备的唯一特定会话密钥。在图 8 20 中，数字签名和签名相关信息 808 被加密，由此无线连接器系统 804 不能识别和重新安排。因此，由无线连接器系统 804 发送到用户 A 和 B 的移动设备的消息 816, 818 中的每个包括加密的数字签名和签名相关信息 808 及原始消息的签名和加密消息体 810 及用于移动设备的唯一各个加密会话密钥 812, 814。在每个移动设备，会话密钥能够被解密并且用于解密 25 消息的加密部分 808, 810 以暴露原始消息体，数字签名和签名相关信息组件。该消息然后可以被观看，并且数字签名验证能够在每个移动设备上进行。

如上所述，当无线连接器系统 804 只发送需要的加密会话密钥给每个移动设备时，接收信息字段（未示出）也可以从加密的消息去除，以进一步减少经无线网络发送的消息的尺寸。
30

如上所述的系统的实施例集中在安全消息发送到移动设备之前重新安排和减少安全消息尺寸上。现在将描述提供不同的方法预处理消息减少必须经无线传送到移动设备的数据的几个另外的实施例。消息预处理的一个优点是可选的技术可应用到签名和加密的消息，这些消息是重新安排以减少尺寸的最困难的消息，正如从前面描述明显看出的。
5

图 9 是展示加密消息预处理系统的方框图。整个系统类似于上述的系统，图 9 中所示的组件实际上与前面图中类似标出的组件相同。如在 916 处示出的，寻址到用户 A 和 B 的来自电子邮件发送者 902 的加密电子消息包括加密消息体 918，和两个加密会话密钥 920 和 922。正如对本领域技术人员明显的是，加密消息 918 的部分不需要必须是图 9 所示的次序。在该例中，假定用户的台式计算机系统（在 907 处示出的之一）和用户移动设备 912 或 914 有效共享共同的地址、由无线连接器系统 909 支持的特征。然而，在某些系统中，消息可寻址到在消息服务器 905 上的用户信件帐户和用户无线信件帐户。当无线连接器系统 909 被实现时，很可能消息将被寻址到消息服务器 905 上的用户帐户。
10
15

在系统的优选实施例中，例如使用图 1 中所示的物理连接 50 和接口 65 或某些其它信任的有线或无线传送机构，通过将私钥装载到移动设备，能够在用户台式计算机系统 907 和移动设备 912, 914 之间共享单个私钥。如果用户台式计算机系统 907 被配置与智能卡或类似可去除安全使能组件操作，由用户通过将其智能卡插入读卡机并且运行无线连接器系统 909 的组件，和/或有可能台式计算机系统 907 上的软件组件，以将私钥从读卡机直接装进移动设备的存储器，能够执行该私钥装载。或者，读卡机能够集成到移动设备，以允许用户使用台式计算机系统或移动设备访问私钥。该共享的私钥在两个场所即用户台式计算机系统 907 和移动设备 912 或 914 提供镜像电子邮件存储。
20
25

当由发送者 902 发送消息 916 时，最终通过 WAN 904 路由到消息服务器 905 用于处理和转发到寻址的接收者用户 A 和 B 的电子邮件帐户。无线连接器系统 909 检测新的信息并且确定是否应该将其发送到任何接收者的移动设备。按照该系统的一个方面，对于消息将被发送到移动设备的每个接收者，无线连接器系统 909 使用会话密钥解密消息，并且使用不
30

同的密钥和可能的对应于在无线连接器系统 909 和其相关移动设备 912, 914 之间实现的无线友好安全方案的不同的加密算法, 重新加密消息, 然后将重新加密的消息发送到接收者的移动设备。该重新加密的消息示于 924 和 926。

5 由于会话密钥的每个版本用特定移动设备 912, 914 的特定公钥加密, 无线连接器系统 909 必须在消息体能够被解密和重新加密之前设法解密会话密钥。在系统的该方面的一个实施例中, 无线连接器系统 909 为接收的消息将被发送到的每个移动设备 912, 914 提取正确的会话密钥 920, 922, 并且将其发送到每个移动设备。例如, 在为移动设备用户诸如用户
10 A 提取正确的加密会话密钥之后, 无线连接器系统 909 可建立只含有加密的会话密钥 920 的消息。移动设备 912 接收该消息并且从消息提取会话密钥 920。会话密钥然后被解密, 最好按照上述无线友好安全方案重新加密, 并且发送回到无线连接器系统 909。无线连接器系统 909 然后解密该重新加密的会话密钥, 并且使用解密的会话密钥代表用户 A 解密加密的消息
15 体。然后, 解密的消息体能够按照无线友好安全方案被重新加密, 并且发送到移动设备 912。然后, 该重新加密的消息可在移动设备 912 被解密并且显示给用户 A。在无线连接器系统 909 和接收的加密消息将发送到的每个移动设备之间将执行类似的过程。

无线连接器系统 909 的该消息解密减少了必须在移动设备上执行的
20 复杂公钥解密操作的量。此外, 在很大的电子邮件消息的情况下, 这允许无线连接器系统 909 只发送消息的部分到每个移动设备。尽管上述的会话密钥和消息交换对于每个用户能够重复, 一旦会话密钥由一个移动设备解密并且返回到无线连接器系统 909, 然后解密的消息体能够被重新加密用于消息将被发送到的每个移动设备。这能够简化在无线连接器系统 909 处的操作, 因为加密的消息体仅被解密一次, 即使当消息被发送到多个移动设备时, 并且还导致对某些移动设备的快速的消息传送, 因为与重新加密的会话密钥的响应只须由无线连接器系统 909 从一个移动设备而不是从消息将被发送到的每个移动设备接收。

在某些系统中, 其中台式计算机系统诸如 907 和移动设备共享一公共
30 私钥, 私钥对于消息服务器 905 和无线连接器系统 909 是可访问的。尽管

根据私钥技术的发展，这可能是一种不可能的情形，该方法具有减少在加密消息的解密和传送过程中的步骤数目，并且还去除了经无线发送解密的会话密钥的需要的优点。正如在前面实施例中，由无线连接器系统 909 的消息解密减少了移动设备必须执行的公钥操作的数目。

5 按照该系统的该实施例，无线连接器系统 909 能够访问设有无线通信服务的任何寻址的接收者的私钥。代替如在先前实施例中直接发送加密的会话密钥到移动设备，无线连接器系统使用与设备共享的私钥，以解密会话密钥。然后，使用该会话密钥解密加密的消息体。例如对于用户 A，无线连接器系统 909 将从消息 916 中提取加密的会话密钥 920，使用用户 A 10 的私钥解密会话密钥，并且使用该会话密钥解密加密的消息体 918。基本如上所述，一旦消息体被解密，其被使用无线友好加密方法重新加密，并且发送到合适的移动设备。然后移动设备解密消息，并且将其以原始形式呈现给用户。该过程在移动设备上用最少量的公钥操作提供了最快的消息传递时间，这趋向于处理器功能的增强和功率增强。

15 很明显的是，由无线连接器系统 909 进行加密消息的解密和重新加密将通常表示对安全的关注。然而，在图 9 所示的系统中，解密和重新加密在安全防火墙之后被执行，并且因此，解密信息保持如在公司 LAN 906 中任何其他信息的安全性。当在无线连接器系统 909 和移动设备 912, 914 20 之间使用强加密方案诸如 3DES 时，任何先前解密的信息包括解密的消息或会话密钥，在无线连接器系统 909 和移动设备 912, 914 之间传送的同时，保持安全。

图 10 是签名消息预处理系统的方框图。在图 10 中的系统类似于图 9 中的系统，图 9 和 10 中类似标出的组件实际上是类似的，尽管图 10 的系统预处理签名的消息。在图 10 中，数字签名验证代表移动设备用户在用户主系统场所（LAN 1006）执行，于是节省了数字签名并且典型的较大签名相关数据的传送。

25 由电子邮件消息发送者 1002 签名的消息 1016 将包括数字签名部分 1018 和消息体部分 1020，如上所述。当签名消息 1016 由消息服务器 1005 接收并且转发到合适的信箱时，无线连接器系统 1009 检测新消息，并且

确定是否它应该发送到一个或多个移动设备。在图 10 中的例子中，消息应被发送到二个移动设备 1012 和 1014。

然后无线连接器系统 1009 检测已经签名的消息，并且设法找出发送者的公钥。该公钥能够从本地存储区或可能从 WAN 1004 上某个地方的 5 PKS 1028 被检索。一旦检索到发送者公钥，由无线连接器系统 1009 代表每个移动设备用户验证数字签名。然后消息被准备和转发到每个移动设备 1012, 1014，该消息最好包括指示是否已经验证数字签名。如在 1024, 1025 和 1026, 1027 中所示的，原始消息体 1020 和签名指示在发送到移动设备 1012 和 1014 之前为了安全被重新加信封和可能加密。尽管签名指示 10 不必要是保密的，其加密防止非授权方插入错误的签名指示或改变签名指示。在每个设备，外部信封被去除，并且消息和签名指示如果需要在被呈现给用户之前被解密。

图 11 是用于已经加密然后签名的接收消息的安全消息预处理的方框图。为了避免图中的拥挤，只示出了消息服务器 1102 和无线连接器系统 15 104。对本领域技术人员明显的是，这些组件能够在诸如在先前附图中示出的系统中实现。

已经加密然后签名的安全消息 1106 可包括这些构成部分如数字签名和签名相关信息部分 1108，加密和签名的消息体 1110 及加密和签名的会话密钥 1112 和 1114。这些信息的产生上面已经详细描述了。当这样的信息在消息服务器 1102 处接收并且分布给用户 A 和 B 的合适的用户信箱时，20 无线连接器系统 1104 检测新消息，并且在该例中确定消息将被发送到用户 A 和 B 中的每一个的移动设备。由于消息已经被签名和加密，消息的预处理包括联系图 9 和 10 如上所述的每个预处理方案的几个步骤。

消息 1106 已经首先被加密然后签名，这样，无线连接器系统 1104 最好使用发送者公钥首先验证签名。该密钥可从本地存储器或例如通过 PKS 25 检索。发送者数字签名无论是否被验证，预处理可进行以获得用于加密消息的会话密钥。如上所述，这可由无线连接器系统 1104 通过发送到移动设备一个会话密钥的相应版本，或如果设备的私钥对于无线连接器系统 1104 是可访问的，通过访问私钥和解密会话密钥，来完成。一旦会话密钥 30 通过连接器系统 1104 解密或返回到无线连接器系统 1104，消息能够被

解密。然后解密的消息，和最好消息被签名和数字签名是否已经被验证的签名指示，使用无线友好加密算法被重新加密和发送到消息将被发送到的每个移动设备。如在 1116 和 1122 处指示的，发送给用户 A 和 B 的移动设备的消息包括消息体 1118，1124 和签名指示 1120，1126，二者最好被
5 加密。然后每个移动设备能够解密消息 1116，1122 及将消息和签名指示呈现给移动设备用户。

图 12 是类似于图 11 的方框图，但是示出了用于已经签名然后加密的接收消息的安全消息预处理。如在图 11 中，只有消息服务器 1202 和无线连接器系统 1204 示于图 12 中以避免拥挤。然而，应理解，在图 12 中的安排将通常被实现为能够进行电子消息交换、例如图 11 示出的较大系统的一部分。
10

如上所述，并且在 1206 中示出的签名然后加密的消息典型地包括数字签名和签名相关信息组件 1208 和消息体部分 1210，二者由发送者使用一次会话密钥、以及用于每个寻址的消息 1206 接收者（该例中用户 A 和
15 B）的会话密钥 1212，1214 的加密版本加密。当消息 1206 由消息服务器 1202 接收并且分配给合适的用户信箱时，无线连接器系统 1206 检测新消息并且检测消息将发送到哪个移动设备（如果有的话）。

因为消息 1206 已经首先签名然后加密，无线连接器系统 1204 必须在任何进一步预处理能够执行之前首先解密消息。为此，无线连接器系统
20 1204 获得会话密钥，其如上所述通过发送相应的各加密会话密钥到移动设备用于解密或通过访问用户私钥和解密会话密钥可以完成。一旦会话密钥已经返回到无线连接器系统 1204 或由无线连接器系统 1204 解密，消息 1206 能够被解密并且数字签名和签名相关信息被提取。如上所述，然后通过检索发送者的公钥能够检验数字签名。然后产生签名指示并且附加到
25 消息体。然后最好使用无线友好加密方法加密消息和指示并且传送到消息将发送到的每个移动设备。如在 1216 和 1222 示出的，到移动设备的消息包括消息体 1218，1224 和消息已经被签名和是否已经验证数字签名的指示 1220，1226。在移动设备，发送的消息被解密以检索原始消息和签名指示。

图 13 和 14 示出了用于在将签名、加密或签名和加密的消息发送到移动设备之前进行预处理的方法流程图。在这些附图中，假定，消息已经被接收并且放进消息存储位置和无线连接器系统已经检测到新消息。应该明显的是，图 13 和 14 所示的方法应用到无线连接器系统所确定的应该处理的那些消息，即要发送到一个或多个移动设备的消息。
5

现在转到图 13，该方法开始于步骤 1300，当要发送到移动设备的消息从消息发送者到达时。在步骤 1305，然后无线连接器系统检验消息是否是明文的。该检验例如通过检验消息的 MIME 类型和/或寻找带有一定格式和 MIME 类型的附件来执行。如果消息是明文的，则它被路由到每个移动设备。如果消息不是明文的，然后在步骤 1315，执行检验以确定消息是否已经被签名但没有加密（即只签名）或最后签名。如果消息不是仅签名或最后签名，这将意味着消息可能已经被加密但没有签名（只加密）或先签名和最后加密，并且加密将必须首先被处理。在步骤 1320，执行确定是否消息只加密或最后加密。如果确定消息没有只加密或最后加密，
10 那么消息可能是在步骤 1305 或 1315 没有检测到的明文消息或只签名或最后签名的消息，或消息具有无线连接器系统不能处理的格式。在这些情况的任何一种中，错误可能已经出现，如在 1325 指示的。如本领域技术人员将理解的，错误处理将取决于实现该方法的系统。如果消息只加密或最后加密，方法进行到在步骤 1330 的处理加密，其在图 14 中详细示出并且
15 下面描述。
20

如果消息已经仅签名或最后签名，如在步骤 1315 中确定的，那么如上所述，在步骤 1340 产生消息的摘要。然后在 1345 检测附加到消息的数字签名。为了继续数字签名验证，在步骤 1350 从本地存储器、从 PKS 或类似系统或可能从附加到原始消息例如包括在消息的签名者信息
25 （SignerInfo）部分中的证书检索发送者公钥。在步骤 1355，使用发送者公钥，提取在被检测数字签名中的摘要并且验证摘要上的签名。

然后，在步骤 1360 比较摘要 A 和 B，以确定是否它们匹配。还确定摘要的签名是否被验证。如果这两种情况中的一个不满足，那么签名没有被验证，并且在步骤 1365，“失败”等签名指示将被附加到消息。如果

两个条件均满足，那么签名得到合适的验证，及在步骤 1370 “已验证”或类似签名指示被添加到消息。

在步骤 1375，确定消息是否仍然被加密。如果仍然被加密，对于被加密然后签名的消息，该方法在步骤 1380 继续，以处理加密的数据，如图 14 所示，并且下面进一步详细描述。如果消息仍然没有被加密，那么在步骤 1385 进行检验以确定是否它已经被加密。对于首先签名最后加密的消息，消息解密在签名验证之前已经被完成。如果它已经被加密，那么在步骤 1395 构建一个消息并且发送到移动设备，该消息包括合适的签名指示、指示消息已经原始被加密的加密指示或标记和消息体。否则，在步骤 1390 发送到移动设备的消息包括签名指示和消息体。或者，如果移动设备用户不需要知道消息是否被原始加密，它将是存储在由无线连接器系统可访问的用户配置文件中的配置设定，步骤 1375 能够直接进行到步骤 1390 并且没有加密指示被发送。

尽管在图 13 中没有示出，在预处理安全消息发送到移动设备之前上述的编码、压缩和加密方案可由无线连接器系统作为步骤 1390 和 1395 的部分采用。

现在转到图 14，示出了与消息的加密部分的处理相关的方法步骤。加密处理可以在消息已经被最后加密或仅加密时（步骤 1330）或当对于一个加密然后签名的消息已经完成签名验证操作时（步骤 1380）开始。

在步骤 1410，通过例如使用接收的消息的接收者信息（RecipientInfo）字段，在处理加密数据中的第一步将定位用于特定移动设备用户的加密会话密钥。在下面步骤 1415，无线连接器系统如上所述产生并且向移动设备发送包含加密的会话密钥的消息。该消息可具有为用户提供这些关于消息的信息如消息的大小、日期和发起者，带有一个消息被加密的指示的文本。当在移动设备处接收该消息时，在步骤 1425，例如通过在移动设备上的安全消息软件应用，确定能够被用于解密会话密钥的私钥是否在设备上存在。如果该设备不具有正确的私钥或用户不想解密该消息，那么不能由用户在移动设备上察看消息。否则，作为可选的步骤 1435，例如，通过在移动设备的信息列表中的菜单可给予用户解密会话密钥的选择（步

骤 1435）。然后，在步骤 1440，解密的会话密钥被传回无线连接器系统和原始消息被解密。

一旦完成解密，在步骤 1445 执行测试，以确定是否将验证数字签名。如果是，该方法在步骤 1450 进行以参照图 13 如上所述处理数字签名。如果 5 没有数字签名将被验证，那么在步骤 1455 执行进一步的测试，以确定是否已经处理数字签名。如果已经处理数字签名，即当在步骤 1380 开始加密处理时，在步骤 1460，具有签名指示和可能如上所述的加密指示的解密的消息被发送到移动设备。否则，如果消息没有被签名，那么如在步骤 1465 示出的，解密的消息和可能一个加密指示发送到移动设备。

10 图 13 和 14 中示出的流程图打算用于图示目的，并且不限制该系统的范围。在流程图中概括的步骤可以不同的次序执行，某些步骤可以与其它步骤组合，或省略，并且可以执行进一步的步骤和操作。例如，对于数字签名验证执行操作的次序可以不同于图 13 中示出的。在某些系统中，可以在产生摘要 A 之前检测数字签名，或产生摘要 A 之前可以恢复摘要 B。15 或者，如果数字签名没有被验证，能够在步骤 1360 停止消息预处理。在图 13 和 14 中的方法的其它变形将对本领域技术人员来说是明显的，并且由此被认为在上述和其中权利要求宣称的本发明的范围。

图 15 是用于预处理从移动设备发送的签名或加密然后签名消息的方法流程图。类似于上述的消息预处理实施例，与无线连接器系统操作的移 20 动设备和主系统能够被配置使得主系统预处理从移动设备发送的消息。

在图 15 中，该方法开始于步骤 1500 当用户在移动设备上编辑消息时。当移动设备被启动用于安全通信时，在步骤 1505，用户可选择附加消息安全特征，包括在图 15 的例子中“最后签名”，即加密然后签名，或“仅签名”消息安全。该类型的消息安全例如通过使用 S/MIME 或某些其它可能的所有安全消息方案被提供。

30 然后在步骤 1510 执行测试，以确定用户是否已经选择在签名之前加密消息。当在签名之前加密消息时，在步骤 1515 产生会话密钥，在步骤 1520 使用会话密钥加密消息，然后在步骤 1525 使用每个计划接收者的公钥加密会话密钥。这些公钥最好存储在移动设备上的存储器中，但是如果需要可改为从外部源诸如 PKS 等系统请求。

当消息已经被加密或消息没有被加密，该方法在步骤 1530 继续，并且在步骤 1530，消息、以及如果消息被加密的话会话密钥的加密版本被传递到摘要函数，使用用户私钥产生数字签名。代替附加签名相关信息诸如发送者证书、证书链和任何 CRL 到移动设备上的消息用于经无线传递到主系统处的无线连接器系统，移动设备最好包括在发送到主系统的消息中由无线连接器系统处理的签名相关信息指示，以确定任何签名相关信息被附加到消息后将会怎样。这允许移动设备通过主系统发送签名相关信息，同时避免经无线通信链路传送较大的签名相关信息。因此，在步骤 1535，移动设备向主系统发送原始消息（现在可能被加密）、数字签名和签名相关信息指示，以及如果消息被加密的话一个或多个加密的会话密钥。所有这些信息在被发送到主系统之前可使用无线友好方法被编码、压缩和加密。

在步骤 1540 开始在主系统的这样一个消息的后处理。在主系统操作的无线连接器系统从消息提取签名相关信息指示，并且确定什么签名相关信息应该被包括在消息中。在步骤 1545，在被提取的签名相关信息指示中标识的合适签名相关信息，例如包括发送者证书、以及可能的成链证书和 CRL，被附加到消息。然后，在步骤 1550，消息、数字签名和附加的签名相关信息从主系统发送到所有接收者。

当移动设备用户编辑一消息，并且选择仅消息加密或签名然后加密，如果操作在主系统的无线连接器系统能够访问用于加密消息的会话密钥，产生的加密消息的后处理可在主系统被执行。否则，主系统不能解密这样的消息，因此不能执行对消息的后处理操作。在该情况下，在移动设备上编辑的消息连同附加的数字签名和任何需要的证书和 CRL，将使用会话密钥在移动设备上被加密，并且加密的消息和会话密钥的加密版本将从移动设备发送到主系统以传递到寻址的接收者，或直接发送到寻址的接收者。任何所需的证书和 CRL 必须附加到移动设备上的消息上，并且整个消息的加密和会话密钥必须在设备上被处理。

然而，如果会话密钥能被传送到主系统，则某些加密和可能其它安全消息处理操作可以由主系统处理，如图 16 所示，这是用于后处理从移动设备发送的加密或签名然后加密的消息的方法的流程图。例如，代替使用

每个寻址的接收者的公钥加密会话密钥，会话密钥能够用与主系统或主系统场所处的移动设备用户台式计算机系统相关的公钥加密。假定无线连接器系统能够访问主系统或用户的相应私钥，然后会话密钥能够在主系统被解密。类似的，如果实现无线友好安全方案用于移动设备和操作在主系统
5 处的无线连接器系统之间的通信，那么会话密钥能够由移动设备根据该方案加密，然后由主系统解密。这潜在地允许主系统而不是移动设备，执行必须由移动设备执行的几个操作。

现在详细参照图 16，在步骤 1600，用户在移动设备上编辑消息，并且在步骤 1605 选择只加密或签名消息安全之后加密（最后加密）。在步
10 骤 1610，确定用户是否选择具有签名然后加密的消息。如果是，那么在步骤 1615 产生摘要和数字签名，在步骤 1620，签名相关信息诸如用户证书、证书链和任何所述的 CRL 附加到消息。当签名完成，或如果消息将被加密而没有先被签名，该方法在步骤 1625 进行，而设备产生将用在加密消息中的会话密钥。如果消息被签名，然后在步骤 1630 使用会话密钥
15 加密消息连同附加的数字签名和签名相关信息。然后，在步骤 1635，使用与可用于操作在主系统处的无线连接器系统的私钥相关的公钥，无线友好安全方法，或可能二者，加密会话密钥，并且加密的消息和加密的会话密钥被发送到主系统。由于无线友好安全方案存在，很明显，加密的消息可以是双加密传送到主系统。编码、压缩和消息加信封技术也可应用于消息和会话密钥以便传送到主系统。
20

当在主系统接收到消息和加密的会话密钥时，由无线连接器系统反转可应用于移动设备和主系统之间的数据传送的任何编码、压缩、加密和加信封。对于会话密钥例如使用公钥由设备进一步加密，那么在步骤 1640 由无线连接器系统使用相应的私钥解密。然后在步骤 1645，无线连接器
25 系统使用解密的会话密钥，利用每个寻址的接收者的公钥能够重新加密会话密钥，并且如在步骤 1650 中指示的，在转发消息以传递到寻址的接收者之前，将加密的会话密钥附加到消息。由此用于每个接收者的会话密钥的加密从移动设备卸载到主系统。

尽管在图 16 中没有示出，能够扩展该方法提供在主系统对加密消息
30 的更多的后处理。由于主系统的无线连接器系统具有会话密钥，消息自身

可以被解密。因此，在解密之前，设备不需要必须附加签名相关信息（其证书、证书链或任何 CRL）到消息上。可替换为，如上联系图 15 所述的，签名相关信息指示能够附加到消息。无线连接器系统使用会话密钥，能够解密该消息，处理签名相关信息指示然后附加任何所需的签名相关信息。

5 一旦该信息被附加，那么无线连接器系统使用会话密钥能够重新加密消息，并且为每个寻址的接收者加密会话密钥。按照该方法，典型的大容量签名相关信息由主系统添加到消息，以避免由设备进行的该信息的加密以及信息的无线传送。

如果强无线友好安全方案位于移动设备和主系统之间，那么消息和会
10 话密钥，以及数字签名和任何签名相关信息指示能够按照该安全方案被加
密并且发送到主系统。然后，主系统能够将签名相关信息指示中标识的所
需签名相关信息附加到消息上，使用会话密钥加密消息、数字签名和签名
15 相关信息，然后为寻址的接收者加密会话密钥。在该情况中，会话密钥能
够由主系统而不是移动设备产生，进一步减少了从移动设备发送的数据
量。然后移动设备只需要使用无线友好安全方案，通过该技术如 S/MIME
和 PGP 启动安全通信。消息后处理将大批数据处理操作从移动设备移到
更强大的主系统。

对于主系统还能够访问移动设备用户的签名密钥，后处理概念甚至能
够进一步扩展到包括安全消息的签名。然后移动设备能够向主系统传送一
20 个消息、一个该消息应该被签名的指示、如果说有的话的签名相关信息、消息
应该被加密的指示、以及或者会话密钥或者主系统应该选择会话密钥的
指示。然后主系统能够代表移动设备处理所有加密和签名的操作。

虽然这些技术减少了安全消息需要的必须从移动设备传送的数据量和
基于设备的处理操作的复杂性，但使用会话密钥在主系统的加密、以及在
25 主系统的签名产生，假定了移动设备和主系统之间的安全传输或主系统能
够访问用户的私钥。

现在转到图 17，示出了能够用于该系统和其中描述的方法的范例无线通信设备的方框图。移动通信设备 100 最好是具有语音和/或数据通信能
30 力的双向通信设备。设备最好具有与互联网上的其它计算机系统通信的能力。根据设备提供的功能，该设备最好称为数据通信设备，双向寻呼机，

具有数据通信能力的蜂窝电话，无线互联网用具或数据通信设备（带有或不带有电话能力）。如上提到的，这些设备在此统统简称为移动设备。

双模式设备 100 包括收发器 1711，微处理器 1738，显示器 1722，闪速存储器 1724，RAM 1726，辅助输入/输出 (I/O) 设备 1728，串行口 1730，
5 键盘 1732，扬声器 1734，麦克风 1736，短距离无线通信子系统 1740，并且还可包括其它设备子系统 1742。收发器 1711 最好包括发送和接收天线
1716，1718，接收器 (Rx) 1712，发送器 (Tx) 1714，一个或多个本地
振荡器 (LO) 1713，和数字信号处理器 (DSP) 1720。在快闪存储器 1724
内，设备 100 最好包括能够由微处理器 1738 (和/或 DSP 1720) 执行的多
10 个软件模块 1724A-1724N，包括：语音通信模块 1724A，数据通信模块
1724B，和用于执行多个其它功能的多个其它操作模块。

移动设备 100 最好是具有语音和数据通信能力的双向通信设备。这样，
例如，设备可通过语音网络诸如任何模拟或数字蜂窝网络通信，并且还能
通过数据网络通信。语音和数据网络在图 17 中由通信塔 1719 描述。这些
15 语音和数据网络可以是使用分离的基础设施诸如基站、网络控制器等的分
离的通信网络，或它们可以集成为一个单个的无线网络。因此，对网络
1719 的引用应解释为包括单个语音和数据网络或分离的网络。

通信子系统 1711 用于与网络 1719 通信。DSP 1720 用于向发送器 1714
发送信号和从接收器 1712 接收通信信号，并且还能与发送器 1714 和接收
20 器 1712 交换控制信息。如果语音和数据通信发生在单个频率上，或近间
隔频率组上，那么单个 LO 1713 可以与发送器 1714 和接收器 1712 一起使
用。或者，如果不同频率用于语音及数据通信，那么多个 LO 1713 能够用
于产生对应于网络 1719 的多个频率。尽管在图 17 中示出了两个天线 1716，
1718，移动设备 100 能够使用单个天线结构。包括语音和数据信息二者
25 的信息通过 DSP 1720 和微处理器 1738 之间的链路与通信模块 1711 通信。

通信子系统 1711 的详细设计，诸如频带，分量选择，功率电平等将
取决于设备 100 将操作的通信网络。例如，打算运行于北美市场的设备
100 可包括设计运行于 Mobitex 或 DataTAC 移动数据通信网络、并且还被
设计运行于各种通信网络诸如 AMPS、TDMA、CDMA、PCS 等的任何一个
30 的通信子系统 1711，其中打算用于欧洲的设备 100 可被配置以操作于

GPRS 数据通信网络和 GSM 语音通信网络。其它类型的数据和语音网络，分离的和集成的，也可用于移动设备 100。

根据网络 1719 的类型，对双模式移动设备 100 的访问需求也可以变化。例如，在 Mobitex 和 DataTAC 数据网络中，移动设备使用与每个设备相关的唯一标识号网络上注册。然而，在 GPRS 数据网络中，网络访问与设备 100 的订户或用户相关。GPRS 设备典型需要用户身份模块（“SIM”），需要该模块以便设备 100 运行在 GPRS 网络上。没有 SIM，本地或非网络通信功能（如果有）可以是可操作的，但是设备 100 将不能执行涉及在网络 1719 上通信的任何功能。除了任何法律上要求的操作，
5 诸如‘911’紧急呼叫之外。
10

在已经完成任何所需的网络注册或激活处理之后，双模式设备 100 可经网络 1719 发送和接收通信信号，最好包括语音和数据二信号。由天线 1716 从通信网络 1719 接收的信号路由到接收器 1712，其提供信号放大、频率下转换、滤波、信道选择等，并且还可提供模拟数字转换。接收信号
15 的模拟数字转换允许更复杂的通信功能诸如使用 DSP 1720 将执行的数字解调和解码。以类似方式，处理将传送到网络 1719 的信号，包括例如由 DSP 1720 执行的调制和编码，然后提供给发送器 1714 用于数字模拟转换、频率上转换、滤波、放大和经天线 1718 传送到通信网络 1719。尽管在图
20 17 中示出了单个收发器 1711 用于语音和数据通信，设备 100 能够包括两个不同的收发器，第一收发器用于传送和接收语音信号，及第二收发器用于传送和接收数据信号。

除了处理通信信号之外，DSP 1720 还提供接收器和发送器控制。例如，应用到接收器 1712 和发送器 1714 中的通信信号的增益电平可通过在
25 DSP 1720 中实现的自动增益控制算法得到自适应控制。其它收发器控制算法也能在 DSP 1720 中实现以便提供收发器 1711 的更复杂的控制。

微处理器 1738 最好管理和控制双模式移动设备 100 的整个操作。在此能够使用很多类型的微处理器或微控制器，或者，可选地，单个 DSP
30 1720 能够用于执行微处理器 1738 的功能。包括至少数据和语音通信的低层通信功能通过在收发器 1711 中的 DSP 1720 执行。其它高层通信应用诸如语音通信应用 1724A 和数据通信应用 1724B 可以存储在闪速存储器

1724 中用于由微处理器 1738 执行。例如，语音通信模块 1724A 可以提供高层用户接口，该高层用户接口可操作以通过网络 1719 传送和接收双模式移动模式 100 和多个其它语音设备之间的语音呼叫。类似地，数据通信模块 1724B 可以提供一高层用户接口，该接口可以操作用于通过网络 1719 在双模式移动设备 100 和多个其它数据设备之间发送和接收数据诸如电子邮件消息、文件、组织者信息、短文本消息等。在设备 100 上，安全消息软件应用可以与数据通信模块 1724B 一起操作，以便实现上述的安全消息技术。

微处理器 1738 还与其它设备子系统交互，这些子系统诸如显示器 1722，闪速存储器 1724，随机访问存储器（RAM）1726，辅助输入/输出（I/O）子系统 1728，串行口 1730，键盘 1732，扬声器 1734，麦克风 1736，短距离通信子系统 1740，和一般表示为 1724 的任何其它通信子系统。例如，模块 1724A-N 由微处理器 1738 执行，并且可提供移动设备用户和移动设备之间的高层接口。该接口典型地包括通过显示器 1722 提供的图形组件，和通过辅助 I/O 1728，键盘 1732，扬声器 1734 或麦克风 1736 提供的输入/输出组件。

图 17 中所示的某些子系统执行通信相关功能，其中其它子系统可以提供“驻留”或设备内置功能。特别地，某些子系统诸如键盘 1732 和显示器 1722 可以用于通信相关功能以及设备驻留功能，所述通信相关功能诸如输入文本消息用于经数据通信网络传送，以及设备驻留功能诸如计算器或任务列表或其它 PDA 类型功能。

由微处理器 1738 使用的操作系统软件最好存储在永久存储器诸如闪速存储器 1724。除了操作系统和通信模块 1724A-N 之外，闪速存储器 1724 还可包括用于存储数据的文件系统。最好还在闪速存储器 1724 中提供存储区域，以存储公钥、私钥和安全消息传送所需要的其它信息。操作系统、特定设备应用或模块或其部件可以临时装载进易失存储器诸如 RAM 1726 用于快速操作。此外，接收的通信信号在将它们永久写到位于永久存储器 1724 中的文件系统之前，还可临时存储到 RAM 1726。

可以装载到双模式设备 100 上的范例应用模块 1724N 是提供 PDA 功能诸如日历事件、约会和任务项的个人信息管理器（PIM）应用。该模块

1724N 还可与用于管理电话呼叫、语音信件等的语音通信模块 1724A 交互，并且还可与用于管理电子邮件通信和其它数据传送的数据通信模块 1724B 交互。或者，语音通信模块 1724A 和数据通信模块 1724B 的所有功能可以集成进 PIM 模块。

5 闪速存储器 1724 最好提供文件系统以方便在设备上 PIM 数据项的存储。PIM 应用最好包括经无线网络 1719 或者通过自身或者与语音和数据通信模块 1724A, 1724B 一起发送和接收数据项的能力。PIM 数据项最好通过无线网络 1719 与存储在主计算机系统或与主计算机系统相关的一相应数据项组无缝集成、同步和更新，由此建立与特定用户相关的数据项的
10 镜像系统。

移动设备 100 还通过将设备 100 放在连接移动设备 100 的串行口与主系统的串行口的接口架中与主系统人工同步。串行口 1730 还能用于使
15 用用户能够通过外部设备或软件应用设定偏爱，下载其它应用模块 1724N 用于安装，和将如上所述装载证书、密钥和其它信息下载到设备上。该有线
下载路径还可用将加密密钥装载到设备上，这是比通过无线网络 1719
交换安全信息更安全的方法。

附加应用模块 1724N 可以通过网络 1719、通过辅助 I/O 子系统 1728、
通过串行口 1730、通过短距离通信子系统 1740 或任何其它合适的子系统
1742 装载到双模式设备 100，并且由用户安装在闪速存储器 1724 或 RAM
20 1726。这种应用安装方面的灵活性增加了设备 100 的功能，并且可以提供
增强的设备内置功能、通信相关功能或二者。例如，安全通信应用可以使
得电子商务功能和其它这种财务交易能够使用设备 100 执行。

当双模式设备 100 操作在数据通信模式中时，接收的信号诸如文本消息或网页下载将由收发器 1711 处理并且提供到微处理器 1738，其将最好
25 进一步处理接收的信号用于输出到显示器 1722 或者，可选地输出到辅助设备 1728。双模式设备 100 还能使用键盘 1732 编辑数据项诸如电子邮件消息，键盘最好是 QWERTY 风格的完全字母数字键盘布局，尽管也可以使用其它风格的完全字母数字键盘诸如 DVORAK 风格。利用多个辅助 I/O 设备 1728 进一步增强了到设备 100 的用户输入，其可包括拇指轮输入设备、触感衰减器、各种开关、摇杆输入开关等。由用户输入的编辑数据项
30

然后可以通过收发器 1711 经通信网络 1719 传送。由移动设备 100 接收和将从移动设备 100 传送的安全消息按照上述的技术由数据通信模块 1724B 或相关安全消息传送软件应用程序处理。

当双模式设备 100 操作在语音通信模式中时，设备 100 的整个操作实际上类似于数据模式，除了接收的信号最好输出到麦克风 1734 和用于传送的语音信号由麦克风 1736 产生之外。此外，上述的安全消息传送技术可以不必应用到语音通信。可选的语音或音频 I/O 子系统诸如语音消息记录子系统也可以在设备 100 上实现。尽管语音或音频信号输出最好主要通过扬声器 1734 实现，显示器 1722 也能用于提供呼叫方身份的指示、语音呼叫的持续或其它语音呼叫相关信息。例如，微处理器 1738 与语音通信模块 1724A 和操作系统软件可以检测输入语音呼叫的呼叫者标识信息，并且将其显示在显示器 1722 上。

短距离通信子系统 1740 也可以包括在双模式设备 100 中。例如，子系统 1740 可包括红外设备和相关电路和组件，或短距离无线通信模块，诸如分别按照蓝牙或 802.11 规范的“蓝牙”模块或 802.11 模块，以提供与类似使能的系统和设备的通信。对本领域技术人员明显的是“蓝牙”和 802.11 分别指涉及无线 LAN 和无线个人区域网络的可从电气和电子工程师协会（IEEE）得到的规范组。

已经详细描述了系统的优选实施例，包括操作的优选方法，应理解该操作能够用不同的单元和步骤执行。该优选实施例仅以例子示出，不打算限制本发明的范围。例如，图 18 和 19 示出了涉及无线移动通信设备的消息的预处理和后处理。

图 18 描述了一个预处理的例子，其中主系统 1806 从消息发送者接收寻址到一个或多个消息接收者的消息 1804。无线连接器系统 1810 产生用于对应于消息接收者的移动设备 1814 的消息 1812。无线连接器系统 1810 对发送者消息 1804 执行验证和/或加密消息处理 1808。可以执行很多类型的处理诸如通过排除相应移动设备的消息接收者不需要的某些或所有会话密钥，减少发送者加密消息的尺寸。通过处理 1808，传送到移动设备 1814 的消息 1812 是关于验证和/或加密方面的发送者消息 1804 的修改。

移动设备 1814 包含用于存储这些预处理的消息的存储器，诸如易失或非易失 RAM（随机存取存储器）。

如果其它移动设备由无线连接器系统 1810 识别，发送者消息 1804 被类似处理，以相应于应该接收发送者消息 1804 的接收者。这样，针对验证和/或加密方面（例如编码方面）修改的消息（例如 1816）被发送到其它移动设备（例如 1818）。

应该理解这样的系统可以以很多种方法变化，诸如允许处理 1808 由主系统 1806 执行，或让无线连接器系统 1808 操作在主系统 1806 内或操作在不同于主系统 1806 的平台上。作为系统变化的宽范围的另一个例子，10 无线连接器系统 1810 可以使用非重定向操作以传送消息到移动设备（例如 1814 和 1818）。

图 19 描述了后处理的例子，其中无线连接器系统 1906 从无线移动通信设备 1902 接收寻址到一个或多个消息接收者（例如 1914 和 1918）的消息 1904。对消息 1904 执行验证和/或加密消息处理 1908。可以执行很多类型的处理，诸如：从设备签名消息去除签名相关信息指示，并且将在签名相关信息指示中标识的签名相关信息附加到签名的消息。然后被处理的消息 1912 通过主系统 1910 发送到一个或多个接收者（例如 1914 和 1918）。

在此描述的这些预处理和后处理系统碰到很多问题，诸如主要由于带宽和与移动设备有关的电池限制、当前系统不设法向移动设备传递整个 S/MIME 消息的困难。一个困难是 S/MIME 消息通常太大不能经无线通信网络有效发送到移动设备。如果发送到移动设备或从移动设备接收整个 S/MIME 消息，仅对于单个消息可能使用超量的存储器和电池电力。考虑由移动设备接收或传送需要的时间，存储需要的存储器和处理消息交换需要的电池电力，设法支持直接的 S/MIME 产品对平均商业用户来说具有不希望的质量。另一个示范的问题是没有可访问无线网络和移动设备的当前可用的公钥服务器。结果，公钥密码操作的使用是很困难的，并且需要在移动设备处的大的缓冲操作，以消除公钥基础设施（PKI）的需要。在交换安全电子邮件消息领域，存在附加的问题，包括：（1）移动设备不能从 PKI 检索公共加密的密钥以加密从移动设备发送的消息，（2）不能检索关于接收的被签名消息的公钥，（3）不能在小型设备上处理很大的

CRL, 和 (4) 在较慢处理器的移动设备上执行涉及公钥加密算法的复杂数学运算的时间延迟。这些问题和其它问题导致当用户设法使用移动设备交换基于 S/MIME 的电子邮件消息时较差和受挫的用户经历。

在此描述的预处理和后处理系统和方法处理安全电子邮件消息使得 5 这些消息例如包括 S/MIME 消息能够与移动设备交换。该系统和方法也影响与移动设备相关的主系统的处理器功率, 以使得与移动设备交换 S/MIME 消息时能够有较好的用户经历。

在图 20-22 中示出了在此公开的系统和方法的宽范围的进一步的例子。图 20-22 描述了在不同的示范通信系统内该系统和方法的附加使用。 10 图 20 是表示示例通信系统的方框图。在图 20 中, 示出了计算机系统 2002, WAN 2004, 安全防火墙 2008 后面的公司 LAN 2006, 无线基础设施 2010, 无线网络 2012 和 2014, 和无线移动通信设备(“移动设备”)2016 和 2018。公司 LAN 2006 包括消息服务器 2020, 无线连接器系统 2028, 包括至少 15 多个信箱 2019 的数据存储器 2017, 具有直接到移动设备的通信链路诸如通过物理连接 2024 到接口或连接器 2026 的台式计算机系统 2022, 和无线虚拟专用网络 (VPN) 路由器 2032。下面将参照消息 2033, 2034 和 2036 描述图 20 中的系统的操作。

计算机系统 2002 例如可以是被配置用于连接到 WAN 2004 的膝上、台式或掌上计算机系统。该计算机系统可以通过 ISP 或 ASP 连接到 WAN 2004。或者, 计算机系统 2002 可以是联网的计算机系统例如象计算机系统 2022 通过 LAN 或其它网络访问 WAN 2004。很多现代移动设备能够通过各种基础设施和网关配置连接到 WAN, 使得计算机系统 2002 也可以是 20 移动设备。

公司 LAN 2006 是已经被用于无线通信的中央基于服务器的消息系统的示例。公司 LAN 2006 可以被称为“主系统”, 因为它主管带有用于消息的信箱 2019 的数据存储器 2017, 以及用于可发送到移动设备 2016 和 2018 或从这些移动设备接收的其它数据项的可能的其它的数据存储器(未示出), 和无线连接器系统 2028, 无线 VPN 路由器 2032, 或实现用于公司 LAN 2006 和一个或多个移动设备 2016 和 2018 之间的通信的可能其它 30 组件。用更一般的术语, 主系统可以是如上所述无线连接器系统运行于其

上或与无线连接器系统运行相关的一个或多个计算机。公司 LAN 2006 是主系统的一个优选实施例，其中主系统是运行在操作于至少一个安全通信防火墙 2008 之后并且被保护的公司网络环境内的服务器计算机。其它可能的中央主系统包括 ISP,ASP 和其它服务提供商或邮件系统。尽管台式计算机系统 2024 和接口/连接器 2026 可以位于这些主系统外部，无线通信操作可以类似于下面描述的这些。

公司 LAN 2006 使用无线连接器系统 2028 做为相关的无线通信实现组件，其将通常是一软件程序、软件应用或建立与至少一个或多个消息服务器一起作的软件组件。无线连接器系统 2028 用于通过一个或多个无线网络 2012 和 2014 发送用户选择的信息到一个或多个移动设备 2016 和 2018 或从这些移动设备接收信息。无线连接器系统 2028 可以是图 20 所示的消息系统的分离组件，或可以替换为是部分或全部包含进其它通信系统组件。例如，消息服务器 2020 可以包含实现无线连接器系统 2028，其一部分，或某些或全部功能的软件程序、应用或组件。

运行在防火墙 2008 后面的计算机上的消息服务器 2020 充当主接口，以用于公司与典型地是一互联网的 WAN 2004 交换消息，例如包括电子邮件、日历数据、语音信件、电子文档和其它个人信息管理（PIM）数据。具体的中间操作和计算机将取决于通过其交换消息的消息传递机构和网络的特定类型，并且因此没有在图 20 中示出。消息服务器 2020 的功能可以扩展到消息发送和接收，提供这些特征象动态数据库存储用于如日历、待办事件表、任务表、电子邮件和文档的数据。

消息服务器诸如 2020 通常为在服务器上具有帐户的每个用户在一个或多个数据存储器诸如 2017 中保持多个信箱 2019。数据存储器 2017 包括用于多个（“n”）用户帐户的信箱 2019。由识别用户、用户帐户、信箱或与用户、帐户或信箱 2019 相关的其它可能的地址为消息接收者的消息服务器 2020 接收的消息将典型地存储在相应的信箱 2019 中。如果消息被寻址到多个接收者或分配表，那么相同消息的复制件可以存储到多于一个信箱 2019 中。或者消息服务器 2020 可以将该消息的单个复制件存储到具有消息服务器上的帐户的所有用户可访问的数据存储器中，并且将指针或其它标识符存储到每个接收者信箱 2019 中。在典型消息系统中，每个用

户可以使用消息客户诸如 Microsoft Outlook 或 Lotus Notes (通常运行在连接在 LAN 2006 中的 PC 诸如台式计算机系统 2022 上) 于是可以访问他或她的信箱 2019 和其内容。尽管在图 20 中只示出了一个台式计算机系统 2022, 本领域技术人员将理解 LAN 将典型地包含很多台式、笔记本和膝上计算机系统。每个消息客户通过消息服务器 2020 正常访问信箱 2019, 尽管在某些情况下, 消息客户可以能够直接访问数据存储器 2017 和由台式计算机系统 2022 存储其上的信箱 2019。消息也可以从数据存储器 2017 下载到台式计算机系统 2022 上的本地数据存储器 (未示出)。

在公司 LAN 2006 内, 无线连接器系统 2028 与消息服务器 2022 一起操作。无线连接器系统 2028 可以驻留在与消息服务器 2022 相同的计算机系统上, 或可以替换为在不同的计算机系统上实现。实现无线连接器系统 2028 的软件也能部分或全部与消息服务器 2022 集成。无线连接器系统 2028 和消息服务器 2020 最好被设计为合作和交互以允许信息推送到移动设备 2016, 2018。在该安装中, 无线连接器系统 2028 最好被配置为通过公司防火墙 2008 和经 WAN2004 及无线网络 2012, 2014 之一向一个或多个移动设备 2016, 2018 发送存储在与公司 LAN 2006 相关的一个或多个数据存储器中的信息。例如, 在数据存储器 2017 中具有帐户和相关信箱 2019 的用户也能具有移动设备诸如 2016。如上所述, 由识别用户、帐户或信箱 2019 的消息服务器 2020 接收的消息由消息服务器 2020 存储到相应的信箱 2019。如果用户具有移动设备诸如 2016, 由消息服务器 2020 接收并且存储到用户信箱 2019 的消息最好由无线连接器系统 2028 检测并且发送到用户的移动设备 2016。该类型的功能表示“推送信息发送技术”。无线连接器系统 2028 还替换为采用“拉回技术”(其中存储在信箱 2019 中的项响应于使用移动设备进行的请求或访问操作被发送到移动设备 2016, 2018) 或两种技术的某些组合。

由此, 无线连接器 2028 的使用能够使包括消息服务器 2020 的消息系统被扩展, 使得每个用户的移动设备 2016, 2018 能够访问消息服务器 2020 存储的消息。

如图 20 所示, 类似于图 1 的系统, 有几个路经用于从公司 LAN 2006 与移动设备 2016, 2018 交换信息。一个可能的信息传送路径是使用接口

或连接器 2026 通过物理连接 2024 诸如串行口。该路径可能是有用的例如用于如上所述的较大 PIM 和签名相关信息、数据同步和私用加密或签名密钥传送。在已知的“同步”型无线消息系统中，物理路径还已经被用于从与消息服务器 2020 相关的信箱 2019 中向移动设备 2016 和 2018 传送消息。
5

用于与移动设备 2016, 2018 数据交换的另一方法是通过无线连接器系统 2028 和使用无线网络 2012, 2014 的无线交换。如图 20 所示，这能够涉及无线 VPN 路由器 2032 或提供到一个或多个无线网络 2012, 2014 的接口的与无线基础设施 2010 的传统 WAN 连接。无线 VPN 路由器 2032 提供直接通过特定无线网络 2012 到无线设备 2016 的 VPN 连接的建立。
10 使用无线 VPN 路由器 2032 的主要优点是它成为不需要无线基础实施 2010 的现成 VPN 组件。VPN 连接可以使用 IP 上传输控制协议 (TCP/IP) 或 IP 上用户数据报协议 (UDP/IP) 连接以直接传递消息到移动设备 2016 和从该移动设备接收消息。

15 如果无线 VPN 路由器 2032 不可用，那么到通常是互联网的 WAN 2004 的连接是可由无线连接器系统 2028 采用的通常使用的连接机构。为了处理移动设备 2016 的寻址和任何其它需要的接口功能，最好使用无线基础实施。

20 在某些实现中，不止一个无线信息交换机构可提供于公司 LAN 2006 内。在例如图 20 的示例通信系统中，与用户相关的移动设备 2016, 2018 被配置操作在不同的无线网络 2012 和 2014，该用户具有与消息服务器 2020 上的用户帐户相关的信箱 2019。如果无线网络 2012 支持 Ipv6 寻址，那么无线 VPN 路由器 2032 可以由无线连接器系统 2028 使用以与操作在无线网络 2012 内的任何移动设备 2016 交换数据。然而，无线网络 2014
25 可以是不同类型的无线网络，诸如 Mobitex 网络，在该情况下，信息可改为通过无线连接器系统 2028 经与 WAN 2004 和无线基础设施 2010 的连接与操作在无线网络 2014 内的移动设备 2018 交换。

30 在图 20 中的系统的操作类似于上述的图的操作。电子邮件消息 2033 从计算机系统 2002 发送并且寻址到具有一个帐户和信箱 2019 等与消息服务器 2020 和移动设备 2016 或 2018 相关的数据存储器的至少一个接收者。

然而，电子邮件消息 2033 打算只用于展示目的。在公司 LAN 2006 之间其它类型信息的交换最好还能由无线连接器系统 2028 实现。

从计算机系统 2002 通过 WAN 2004 发送的电子邮件消息 2033 根据使用的特定消息方案可能是完全未加密的，或用数字签名签名和/或加密的。

5 例如，如果计算机系统 2002 被用于使用 S/MIME 的安全消息传送，那么电子邮件消息 2003 可以是签名的，加密的或两者。

电子邮件消息 2033 到达消息服务器 2020，其确定电子邮件消息 2033 应该存进哪个信箱 2019。如上所述，诸如电子邮件消息 2033 的消息可包括用户名、用户帐户、信箱标识符或可由消息服务器 2020 映射到特定帐户或相关信箱的其它类型的标识符。对于电子邮件消息 2033，接收者典型地使用对应于用户帐户和由此的信箱 2019 的电子邮件地址被标识。

10 无线连接器系统 2028 最好一旦检测到一个或多个已经发生的触发事件，通过无线网络 2012 或 2014 从公司 LAN 2006 到用户移动设备 2016 或 2018 发送或映射某些用户选择的数据项或数据项的部分。触发事件包

15 括但不限于下列一个或多个：在用户联网的计算机系统 2022 处的屏幕保护程序的激活，用户移动设备 2016 或 2018 从接口 2026 断开，或接收到从移动设备 2016 或 2018 发送到主系统以开始发送存储在主系统处的一个或多个消息。于是，无线连接器系统 2028 可以检测与消息服务器 2020 相

20 关的触发事件诸如一个命令的接收，或与一个或多个联网的计算机系统 2022 相关的触发事件诸如上述的屏幕保护和断开事件。当在 LAN 2006 已经激活移动设备 2016 或 2018 对公司数据的无线访问，例如当无线连接器

25 系统 2028 为移动设备用户检测到触发事件的发生，由用户选择的数据项最好发送到用户的移动设备。在电子邮件消息 2033 的例子中，假定已经检测到一触发事件，由无线连接器系统 2028 检测到在消息服务器 2020 处消息 2033 的到达。这个例如可以通过监视或轮询与消息服务器 2020 相

的信箱 2019 完成，或如果消息服务器 2020 是 Microsoft Exchange（微软交换）服务器，那么无线连接器系统 2028 可以登记由微软消息应用编程接口（MAPI）提供的建议同步（advise syncs），由此当新消息存储到信箱 2019 时接收通知。

当一数据项诸如电子邮件消息 2033 将发送到移动设备 2016 或 2018 时，无线连接器系统 2028 最好重新打包数据项，如在 2034 和 2036 中指示的。重新打包技术可以类似用于任何有效的传送路径或可以取决于特定的传送路径，无线基础设施 2010 或无线 VPN 路由器 2032。例如，电子邮件消息 2033 最好被压缩和加密，或者在 2034 被重新打包之前或之后，以由此有效提供到移动设备 2018 的安全传送。压缩减少发送消息需要的带宽，而加密保证发送到移动设备 2016 和 2018 的任何消息或其它信息的保密性。相反，通过 VPN 路由器 2032 传送的消息可能仅仅被压缩并且不加密，因为由 VPN 路由器 2032 建立的 VPN 连接是固有安全的。由此经在无线连接器系统 2028 处的加密，例如可被考虑一非标准的 VPN 隧道或类 VPN 连接，或者经 VPN 路由器 2032，消息被安全发送到移动设备 2016 和 2018。由此使用移动设备 2016 或 2018 访问消息决不比使用桌上型计算机系统 2022 访问 LAN 2006 处信箱不安全。

当重新打包的消息 2034 或 2036 经无线基础设施 2010 或经无线 VPN 路由器 2032 到达移动设备 2016 或 2018 时，移动设备 2016 或 2018 从重新打包的消息 2034 或 2036 去除外面的电子信封，并且执行任何需要的解压缩和解密操作。从移动设备 2016 或 2018 发送并且指向一个或多个接收者的消息最好被类似重新打包，并且可能压缩和加密，和发送到主系统诸如 LAN 2006。然后主系统从重新打包的消息去除电子信封，如果需要，解密和解压缩消息，并且将消息路由到被寻址的接收者。

图 21 是可选的示例通信系统的方框图，其中无线通信由与无线网络运营者相关的组件实现。如图 21 所示，该系统包括：计算机系统 2002，WAN 2004，位于安全防火墙 2008 后面的公司 LAN 2007，网络运营者基础设施 2040，无线网络 2011，和移动设备 2013 和 2015。计算机系统 2002，WAN 2004，安全防火墙 2008，消息服务器 2020，数据存储器 2017，信箱 2019，和 VPN 路由器 2035 实际上与图 20 中类似标记的组件相同。然而，由于 VPN 路由器 2035 与网络运营者基础设施 2040 通信，它不必是图 21 的系统中的无线 VPN 路由器。网络运营者基础设施 2040 实现分别与计算机系统 2042 和 2052 相关并且配置运行在无线网络 2011 中的 LAN2007 和移动设备 2013，2015 之间的无线信息交换。在 LAN 2007 中，

示出了多个台式计算机系统 2042, 2052, 每个具有到接口或连接器 2048, 2058 的物理连接 2046, 2056。无线连接器系统 2044, 2054 运行在每个计算机系统 2042, 2052 上或与每个计算机系统 2042, 2052 一起工作。

5 无线连接器系统 2044, 2054 类似于上述的无线连接器系统 2028,
因为它们使得数据项诸如电子邮件消息和存储在信箱 2019 中的其它项、
并且可能的存储在本地或网络数据存储器中的数据项，从 LAN 2007 发送
到一个或多个移动设备 2013, 2015。在图 21 中，然而，网络运营者基础
设施 2040 提供移动设备 2013, 2015 和 LAN 2007 之间的接口。如同上面，
下面将以电子邮件消息的内容作为能够发送到移动设备 2013, 2015 的数
10 据项的示例描述图 21 所示的系统的操作。

当由消息服务器 2020 接收寻址到具有消息服务器 2020 上的帐户的一个或多个接收者的电子邮件消息 2033 时，消息或可能是存储在中央信箱或数据存储器中的消息的单个复印件的指针，被存储在每个这种接收者的信箱 2019 中。一旦电子邮件消息 2033 或指针已经存储在信箱 2019 中，
15 它最好能够使用移动设备 2013 或 2015 被访问。在图 21 示出的例子中，
电子邮件消息 2033 已经被寻址到与台式计算机系统 2042 和 2052 二者以
及由此的移动设备 2013 和 2015 二者相关的信箱 2019 中。

正如本领域技术人员将理解的，通常用在有线网络诸如 LAN 2707
和/或 WAN 2004 中的通信网络协议不适合于或不匹配无线网络诸如 2011
20 中使用的无线网络通信协议。例如，在无线网络中主要关心的通信带宽、
协议开销和网络等待时间，在有线网络中不重要，有线网络比无线网络典型地具有更高容量和速度。因此，移动设备 2013 和 2015 不能直接正常访问
数据存储器 2017。网络运营者基础设施 2040 提供无线网络 2011 和
LAN2007 之间的桥梁。

25 网络运营者基础设施 2040 使得移动设备 2013, 2015 能够通过 WAN
2004 建立到 LAN 2007 的连接，并且例如可以由无线网络 2011 的运营者
或为移动设备 2013 和 2015 提供无线通信服务的服务提供商操作。在基于
拉回的系统中，使用无线网络匹配通信方案，当信息应该保持保密时最好
使用安全方案诸如无线传输层安全（WTLS），和无线网络浏览器诸如无
30 线应用协议（WAP）浏览器，移动设备 2013, 2015 可以建立与网络运营

者基础设施 2040 的通信会话。然后用户可以请求（通过人工选择或驻留在移动设备里的软件中的预选择缺省）存储在 LAN 2007 上数据存储器 2017 中的信箱 2019 中的任何或所有信息或例如仅仅新信息。然后如果没有会话已经被建立，例如使用安全超文本传输协议（HTTPS），网络运营者基础设施 2040 建立与无线连接器系统 2044, 2054 的连接或会话。正如上述，可以经一个典型的 WAN 连接或通过 VPN 路由器 2035（如果有的话）进行网络运营者基础设施 2040 和无线连接器系统 2044, 2054 之间的会话。当接收来自移动设备 2013, 2015 的一个请求和将所请求的信息传递回到设备之间的时间延迟将被最小化，可以配置网络运营者基础设施 2040 和无线连接器系统 2044, 2054 使得通信连接一旦被建立保持开通。

在图21的系统中，来自移动设备A 2013和B 2015的请求将分别发送到无线连接器系统2044和2054。一旦接收到来自网络运营者基础设施2040的信息请求，无线连接器系统2044, 2054从数据存储器中检索所请求的信息。对于电子邮件信息2033，无线连接器系统2044, 2054典型地通过结合计算机系统2042, 2052操作的消息传送客户机，从适当的信箱2019检索电子邮件消息 2033，其中这些计算机系统或者经消息服务器2020或者直接可访问信箱2019。或者，可以配置无线连接器系统2044, 2054直接或通过消息服务器2020访问信箱2019本身。此外，其它数据存储器，类似于数据存储器2017的网络数据存储器和与每个计算机系统2042, 2052相关的本地数据存储器，可以对无线连接器系统2044, 2054访问，并且于是可访问移动设备2013, 2015。

如果电子邮件消息2033寻址到与计算机系统2042和2052及设备2013和2015两者相关的消息服务器帐户或信箱2019，那么电子邮件消息2033可发送到网络运营者基础设施2040如2060和2062示出的，然后发送一个电子邮件消息的复制件到每个移动设备2013和2015，如2064和2066指示的。信息可以经到WAN 2004的连接或VPN路由器2035在无线连接器系统 2044, 2054和网络运营者基础设施2040之间传送。当网络运营者基础设施 2040经不同的协议与无线连接器系统2044, 2054和移动设备2013, 2015通信时，可由网络运营者基础设施2040执行翻译操作。重新打包技术也可以在无线连接器系统2044, 2054和网络运营者基础设施2040之间，和每个

移动设备2013, 2015和网络运营者基础设施2040之间使用。

要从移动设备2013, 2015发送的消息或其它信息可以以类似方式得到处理, 这些信息首先从移动设备2013, 2015传送到网络运营者基础设施2040。然后网络运营者基础设施2040可以发送信息到无线连接器系统
5 2044, 2054以便存储在信箱2019中并且例如通过消息服务器2020传递到任何寻址的接收者, 或者可选地将信息传递到寻址的接收者。

图21中的系统的上述描述涉及基于拉回的操作。无线连接器系统
2044, 2054和网络运营者基础设施可被替换地配置为将数据项推送到移动
设备2013和2015。也能够是一组合的推送/拉回系统。例如, 当前存储在
10 LAN 2007处的数据存储器中的一列数据项或新消息的通知可以推送到移
动设备2013, 2015, 然后可以用来经网络运营者基础设施2040从LAN 2007
请求消息或数据项。

如果与LAN 2007上的用户帐户相关的移动设备被配置操作于不同的
15 无线网络内, 然后, 每个无线网络可以具有类似于2040的相关无线网络
基础设施部件。

尽管在图21的系统中为每个计算机系统2042, 2052示出了分离的专
用的无线连接器系统2044, 2054。最好可配置一个或多个无线连接器系统
2044, 2054以与多于一个计算机系统2042, 2052一起操作, 或访问与多于
一个计算机系统相关的数据存储器或信箱2019。例如, 无线连接器系统
20 2044可被授权访问与计算机系统2042和计算机系统2052二者相关的信箱
2019。然后从移动设备A 2013或B 2015请求数据项可以由无线连接器系统
2044处理。该配置可用于实现LAN 2007和移动设备2013和2015之间的通
信, 而不需要为每个移动设备用户运行的台式计算机系统2042, 2052。无线
连接器系统可被替换为与消息服务器2020一起实现以启动无线通信。

25 图22是另一个可选的通信系统的方框图。该系统包括: 计算机系统
2002, WAN 2004, 位于安全防火墙2008后面的公司LAN 2009, 访问网关
2080, 数据存储器2082, 无线网络2084和2086, 和移动设备2088和2090。
在LAN 2009中, 计算机系统2002, WAN 2004, 安全防火墙2008, 消息服
务器2020, 数据存储器2017, 信箱2019, 台式计算机系统2022, 物理连接
30 2024, 接口或连接器2026和VPN路由器2035实质上与上述相应的组件相

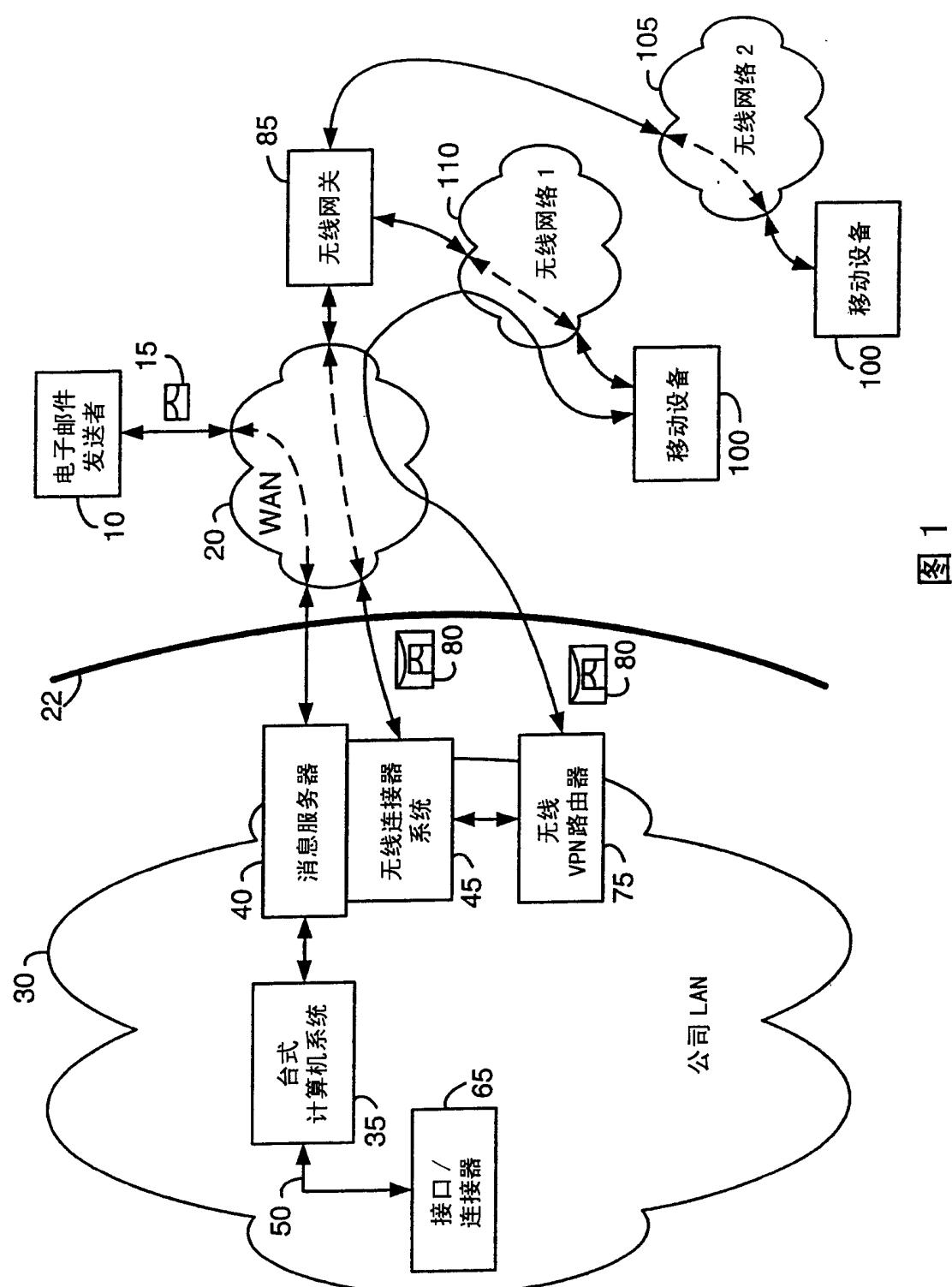
同。访问网关2080和数据存储器2082为移动设备2088和2090提供对存储在 LAN 2009中的数据项的访问。在图22中，无线连接器系统2078运行于消息服务器2020上或与消息服务器2020一起操作，尽管无线连接器系统可替换为运行于LAN 2009中的一个或多个台式计算机系统上或与LAN 2009中的一个或多个台式计算机系统一起工作。

10 无线连接器系统2078提供存储在LAN 2009上的数据项到一个或多个移动设备2088，2090的传送。这些数据项最好包括，存储在数据存储器2017上的信箱2019中的电子邮件消息，以及存储在数据存储器2017或另一网络数据存储器或计算机系统诸如2022的本地数据存储器上的其它数据项。

如上所述，寻址到具有消息服务器2020上的帐户的一个或多个接收者并且由消息服务器2020接收的电子邮件消息2033可以存储到每个这样的接收者的信箱2019中。在图22的系统中，外部数据存储器2082最好具有与数据存储器2017类似的结构，并且保持与数据存储器2017同步。存储在 15 数据存储器2082中的PIM信息或数据最好独立于存储在主系统上的PIM信息或数据并可修改的。在该种具体配置中，在外部数据存储器2082的独立可修改的信息可保持与一个用户相关的多个数据存储器（移动设备上的数据，家中个人计算机上的数据，公司LAN上的数据）的同步。该同步可以通过如下完成：例如可通过由无线连接器系统2078以一定的时间间隔发送 20 到数据存储器2082的更新数据，其中每次数据存储器2017中的一项被添加或改变，在一天的某些时候，或在LAN 2009启动时，由消息服务器2020或计算机系统2022在数据存储器2082的更新数据，或可能由移动设备2088，2090通过访问网关2080发送到数据存储器2082的更新数据。在例如电子邮件消息2033的情况下，接收电子邮件消息2033之后的某时间发送到 25 数据存储器2082的更新数据可以指示消息2033已经存储在存储器2017中的某一信箱2019中，并且电子邮件消息的一个复印件将被存储到数据存储器2082中的相应的存储区域中。当电子邮件消息2033已经存储在例如对应于移动设备2088和2090的信箱2019中时，在图22中以2092和2094指示的电子邮件消息的一个或多个复印件将被发送到并且存储到数据存储器2082 30 中的相应的存储区域或信箱中，正如示出的，在数据存储器2017中存储信

息的更新或复制可通过到WAN 2004的连接或VPN路由器2035发送到数据存储器2082。例如，无线连接器系统2078可经HTTP投寄请求投寄更新数据或存储的信息到数据存储器2082中的资源。或者，可以使用安全协议诸如HTTPS或安全套接字层(SSL)。本领域技术人员将理解存储在LAN 2009
5 处的数据存储器中多于一个位置的一个数据项的单个复制件可以被替换为发送到数据存储器2082。然后，数据项的该复制件，用存储在数据存储器2082中的每个相应位置中的所有存储数据项的指针或其它标识符，能够存储在数据存储器2082中多于一个相应的位置，或者单个复制件可存储在数据存储器2082中。

10 访问网关2080是一个有效的访问平台，因为它为移动设备2088和2090提供了对数据存储器2082的访问。数据存储器2082可以配置为在WAN 2082上可访问的资源，并且访问网关2080可以是ISP系统或WAP网关，通过其移动设备2088和2090可以连接到WAN 2004。然后与无线网络 2084和2086匹配的WAP浏览器或其它浏览器可被用于访问与数据存储器2017同步的数据存储器2082，并且或者自动地或者响应于来自移动设备2088，2090的请求，下载存储的数据项。如在2096和2098示出的，存储在数据存储器2017
15 中的电子邮件消息2033的复制件，可发送到移动设备2088和2090。由此，在每个移动设备2088，2090上的数据存储器（未示处）可以与公司LAN 2009上的数据存储器2017的一部分诸如信箱2019同步。移动设备数据存储器的变化可类似地反映在数据存储器2082和2017中。
20



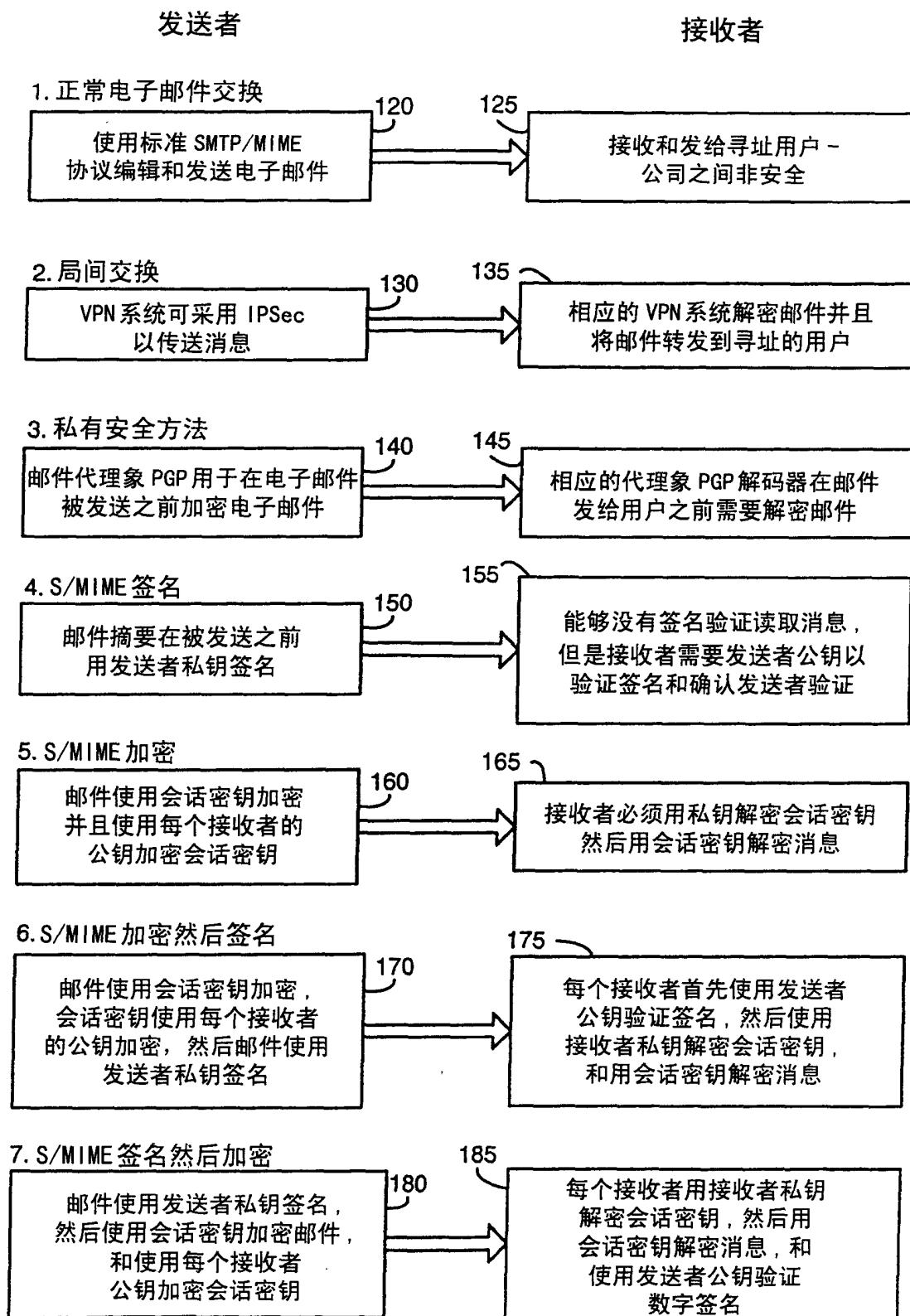


图 2

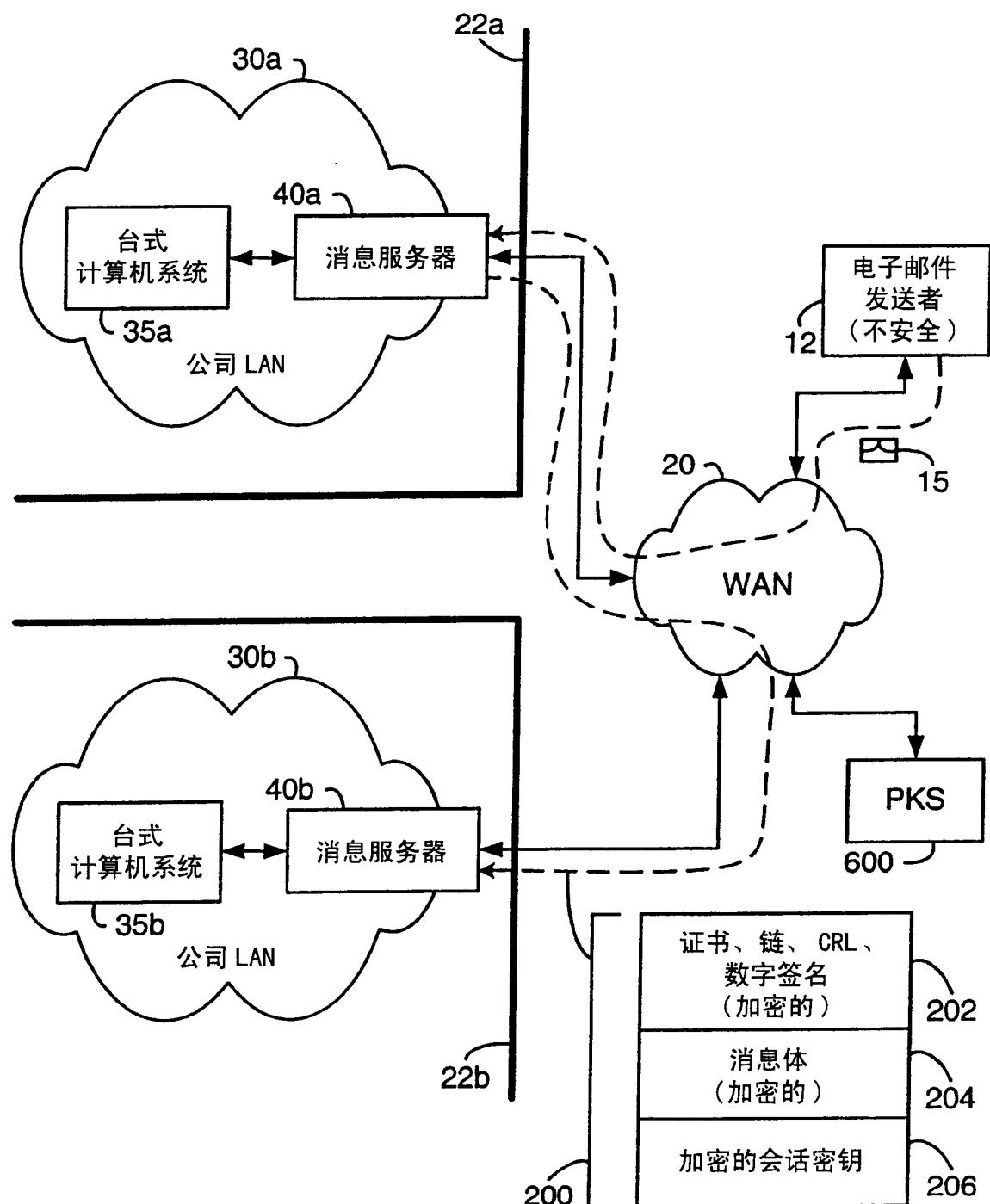


图 3

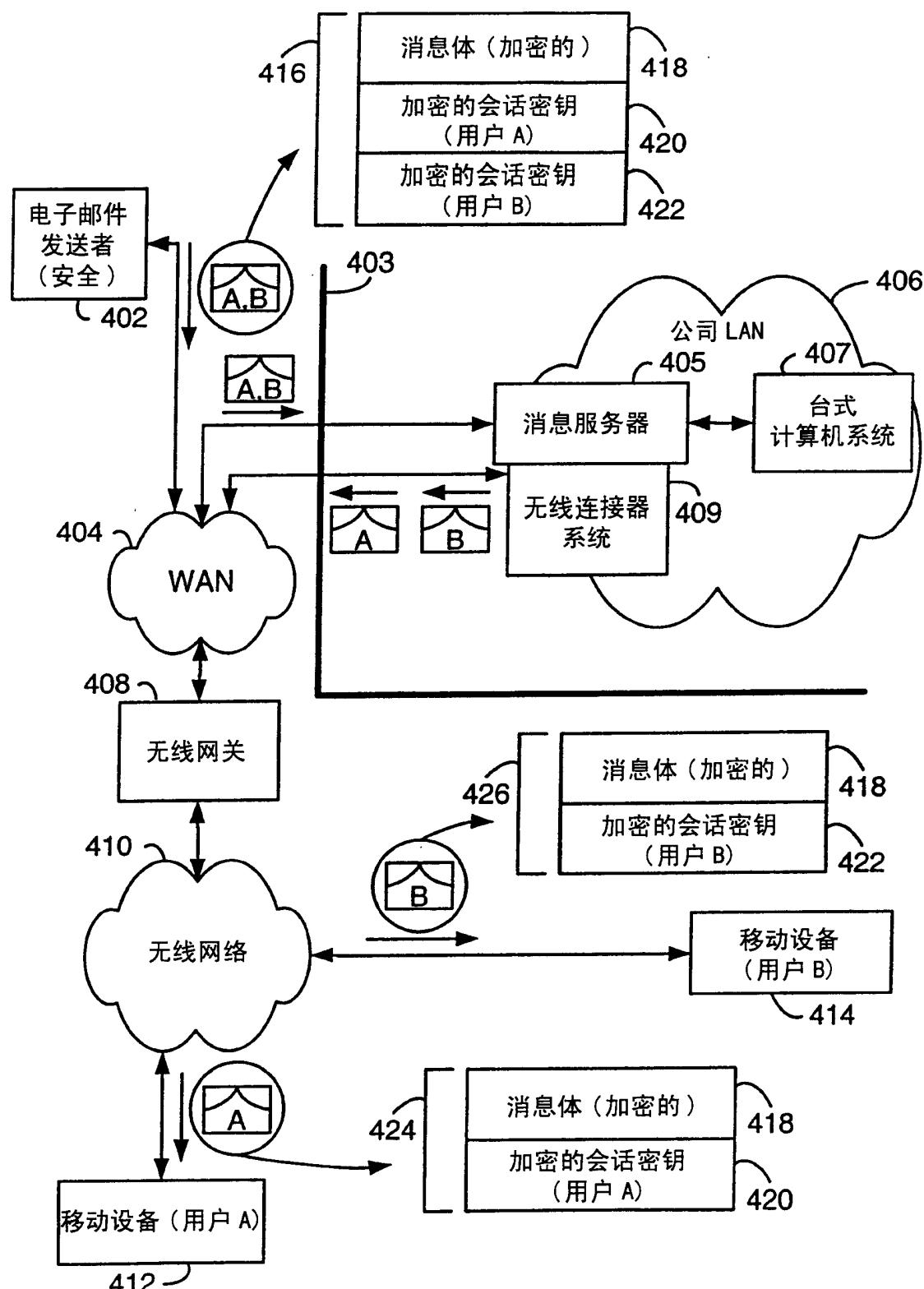


图 4

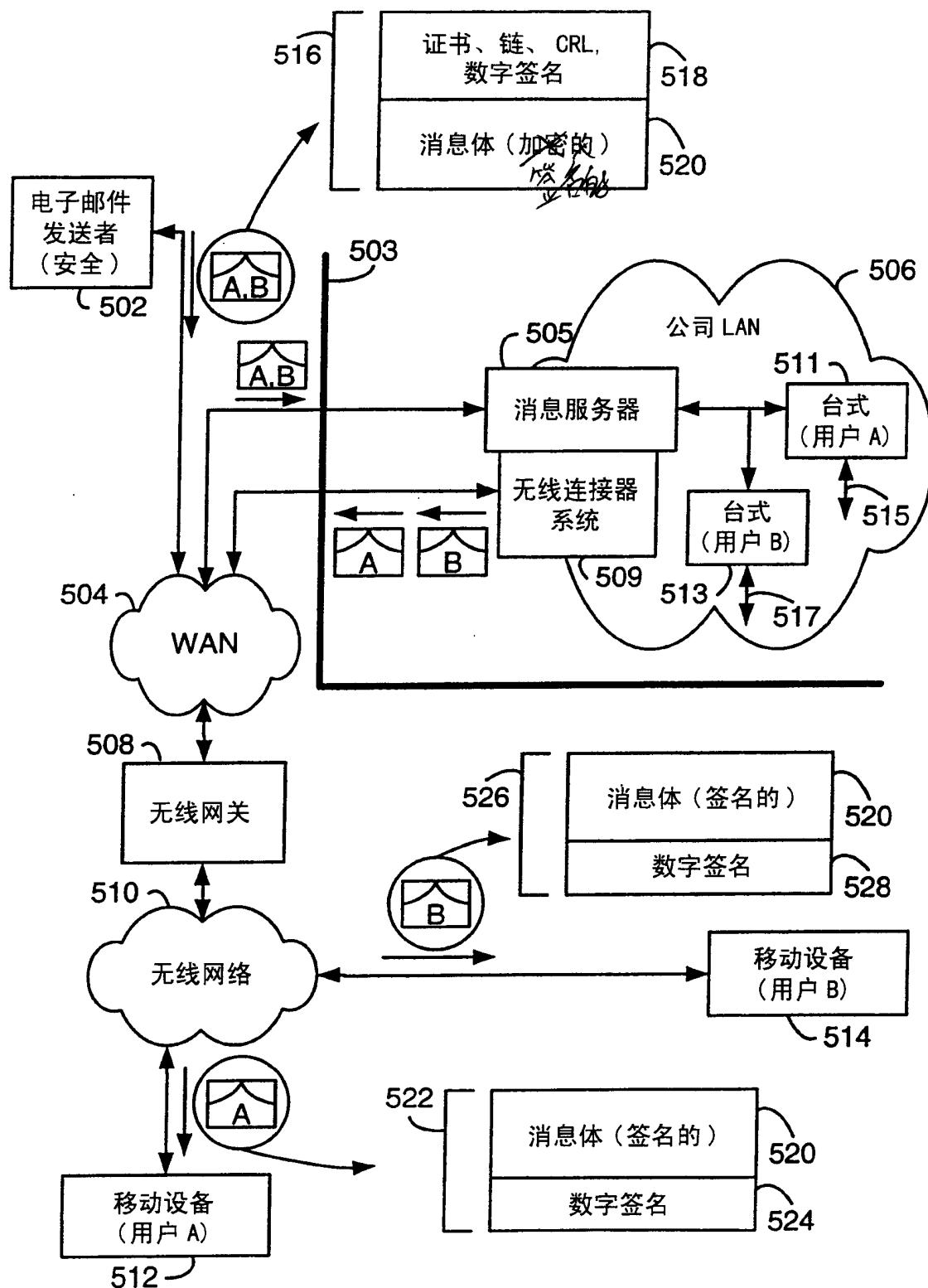


图 5

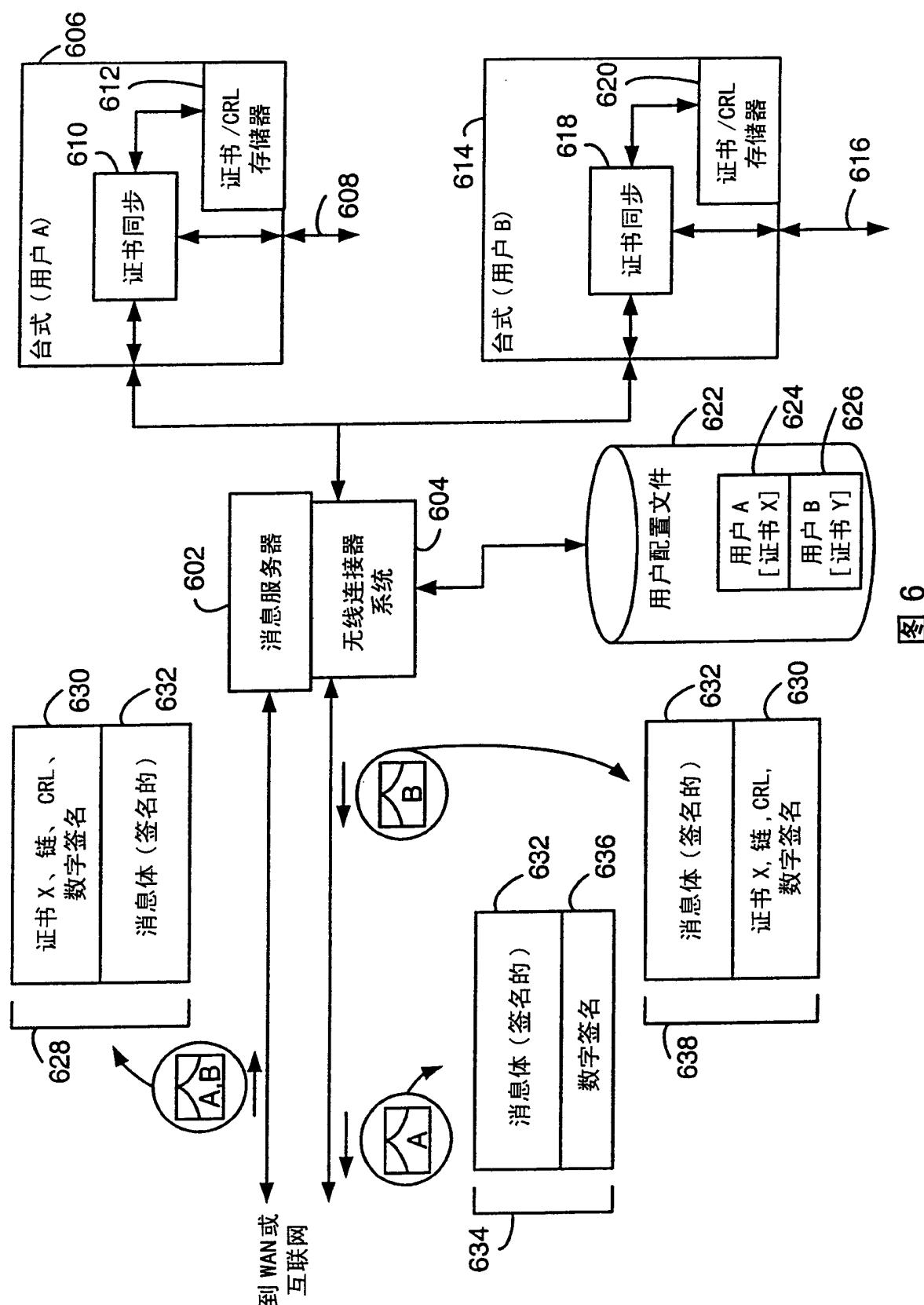


图 6

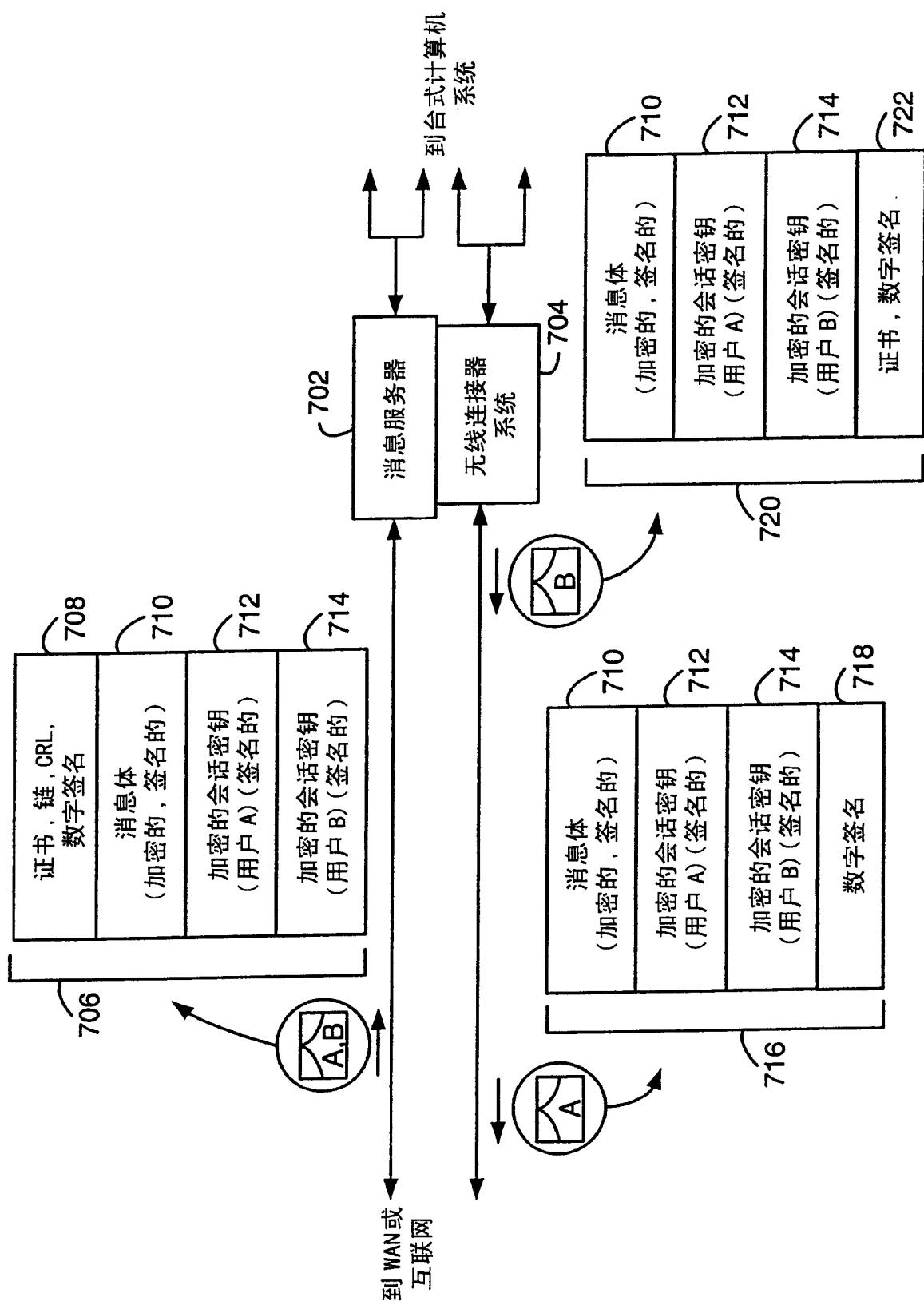


图 7

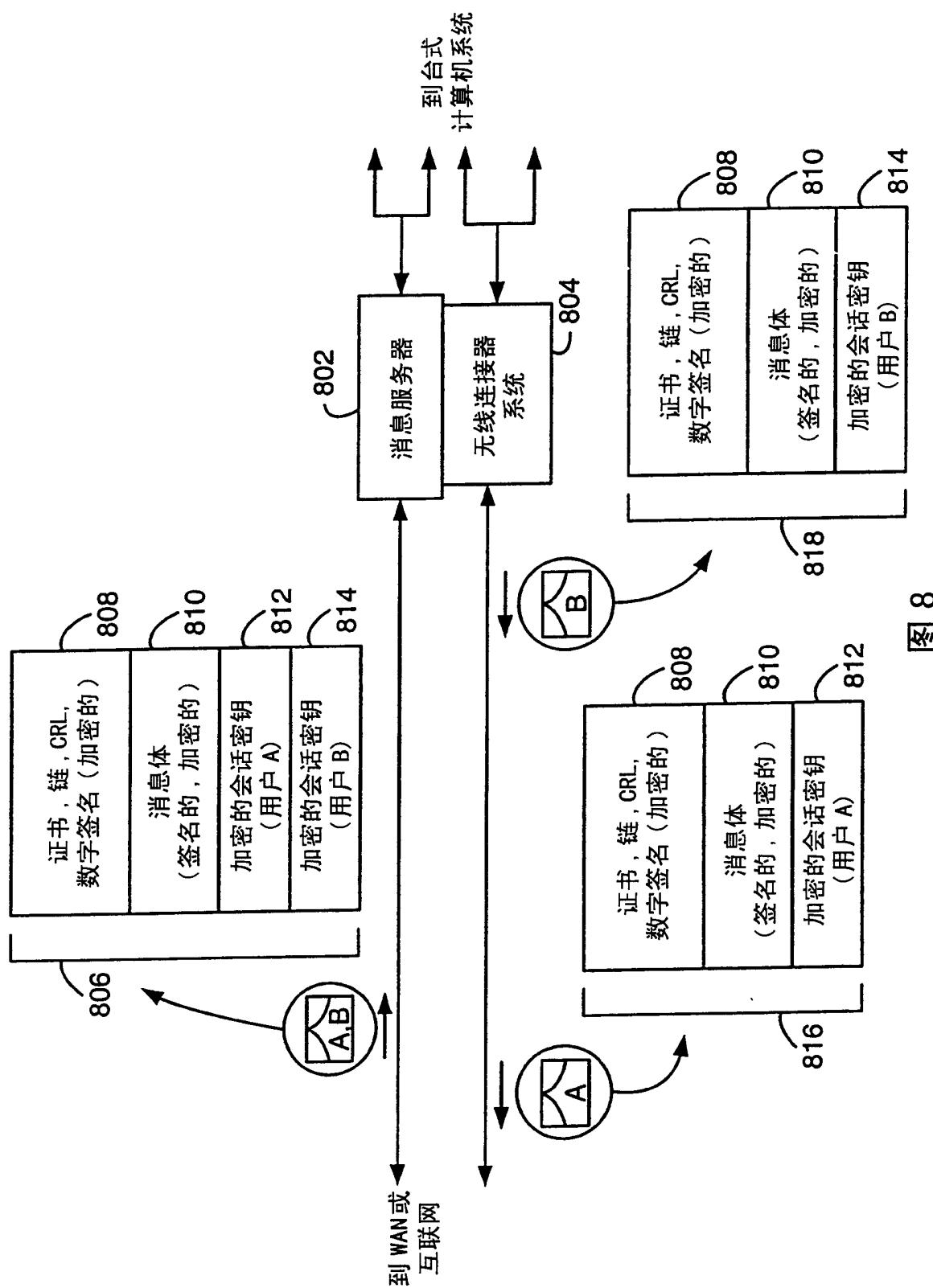


图 8

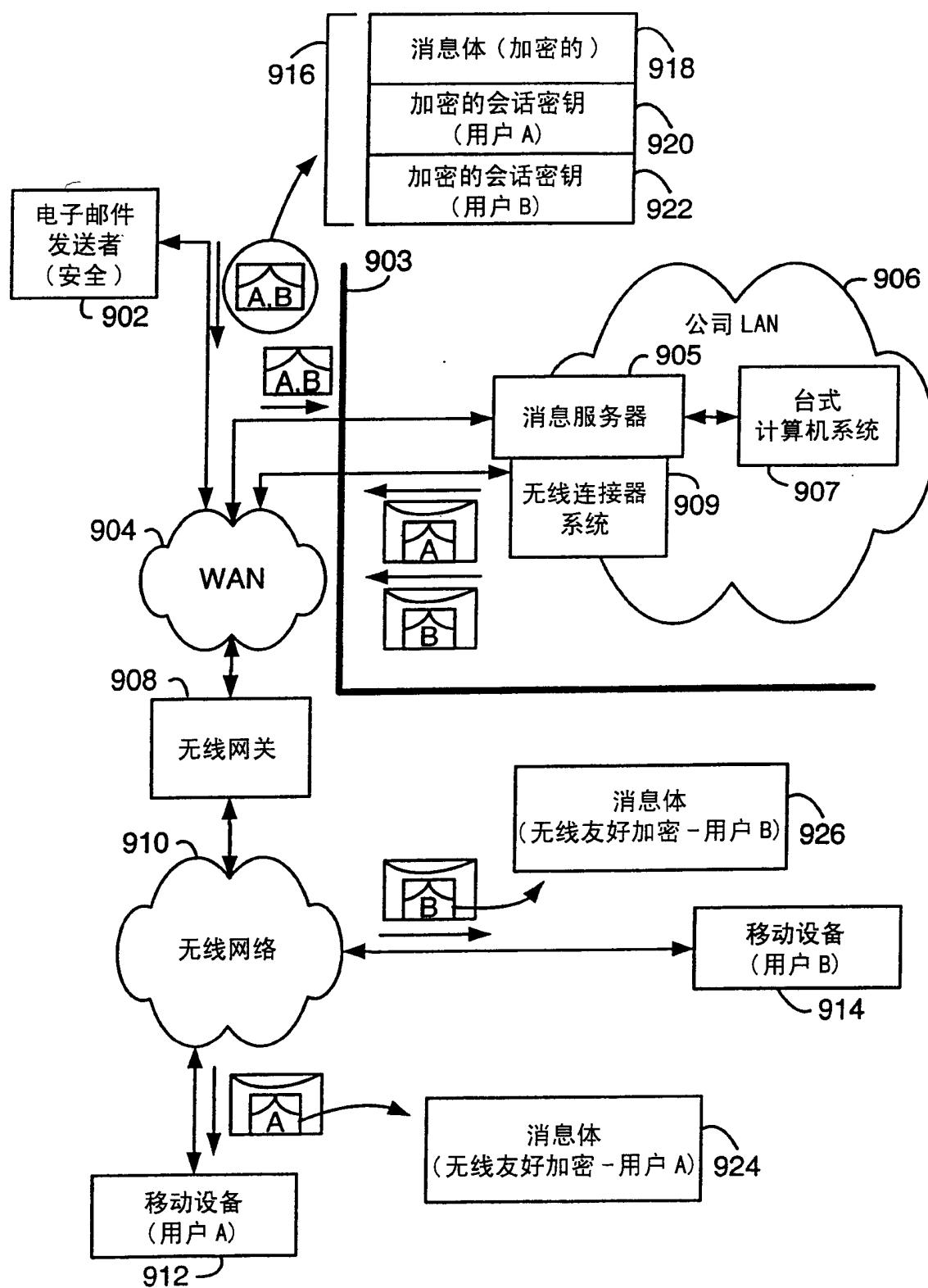


图 9

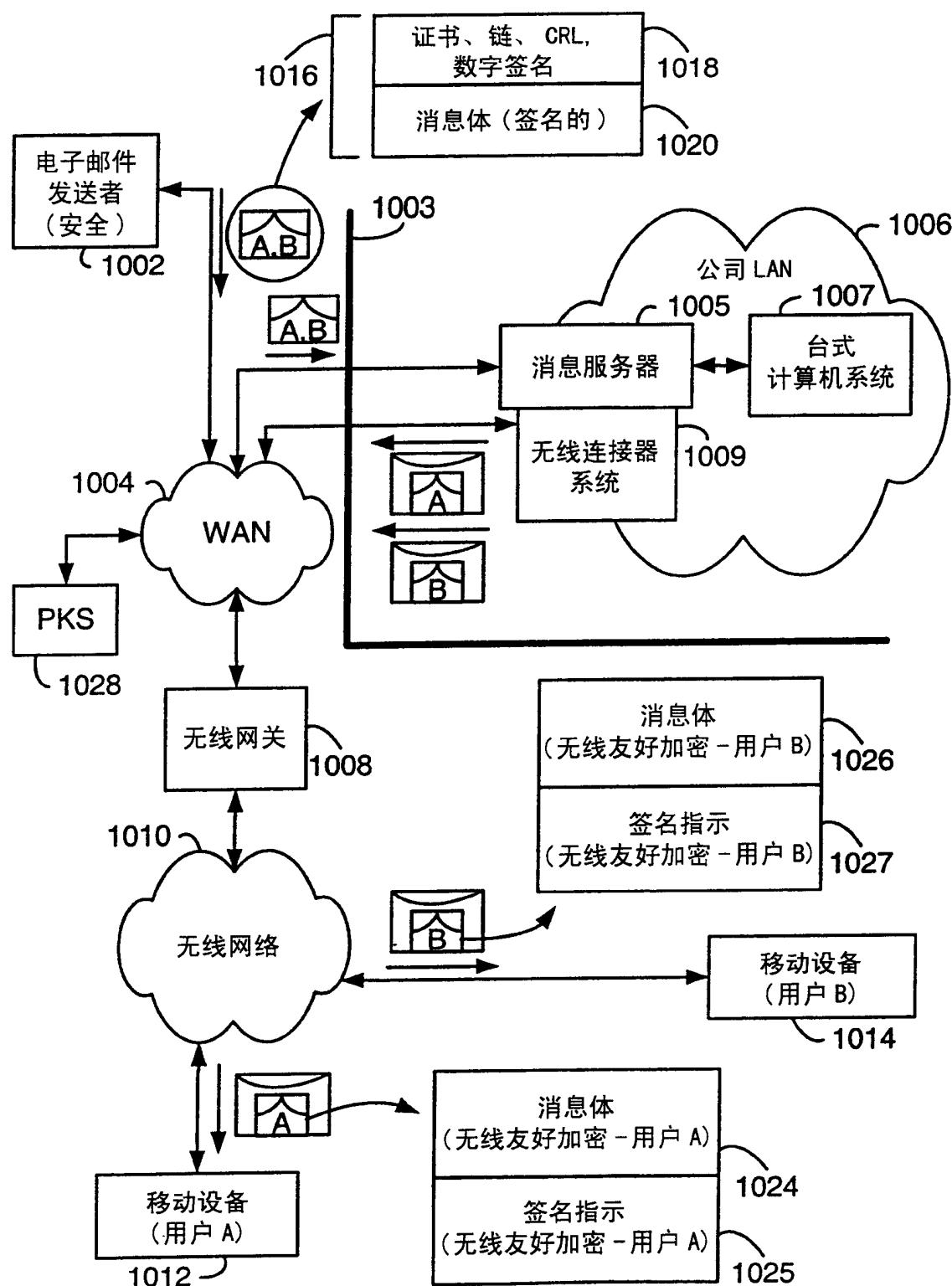


图 10

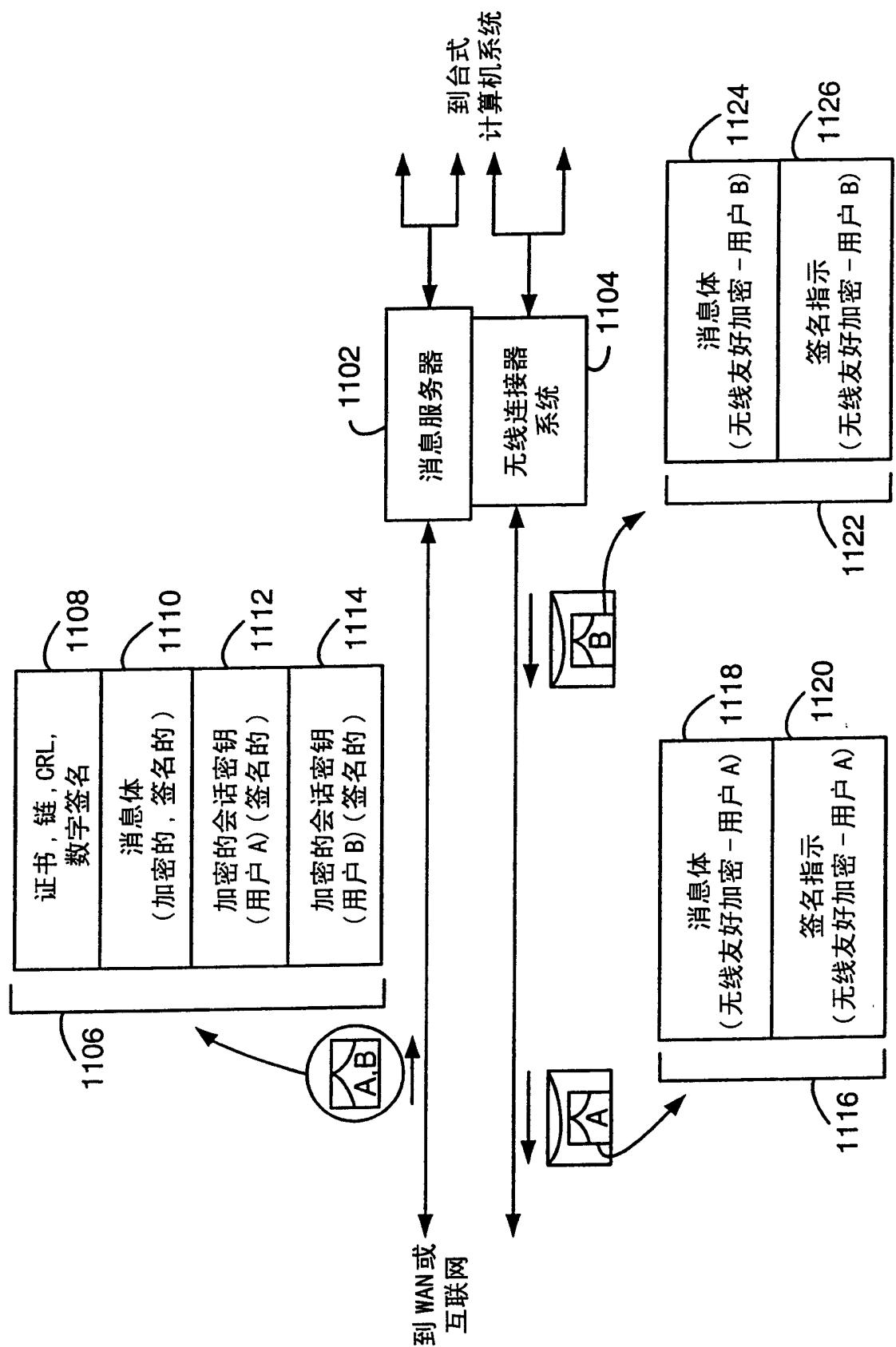


图 11

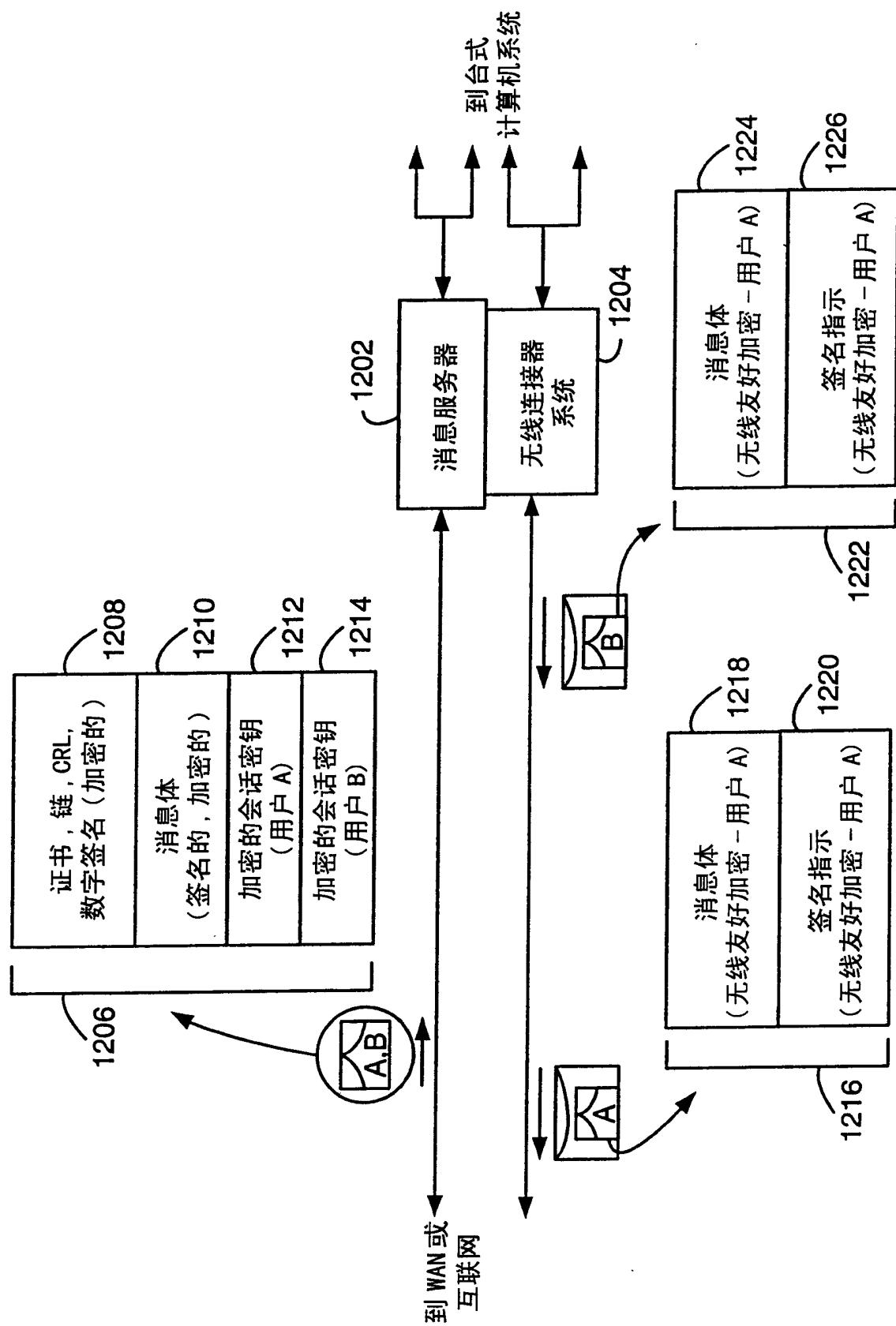


图 12

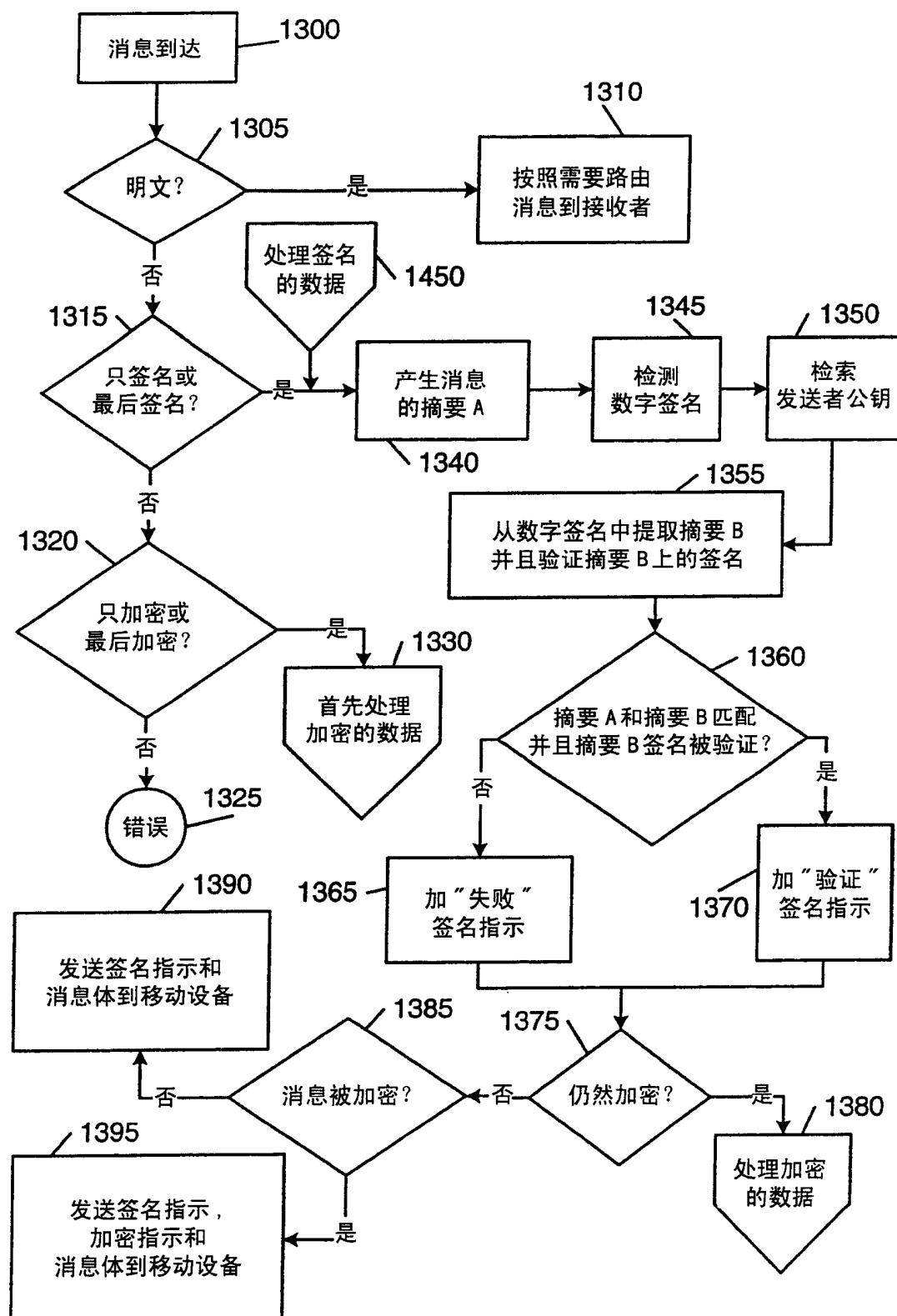


图 13

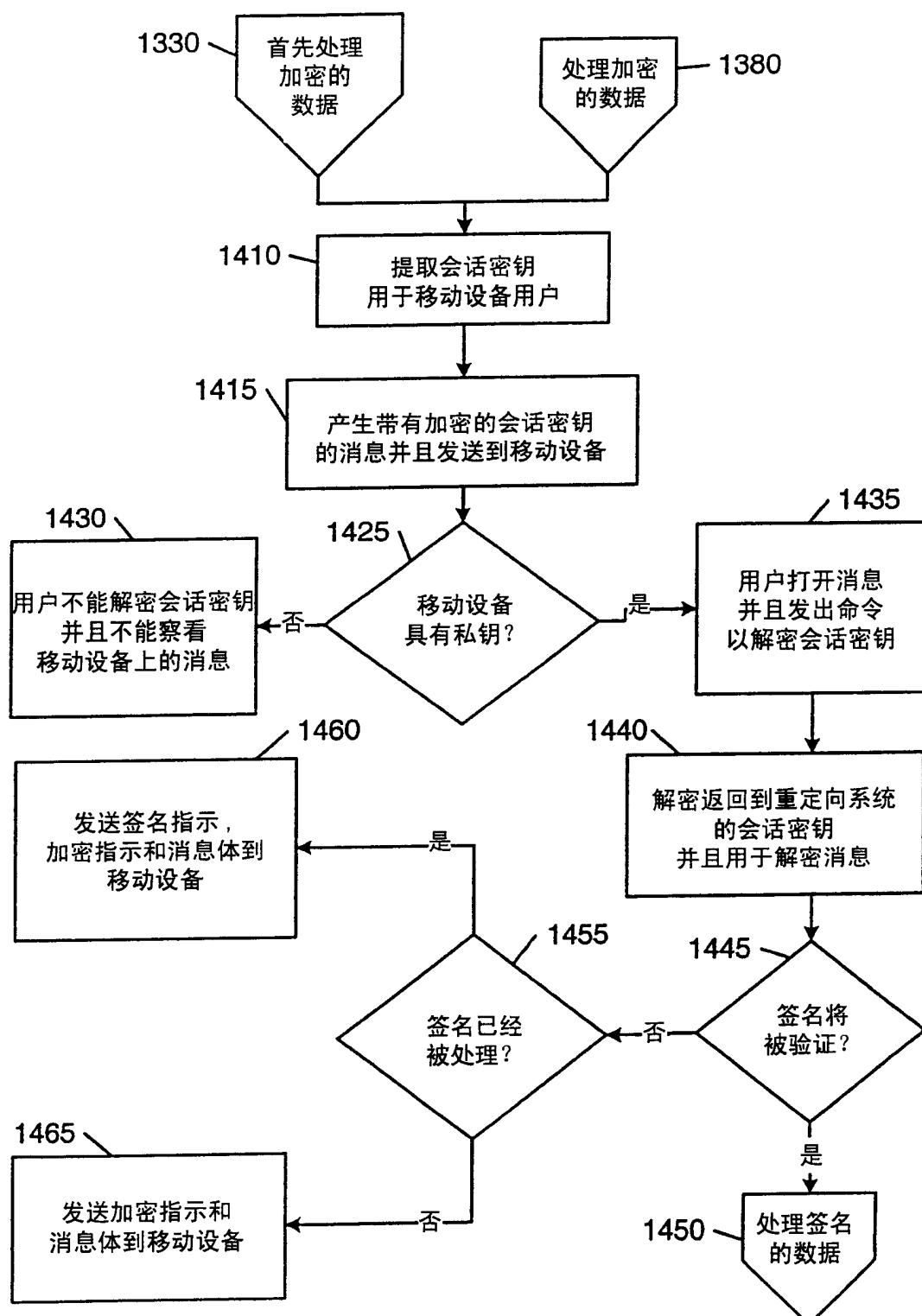


图 14

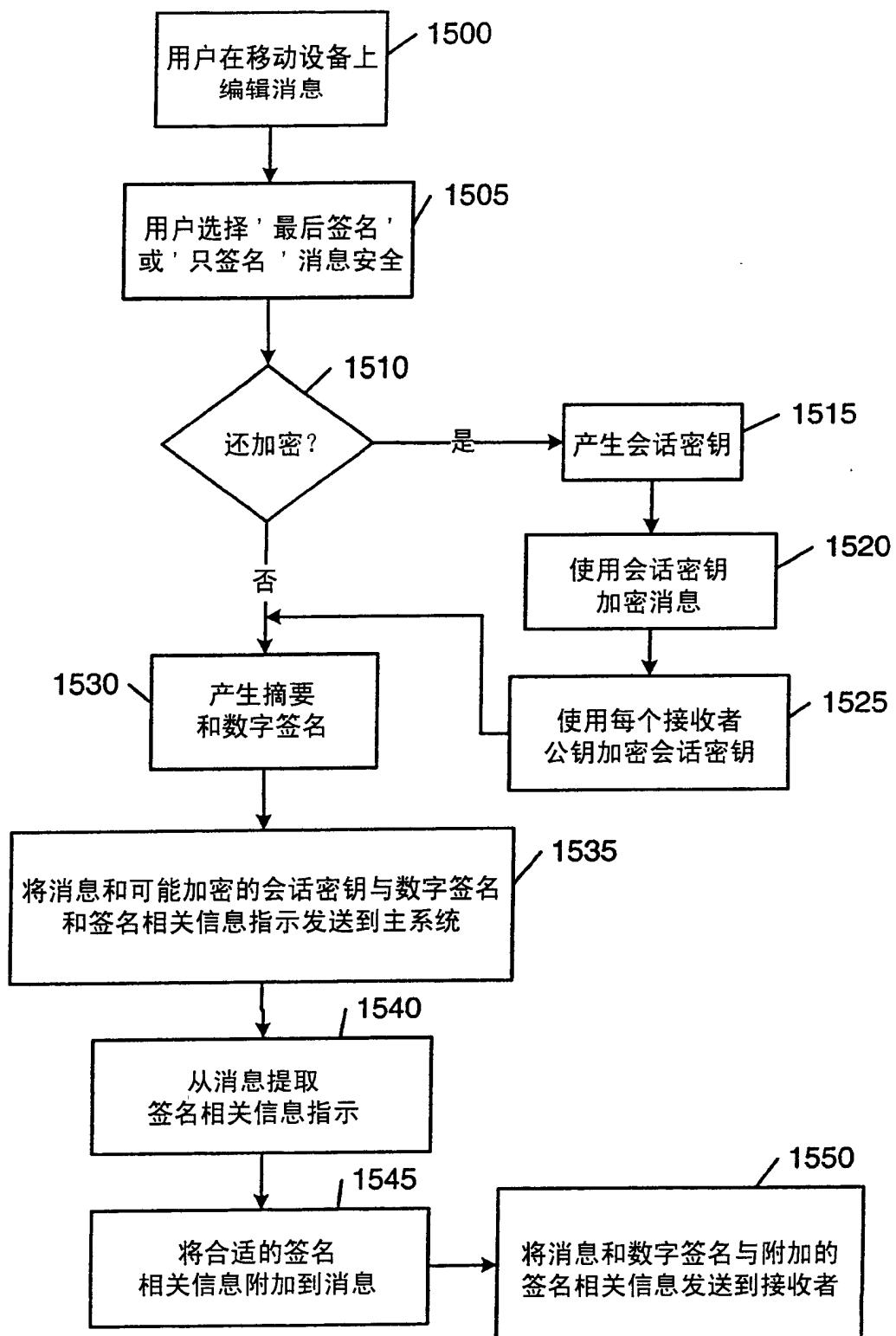


图 15

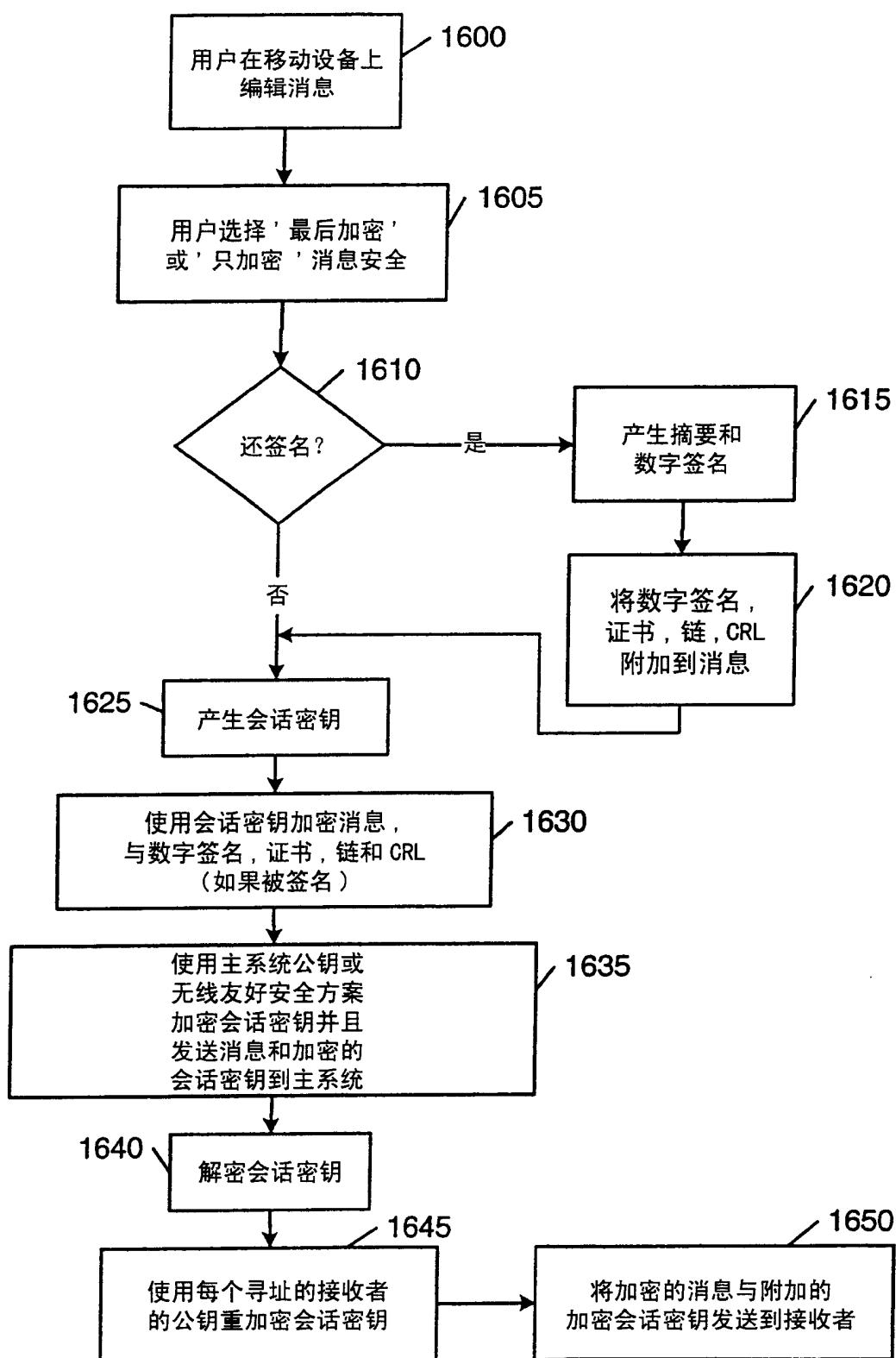


图 16

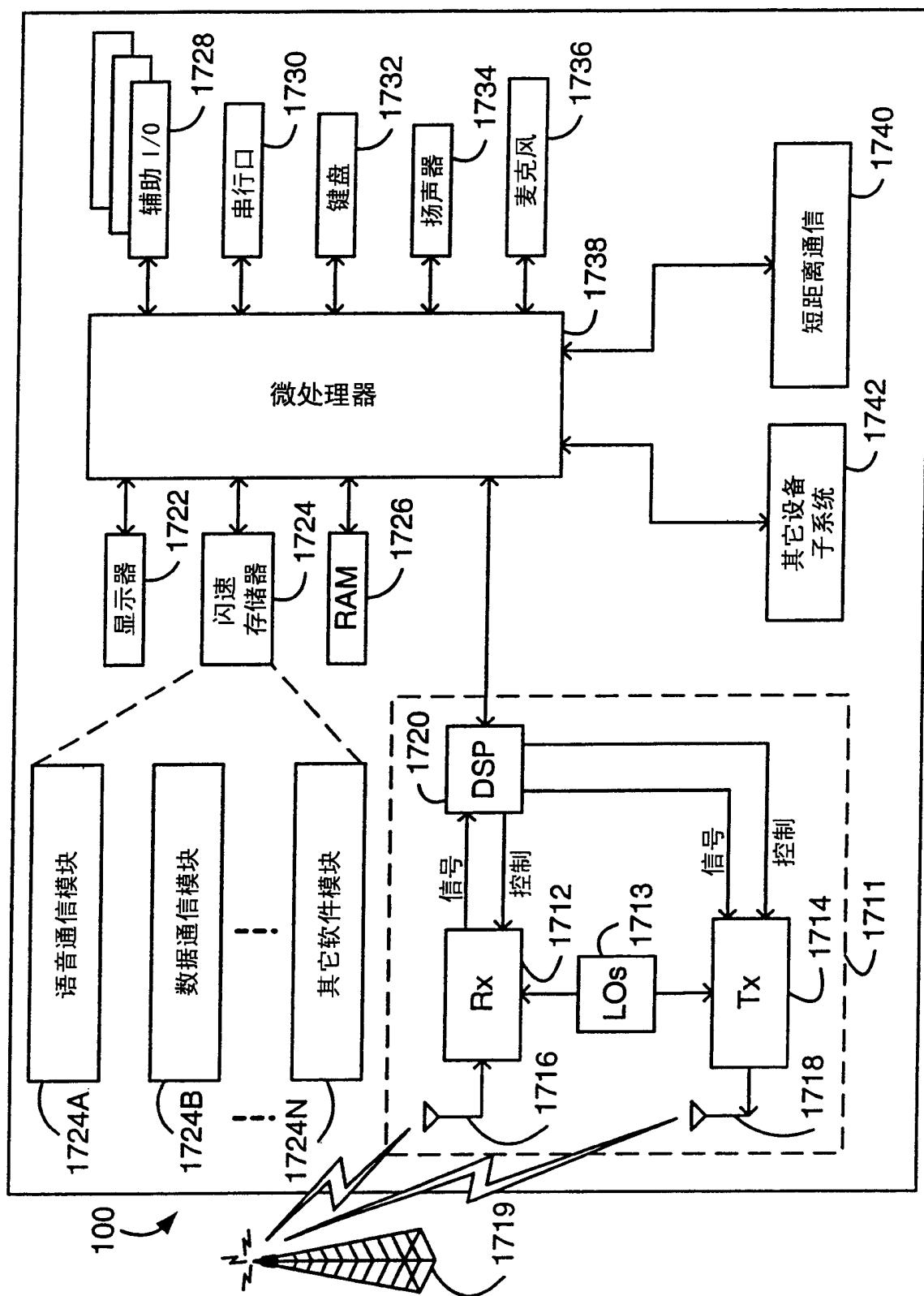


图 17

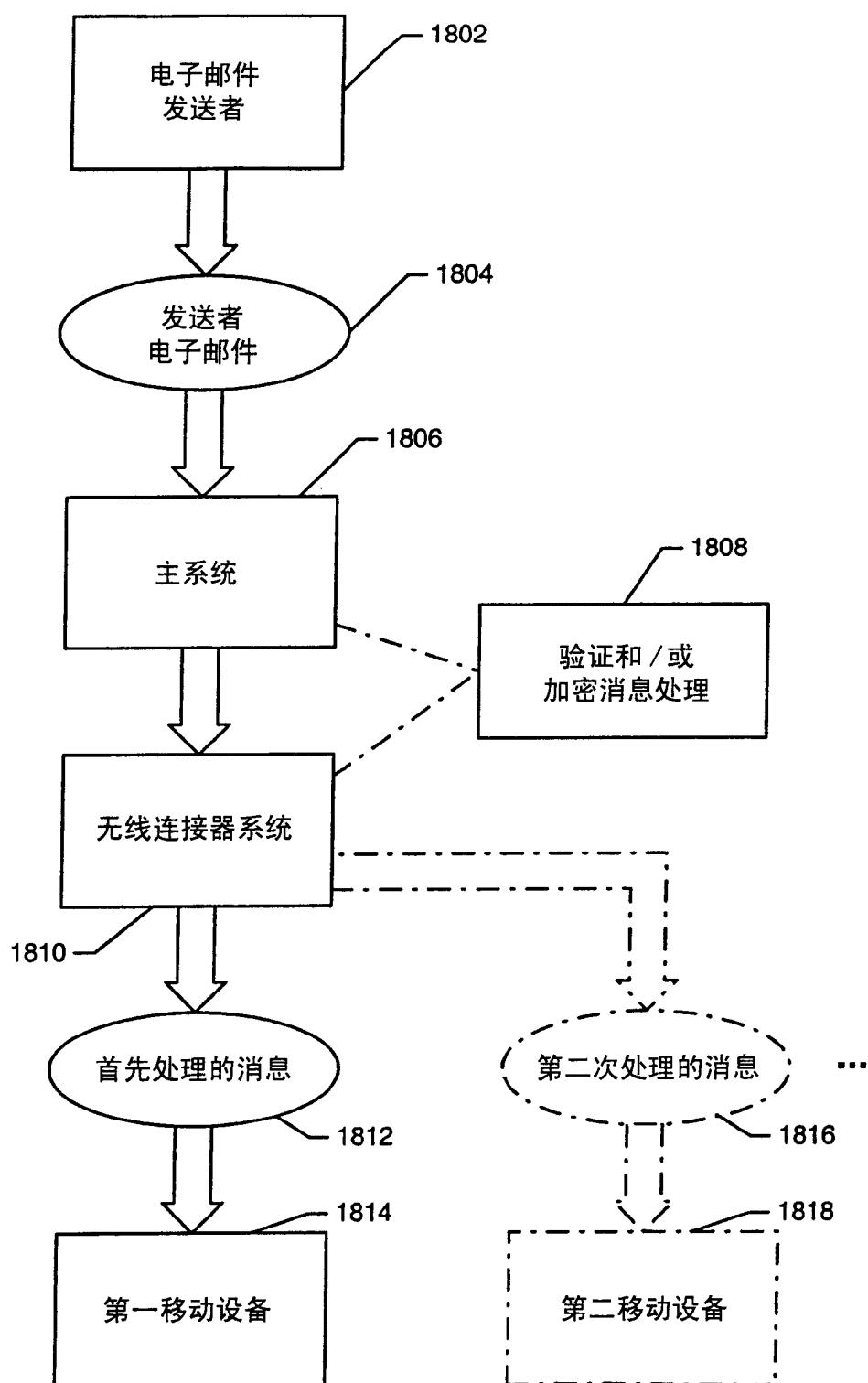


图 18

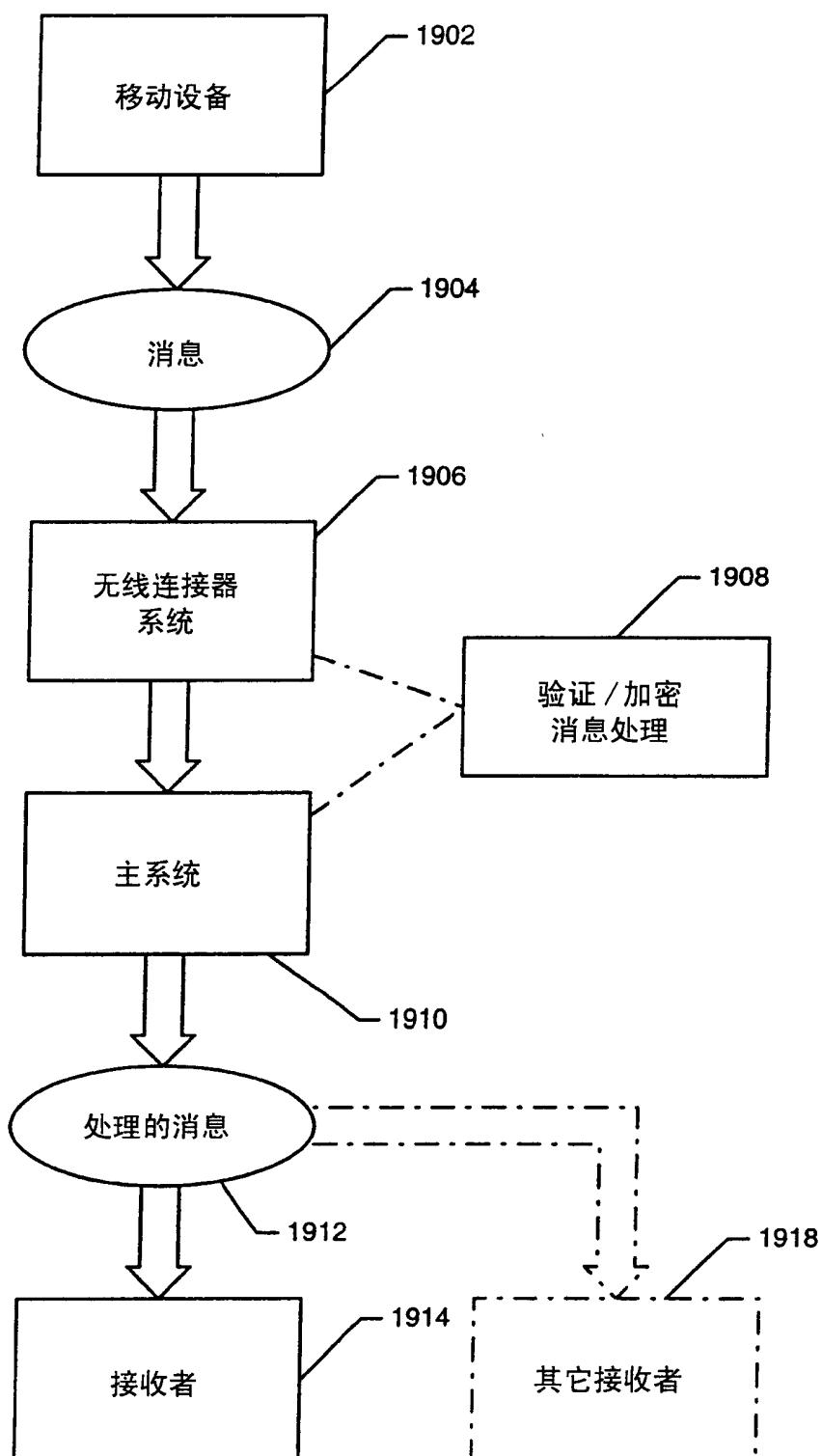


图 19

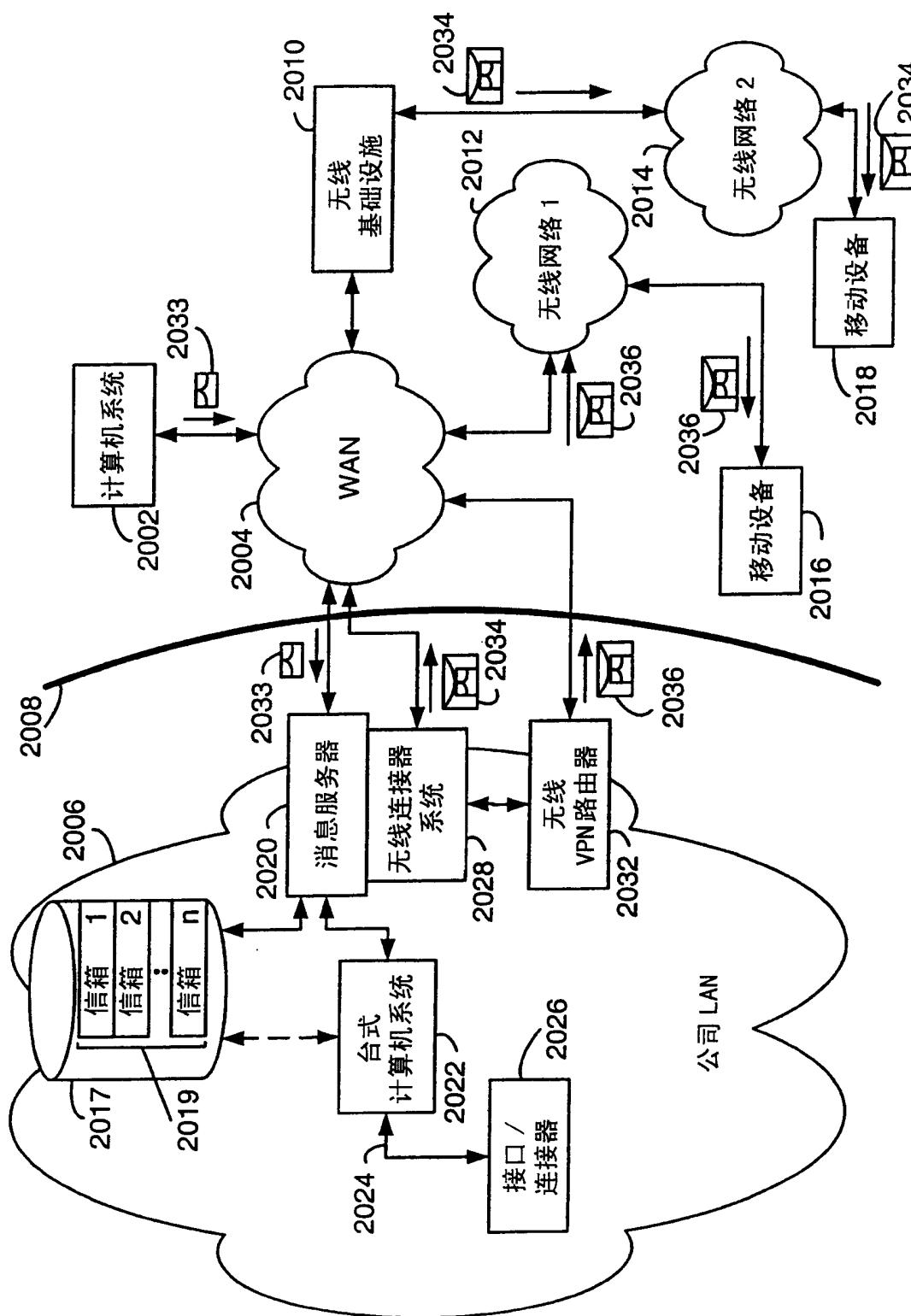
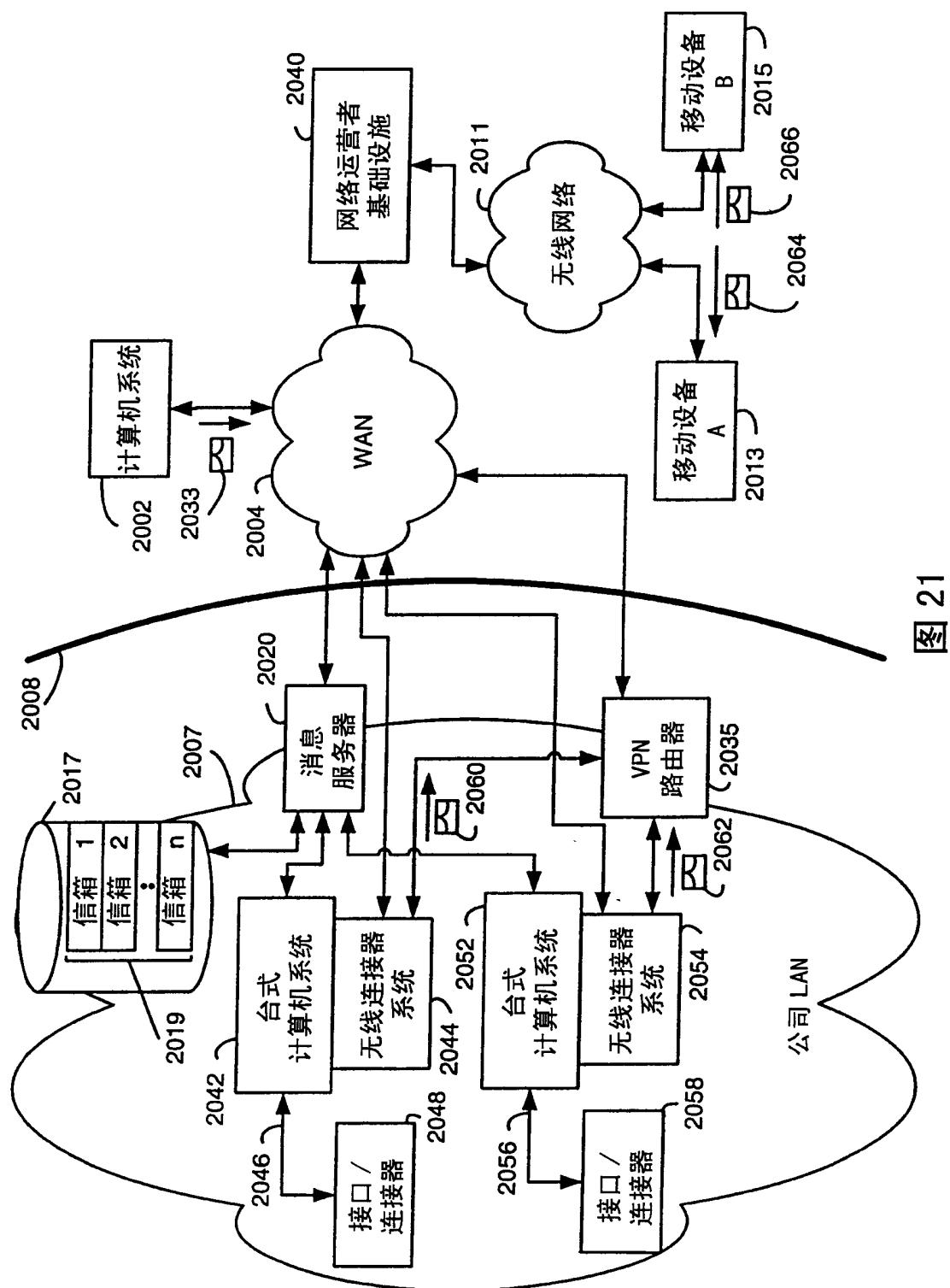


图 20



21

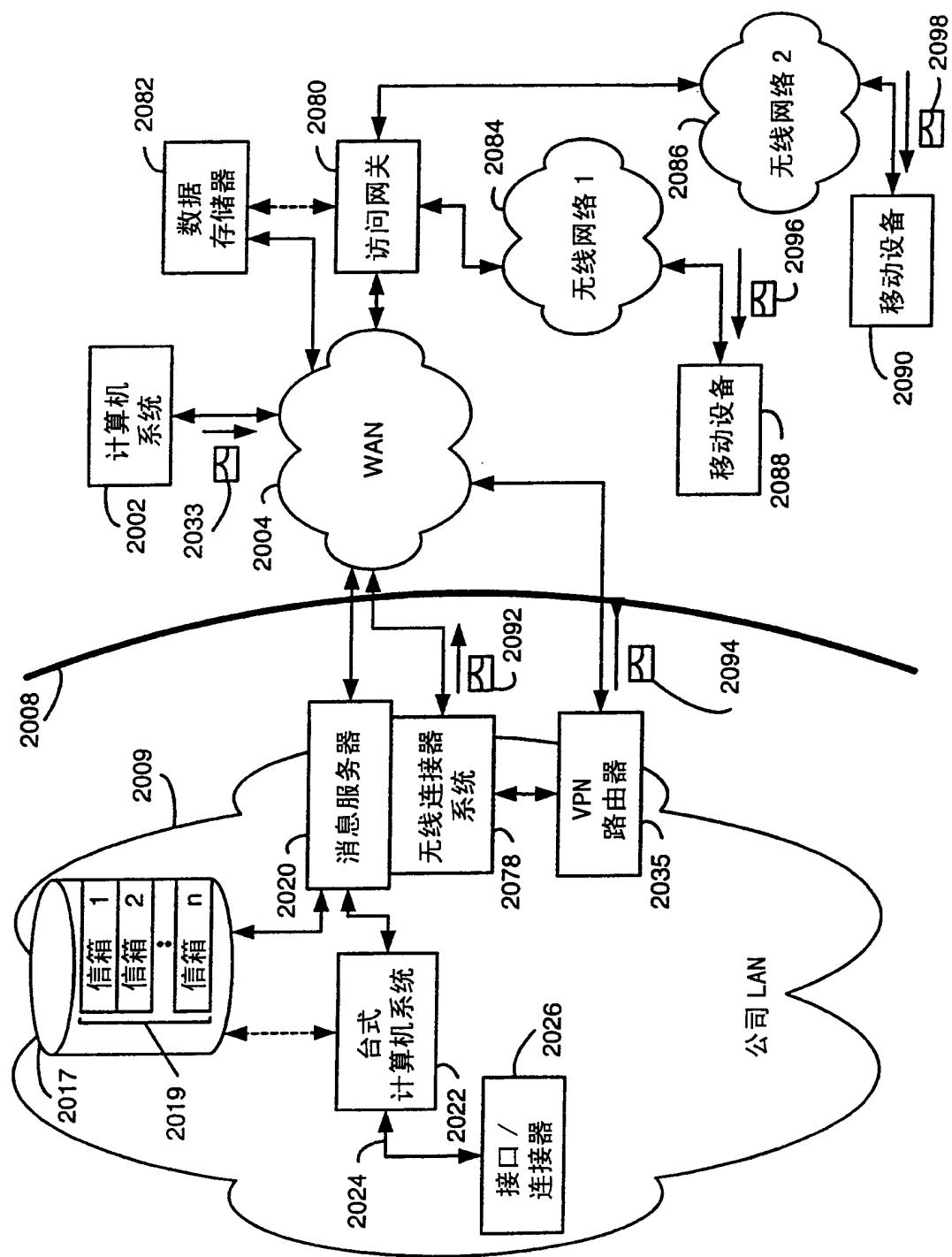


图 22