(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 101416458 B
(45)授权公告日 2011.12.21

(21)申请号 200780012193.0
(22)申请日 2007.04.03
(30)优先权数据
0606686.4 2006.04.03 GB
(85)PCT申请进入国家阶段日
2008.10.06
(86)PCT申请的申请数据
PCT/GB2007/001220 2007.04.03
(87)PCT申请的公布数据
WO2007/113547 EN 2007.10.11
(73)专利权人 趋势科技(加密技术)有限公司
地址 英国布里斯托尔
(72)发明人 安德鲁·当塞 马克·希姆利
(74)专利代理机构 北京德琦知识产权代理有限公司 11018
代理人 罗正云 王琦
(51)Int.Cl.
H04L 12/58(2006.01)
H04L 29/06(2006.01)
(56)对比文件
CN 1338693 A,2002.03.06,
US 6904521 B1,2005.06.07,
US 2004148500 A1,2004.07.29,
CN 1319976 A,2001.10.31,
审查员 张翠玲

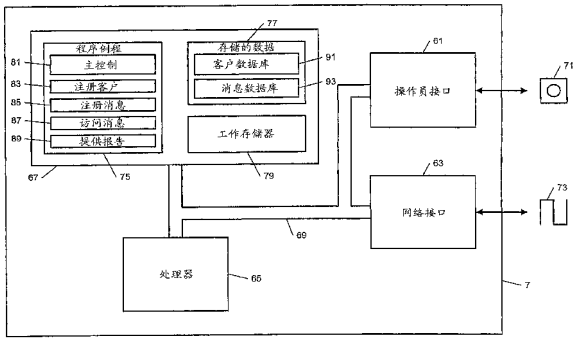
权利要求书 5 页 说明书 12 页 附图 9 页

(54)发明名称

电子数据通信系统

(57)摘要

描述了一种电子邮件消息接发系统，其中多个用户计算机通过因特网连接至邮件注册服务器。邮件注册服务器储存多个解密数据集合，每个集合需用于对对应的已加密电子邮件消息进行解密。在接收到已加密电子邮件后，用户计算机即与邮件注册服务器进行通信，以实现使用由邮件注册服务器储存的解密数据对对应已加密电子邮件消息的解密。以此方式，对电子邮件消息的访问可以由邮件注册服务器监视。



CN 101416458 B

1. 一种通信网络，用于从发送方将电子邮件消息可跟踪地安全传达到接收方，包括连接到邮件注册服务器、发送方设备和接收方设备的网络，

其中所述发送方和所述接收方各自具有用于对数据进行非对称加密和解密的公共和私有加密密钥；

其中所述邮件注册服务器包括：

从发送方设备接收对已加密电子邮件消息的跟踪密钥和跟踪代码的请求的装置；

响应于来自发送方设备的请求而生成跟踪密钥和跟踪代码的装置；

储存所述跟踪代码、所述跟踪密钥和标识该已加密电子邮件消息的所述发送方和接收方的数据的装置；

向所述发送方设备发送所述跟踪密钥及其相应的跟踪代码的装置；

从所述接收方接收包括跟踪密钥和基于所述接收方的私有加密密钥的验证信息的请求的装置；

使用所述验证信息和所述接收方的公共加密密钥验证所述接收方的装置；

从存储器中取回与从经验证的接收方接收的跟踪代码相对应的跟踪密钥的装置；

向所述经验证的接收方发送所取回的跟踪密钥的装置；

向所述发送方发送确认所述跟踪密钥已发送到所述经验证的接收方的消息的装置；

并且其中所述发送方设备包括：

用于输入消息数据的输入装置；

用于向所述邮件注册服务器提供标识已加密电子邮件消息的所述发送方和接收方的数据的装置；

用于从所述邮件注册服务器请求并从所述邮件注册服务器接收该邮件消息的跟踪代码和对应的跟踪密钥的装置；

用于使用会话密钥对所述消息数据进行对称加密的装置；

用于使用所接收的跟踪密钥对所述会话密钥进行加密以产生中间密钥的装置；

用于使用所述消息的接收方的公共密钥对所述中间密钥进行非对称加密以产生已加密中间密钥的装置；

用于向所述接收方设备发送包括所述已加密消息数据、所述已加密中间密钥和所述跟踪代码的已加密电子邮件消息的装置；以及

从所述邮件注册服务器接收确认所述跟踪密钥已发送到所述接收方的消息的装置；

并且其中所述接收方设备包括：

用于从所述发送方设备接收包括已加密消息数据、所述已加密中间密钥和所述跟踪代码的已加密电子邮件消息的装置；

用于使用所述接收方的私有密钥对所述已加密中间密钥进行非对称解密以取回所述中间密钥的装置；

向所述邮件注册服务器发送对与所接收的跟踪代码相对应的跟踪密钥的请求和基于所述接收方的私有密钥的验证信息的装置；

从所述邮件注册服务器接收与所接收的跟踪代码相对应的跟踪密钥的装置；

用于使用所接收的跟踪密钥对所述中间密钥进行解密以复原所述会话密钥的装置；以及

利用所述会话密钥对所述消息数据进行解密的装置。

2. 根据权利要求 1 所述的通信网络，其中所述邮件注册服务器储存已加密电子邮件消息的跟踪代码和对应的跟踪密钥，以及该已加密电子邮件消息的接收方电子邮件地址列表；并且

其中所述发送方设备中的用于对所述中间密钥进行非对称加密的装置使用该消息的各个预期接收方的相应公共密钥来产生针对该接收方的已加密中间密钥；并且

其中响应于接收到对与已加密电子邮件消息相对应的跟踪密钥进行访问的请求，所述邮件注册服务器验证该请求发自所列出的所述对应已加密电子邮件消息的接收方之一。

3. 根据权利要求 1 所述的通信网络，其中所述邮件注册服务器储存已加密电子邮件消息的接收方电子邮件地址列表，以及所列出的各个电子邮件地址的相应跟踪代码和对应的跟踪密钥，并且

所述发送方设备包括用于使用与接收方相对应的跟踪密钥来对与该接收方相对应的会话密钥进行加密以产生针对该接收方的中间密钥的装置；

其中所述发送方设备中的用于对所述中间密钥进行非对称加密的装置使用该消息的接收方的相应公共密钥来产生针对该接收方的已加密中间密钥；并且

其中响应于接收到对与所列出的电子邮件地址所关联的跟踪代码相对应的跟踪密钥进行访问的请求，所述邮件注册服务器验证该请求发自与所述对应已加密电子邮件消息的跟踪代码相对应的电子邮件地址。

4. 根据权利要求 2 或 3 所述的通信网络，其中所述邮件注册服务器包括在预定时间向所述发送方设备发送表示跟踪密钥已发送到的接收方的电子邮件地址的消息的装置。

5. 根据权利要求 1-3 中任一项所述的通信网络，其中所述邮件注册服务器通过检查由使用与所述接收方相关联的公共密钥的接收方提供的数字签名，来验证该接收方。

6. 根据权利要求 5 所述的通信网络，其中所述邮件注册服务器使用与该接收方相关联的标识信息来计算该接收方的公共密钥。

7. 根据权利要求 6 所述的通信网络，其中所述标识信息包括该接收方的电子邮件地址。

8. 根据权利要求 1 所述的通信网络，其中所述邮件注册服务器禁止在预定的时间之前传送电子邮件消息的所述跟踪密钥。

9. 根据权利要求 1 所述的通信网络，其中所述中间密钥和所述跟踪密钥是二进制数，并且其中复原所述会话密钥包括对所述中间密钥和所述跟踪密钥执行位异或运算。

10. 一种电子邮件注册服务器，包括：

网络接口，用于与远程网络设备通信；

从邮件发送方接收请求的装置；

响应于来自邮件发送方的请求而生成跟踪密钥和跟踪代码的装置；

被配置为储存多个跟踪代码的数据储存器，每个跟踪代码与相应的跟踪密钥和标识发送方和接收方的数据相关联；

向所述邮件发送方发送跟踪密钥及其相应的跟踪代码的装置；

从接收方接收包括跟踪代码和基于所述接收方的私有加密密钥的验证信息的请求的装置；

使用来自所述接收方的验证信息和所述接收方的公共加密密钥来验证所述接收方的装置；

从存储器中取回与从经验证的接收方接收的跟踪代码相对应的跟踪密钥的装置；

向所述经验证的接收方发送所取回的跟踪密钥的装置；以及

向所述邮件发送方发送确认所述跟踪密钥已发送到所述经验证的接收方的消息的装置。

11. 根据权利要求 10 所述的电子邮件注册服务器，其中发送所取回的跟踪密钥的装置禁止在预定的时间之前传送电子邮件消息的跟踪密钥。

12. 根据权利要求 10 或 11 所述的电子邮件注册服务器，其中所述数据储存器被配置为储存各自与相应跟踪密钥和标识该已加密电子邮件消息的邮件发送方和接收方列表的数据相关联的跟踪代码，并且

响应于接收到对与已加密电子邮件消息相对应的跟踪密钥进行访问的请求，所述邮件注册服务器验证所述请求发自所列出的所述对应已加密电子邮件消息的接收方之一。

13. 根据权利要求 10 或 11 所述的电子邮件注册服务器，其中该数据储存器被配置为储存标识已加密电子邮件消息的邮件发送方、该已加密电子邮件消息的接收方电子邮件地址列表以及与各个接收方地址的相应跟踪密钥相关联的相应跟踪代码的数据；并且

其中响应于接收到跟踪代码和对与已加密电子邮件消息的接收方地址相对应的跟踪密钥的请求，所述邮件注册服务器验证该请求发自所列出的与该跟踪代码和跟踪密钥相对应的接收方。

14. 根据权利要求 12 所述的电子邮件注册服务器，其中所述邮件注册服务器包括在预定时间向所述邮件发送方发送表示跟踪密钥已发送到的所述接收方电子邮件地址的消息的装置。

15. 根据权利要求 10 所述的电子邮件注册服务器，其中所述邮件注册服务器通过使用与所述接收方相关联的公共密钥检查由所述接收方提供的数字签名来验证所述接收方。

16. 根据权利要求 15 所述的电子邮件注册服务器，其中所述邮件注册服务器使用与所述接收方相关联的标识信息来计算所述接收方的公共密钥。

17. 根据权利要求 16 所述的电子邮件注册服务器，其中所述标识信息包括该接收方的电子邮件地址。

18. 一种网络设备，包括：

网络接口，用于向远程网络设备发送数据，并从远程网络设备接收数据；

用于从邮件发送方接收发往接收方的已加密电子邮件消息的装置，所述已加密电子邮件消息包括已加密消息数据、已加密中间密钥和跟踪代码；

用于使用所述接收方的私有密钥对所述已加密中间密钥进行非对称解密以取回所述中间密钥的装置；

向邮件注册服务器发送对跟踪密钥的请求的装置，该请求包括所接收的跟踪代码和基于所述接收方的私有密钥的验证信息；

从所述邮件注册服务器接收与所接收的跟踪代码相对应的跟踪密钥的装置；

用于使用所接收的跟踪密钥对所述中间密钥进行解密以产生会话密钥的装置；以及

使用所述会话密钥对所述消息数据进行解密的装置。

19. 根据权利要求 18 所述的网络设备，其中所述验证信息包括数字签名。

20. 根据权利要求 18 或 19 所述的网络设备，其中所述中间密钥和所述跟踪密钥是二进制数，并且其中复原所述会话密钥包括对所述中间密钥和所述跟踪密钥执行位异或运算。

21. 一种通过网络设备连接到的网络从发送方向接收方可跟踪地安全传达电子邮件消息的方法，所述网络设备包括邮件注册服务器、发送方设备和接收方设备，其中所述发送方和所述接收方各自具有用于对数据进行非对称加密和解密的公共和私有加密密钥，该方法包括：

在发送方设备处输入消息数据；

从所述发送方设备向所述邮件注册服务器发送标识已加密电子邮件消息的接收方的数据，并且从所述邮件注册服务器请求该邮件消息的跟踪代码和对应的跟踪密钥；

响应于来自所述发送方设备的请求，在所述邮件服务器中生成跟踪密钥和跟踪代码；

在所述邮件服务器中的存储器中储存所述跟踪代码和对应的跟踪密钥以及标识该加密电子邮件消息的所述发送方和接收方的数据，并且向所述发送方设备发送所述跟踪密钥及其相应的跟踪代码；

在所述发送方设备中使用会话密钥对所述消息数据进行对称加密；

在所述发送方设备中使用所接收的跟踪密钥对所述会话密钥进行加密以产生中间密钥；

在所述发送方设备中使用所述消息的预期接收方的公共密钥对所述中间密钥进行非对称加密以产生已加密中间密钥；

从所述发送方设备向所述接收方设备发送包括已加密消息数据、所述已加密中间密钥和所述跟踪代码的已加密电子邮件消息；

在所述接收方设备中从所述发送方设备接收包括所述已加密消息数据和所述已加密中间密钥和所述跟踪代码的已加密电子邮件消息；

在所述接收方设备中使用所述接收方的私有密钥对所述已加密中间密钥进行非对称解密以取回所述中间密钥；

从所述接收方设备向所述邮件注册服务器发送对与所接收的跟踪代码相对应的跟踪密钥的请求和基于所述接收方的私有密钥的验证信息；

在所述邮件服务器中从接收方设备接收包括所述跟踪代码和基于所述接收方的私有加密密钥的验证信息的请求；

在所述邮件服务器中使用来自所述接收方设备的验证信息和所述接收方的公共加密密钥来验证所述接收方；

从所述存储器中取回与从经验证的接收方接收的跟踪代码相对应的跟踪密钥；

从所述邮件服务器向所述经验证的接收方发送所取回的跟踪密钥；以及

从所述邮件服务器向所述发送方发送确认所述跟踪密钥已发送到所述经验证的接收方的消息；

在所述接收方设备处从所述邮件注册服务器接收与所取回的跟踪代码相对应的跟踪密钥；

在所述接收方设备中使用所接收的跟踪密钥对所述中间密钥进行解密以复原所述会话密钥；以及

在所述接收方设备中使用所复原的会话密钥对所述消息数据进行解密。

22. 根据权利要求 21 所述的方法，其中：

所述发送方设备向所述邮件注册服务器发送标识多个接收方的数据；

所述邮件注册服务器储存标识发送方、接收方列表、跟踪密钥和跟踪代码的数据；

所述发送方设备使用所述消息的各个接收方的公共密钥对所述中间密钥进行非对称加密，以针对各个接收方设备产生相应的已加密中间密钥；以及

所述发送方设备向所述接收方发送包括所述已加密消息数据、所述已加密中间密钥和所述跟踪代码的已加密电子邮件消息。

23. 根据权利要求 21 所述的方法，其中：

所述发送方设备向所述邮件注册服务器发送标识多个接收方的数据；

所述邮件注册服务器储存标识所述发送方设备、所述多个接收方和各个接收方的相应跟踪密钥和跟踪代码的数据；

所述发送方设备使用各个接收方的相应跟踪密钥对所述会话密钥进行加密，以针对各个接收方产生相应的中间密钥；

所述发送方设备使用各个接收方的公共密钥对相应的中间密钥进行非对称加密，以针对各个接收方产生已加密中间密钥；以及

所述发送方设备向所述接收方发送包括所述已加密消息数据、所述已加密中间密钥和所述跟踪代码的已加密电子邮件消息。

24. 根据权利要求 21 或 22 所述的方法，其中所述中间密钥和所述跟踪密钥是二进制数，并且其中对所述中间密钥进行解密以复原所述会话密钥包括对所述中间密钥和所述跟踪密钥执行位异或运算。

25. 根据权利要求 21 所述的方法，其中所述邮件注册服务器在延迟预定的时间之后才将电子邮件消息的跟踪密钥发送到所述接收方设备。

电子数据通信系统

技术领域

[0001] 本发明涉及电子数据通信系统和电子通信系统的部件。本发明与用于以电子方式向人发送邮件消息并从人接收邮件消息的系统具有特别相关性。

背景技术

[0002] 电子邮件消息接发 (messaging) 涉及正被发送到一电子邮件地址的电子邮件消息，其该电子邮件地址将该电子邮件消息指向一虚拟邮箱。这种电子邮件消息接发的使用正在变得越来越广泛，而这种电子邮件消息接发主要使用诸如 Microsoft Outlook 之类的电子邮件程序。传统电子邮件程序的问题在于所发送的邮件可能会被拦截和读取。

[0003] 已存在使用公共密钥密码技术对电子邮件消息进行加密的建议，在该公共密钥密码技术中使用非对称加密算法。具体来说，发送方使用与电子邮件消息的接收方相关联的公共密钥来对该消息进行加密。得到的加密后的消息仅能够使用与公共密钥不同的私有密钥进行解密，且对该私有密钥的访问由该消息的接收方控制。

[0004] 公共密钥加密技术不但保证消息仅由期望的接收方读取，还能够使消息的作者和消息内容得到验证。具体来说，可以给该消息添加数字签名，该数字签名通过使用发送方的私有密钥来签署该消息的单向散列 (one-way hash) 而形成。然后，该消息的接收方能够使用该发送方的数字签名和公共密钥，来生成所接收消息的单向散列并对发送方的身份和该消息的内容进行验证。

[0005] 与使用同一种加密密钥进行加密和解密的对称加密算法相比，在公共密钥加密技术中使用的非对称加密算法较慢。该问题针对电子邮件消息接发先前已经通过采用所谓的 KEM-DEM 方法得到了解决，在 KEM-DEM 方法中，加密后的电子邮件消息由密钥封装机制 (KEM) 部分和数据封装机制 (DEM) 部分形成，其中密钥封装机制 (KEM) 部分存储使用接收方的公共密钥进行加密的会话密钥（该会话密钥对该消息来说是独一无二的），数据封装机制 (DEM) 部分存储由使用在 KEM 部分中存储的会话密钥作为加密密钥的对称加密算法进行加密的电子邮件消息。以此方式，由非对称加密算法执行的加密量和解密量得到了减少。

[0006] 在特定情况下，期望知道何时消息已被接收和访问。在如何获取这种针对加密电子邮件的确认上存在技术问题。本发明提供一种新颖且有益的解决方案来解决该问题。

发明内容

[0007] 根据本发明，提供一种电子邮件消息接发系统，其中多个用户计算机通过因特网连接至邮件注册服务器。邮件注册服务器存储多组解密数据，每组是对与对应已加密电子邮件消息相关联的已加密的加密数据进行解密所必需的。紧随已加密电子邮件消息的接收，用户计算机与邮件注册服务器进行通信，以使用由邮件注册服务器存储的对应解密数据来实现对已加密的加密数据的解密。以此方式，对电子邮件消息的访问就能够被邮件注册服务器监视。此外，解密数据用于为已加密电子邮件消息转换已加密的加密数据，而不用于对加密电子邮件消息本身进行解密。因此邮件注册服务器不具有已加密电子邮件消息的

解密数据。

附图说明

[0008] 现在将参考附图描述本发明的示例性实施例，在附图中：

[0009] 图 1 示意性地示出根据本发明的电子邮件消息接发系统的主要部件；

[0010] 图 2 示意性地示出形成图 1 所示电子邮件消息接发系统的一部分的加密授权服务器的主要部件；

[0011] 图 3 示意性地示出形成图 1 所示电子邮件消息接发系统的一部分的邮件注册授权服务器的主要部件；

[0012] 图 4 示意性地示出形成图 1 所示电子邮件消息接发系统的一部分的用户计算机的主要部件；

[0013] 图 5 示意性地示出形成图 4 所示用户计算机的一部分的电子邮件程序的加密插件的主程序例程；

[0014] 图 6 示意性地示出与存储在图 4 所示用户计算机中的加密插件相关联的数据的映射；并且

[0015] 图 7A 至 7D 示出示意性地显示在图 1 所示电子邮件消息接发系统中，将加密后的注册电子邮件从发送方发送到接收方所要执行的主要步骤的流程图。

具体实施方式

[0016] 系统概述

[0017] 如图 1 所示，在图示的实施例中，电子邮件消息接发系统具有多个连接至因特网 3 的用户计算机，其中为方便图示，仅示出发送计算机 1a 和接收计算机 1b。加密授权服务器 5 和邮件注册授权服务器 7 也连接至因特网 3。

[0018] 加密授权服务器 5 给用户计算机 1 提供加密密钥。具体来说，在该实施例中，加密授权服务器 5 发布为 WO03/017559 中所描述的加密算法提供根公共密钥$\mathbf{K}_{\mathrm{pub}}^{\mathrm{G}}$的公共密钥证书，该专利的全部内容通过引用合并于此。根据该加密算法，具有电子邮件地址“client_ID”的客户的公共密钥$\mathbf{K}_{\mathrm{pub}}^{\mathrm{c}}$可以由以下公式给出：

[0019] $$K_{pub}^{c} = F(client\_ID, K_{pub}^{G})$$

[0020] 其中，F 是可公开获得的函数。以此方式，任何知道客户的电子邮件地址、加密授权的根公共密钥$\mathbf{K}_{\mathrm{pub}}^{\mathrm{G}}$和函数 F（这些都是可公开获得的）的人都可以计算出与该客户相关联的公共密钥$\mathbf{K}_{\mathrm{pub}}^{\mathrm{c}}$

[0021] 与客户相关联的私有密钥仅能够在知道根私有密钥$\mathbf{K}_{\mathrm{pri}}^{\mathrm{G}}$的情况下被计算出，该根私有密钥$\mathbf{K}_{\mathrm{pri}}^{\mathrm{G}}$由对加密授权服务器 5 进行管理的加密机构保密。具体来说，具有电子邮件地址“client_ID”的客户的私有密钥$\mathbf{K}_{\mathrm{pri}}^{\mathrm{c}}$由加密授权服务器 5 根据以下关系计算出：

[0022] $$K_{pri}^{c} = G(client\_ID, K_{pri}^{G})$$

[0023] 其中，G 是与 F 配对的函数。

[0024] 在说明书的所有剩余部分中，除非另外指出，引用使用公共密钥被非对称加密的

数据意味着，该数据使用 WO03/017559 中所描述的、以公共密钥形成加密密钥的非对称加密算法被加密，并且类似地，引用使用私有密钥被非对称解密的数据意味着，该数据使用 WO03/017559 中所描述的、以私有密钥形成加密密钥的非对称加密算法被解密。

[0025] 在整个说明书中，还会引用使用对称密钥被对称加密或对称解密的数据。除非特别指出，这是指使用将对称密钥用作加密密钥的高级加密标准 (AES) 算法对该数据进行的加密或解密。

[0026] 在该实施例中，当发送计算机 1a 用于向与接收计算机 1b 相关联的接收方发送电子邮件时，使用 KEM-DEM 方法的变型，其中该消息的接收方必须从邮件注册授权服务器 7 下载跟踪密钥，以便复原对该消息的 DEM 部分进行解密所需的会话密钥。具体来说，当发送消息时，发送方向邮件注册授权服务器 7 注册该消息，并且邮件注册授权服务器 7 向发送方发送跟踪代码和跟踪密钥。发送方使用该跟踪密钥来生成加密后的消息，并将该跟踪代码与该加密后的消息一起发送出去。接收方一旦接收到该加密后的消息，即向邮件注册授权服务器 7 发送跟踪代码和身份证明，邮件注册授权服务器 7 向接收方发送对该消息进行解密所需的跟踪密钥作为答复。

[0027] 现在将更详细地描述加密授权服务器 5、邮件注册授权服务器 7 和用户计算机 1。

[0028] 加密授权服务器

[0029] 如图 2 所示，加密授权服务器 5 具有通过总线系统 29 互连的操作员接口 21、网络接口 23、处理器 25 和存储器 27。

[0030] 操作员接口 21 包括供操作员将数据输入加密授权服务器 5 的键盘（未示出）和允许操作员读取加密授权服务器 5 所产生的数据的显示器（未示出）。操作员接口 21 还包括 CD-ROM 读写器（未示出），通过该 CD-ROM 读写器，储存在 CD-ROM31 上的数据可以被输入到加密授权服务器 5，由加密授权服务器 5 产生的数据也可以被写入到可记录的 CD-ROM31。

[0031] 网络接口 23 以网络信号 33 的形式从因特网 3 接收数据且向因特网 3 输出数据。

[0032] 处理器 25 根据储存在存储器 27 中的程序例程执行处理操作。这些程序例程可以在生产过程中储存，也可以通过操作员接口 21 或网络接口 23 输入到加密授权服务器 5。程序例程处理储存在存储器 27 中的数据和由加密授权服务器 5 通过操作员接口 21 和网络接口 23 接收的数据。

[0033] 存储器 27 由不同类型的分别具有不同访问时间的存储器形成，并且采用传统的处理技术通过预先将可能会需要的数据缓存到快速访问时间存储器中来改进处理速度。

[0034] 存储器 27 包括储存加密授权服务器 5 所使用的程序例程的区域 35、储存数据的区域 37 和提供工作存储的区域 39。

[0035] 具体来说，程序例程存储区域 35 储存：

[0036] -Master_Control（主控制）例程 41；

[0037] -Key_maintenance（密钥维护）子例程 43；

[0038] -Register_Client（注册客户）子例程 45；

[0039] -Calculate_Private_Key（计算私有密钥）子例程 47；和

[0040] -Supply_Root_Public_Key（供应根公共密钥）子例程 49。

[0041] 所储存数据的存储区域 37 储存：

[0042] - 客户数据库 51；和

[0043] - 密钥数据库 53。

[0044] 主控制例程 41 协调加密授权服务器 5 的操作。这包括在需要时执行子例程。

[0045] 应该理解，用户私有密钥的安全性依赖于保密的根私有密钥 $\mathbf{K}_{pri}^{G}$。作为防范措施，在该实施例中，密钥维护子例程被周期性地执行以生成新的核心公共密钥和私有密钥，这些新生成的密钥与旧的公共密钥和私有密钥一起被储存在密钥数据库 53 中。具体来说，密钥数据库 53 储存指示核心公共密钥和私有密钥对以及针对每一对该对有效的时限的数据。

[0046] 注册客户子例程 45 由主控制子例程 41 响应于预期客户所接收的注册请求而启动。注册客户子例程 45 在客户数据库 51 中储存与该客户有关的数据，使用计算私有密钥子例程 45 来计算客户私有密钥，并将所计算出的客户私有密钥供应给该客户，其中计算私有密钥子例程 45 使用当前有效的核心私有密钥 K_{pri}^{G} 和该客户的电子邮件地址来计算客户私有密钥。接下来，每当密钥维护子例程 43 生成新的核心私有密钥 K_{pri}^{G} 时，密钥维护子例程 43 就使用计算私有密钥子例程 47 来基于新的核心私有密钥为每个客户计算新的客户私有密钥。

[0047] 供应根公共密钥子例程 49 由主控制例程 41 响应于对根公共密钥 $\mathbf{K}_{pub}^{G}$ 的请求而启动，并且为所请求的根公共密钥 $\mathbf{K}_{pub}^{G}$ 供应公共密钥证书。

[0048] 邮件注册授权服务器

[0049] 如图 3 所示，邮件注册授权服务器 7 具有通过总线系统 69 互连的操作员接口 61、网络接口 63、处理器 65 和存储器 67。

[0050] 操作员接口 61 包括供操作员将数据输入邮件注册授权服务器 7 的键盘（未示出）和允许操作员读取邮件注册授权服务器 7 所产生的数据的显示器（未示出）。操作员接口 61 还包括 CD-ROM 读写器（未示出），通过该 CD-ROM 读写器，储存在 CD-ROM71 上的数据可以被输入到邮件注册授权服务器 7，由邮件注册授权服务器 7 所产生的数据也可以被写入到可记录 CD-ROM71 上。

[0051] 网络接口 63 以网络信号 73 的形式从因特网 3 接收数据且向因特网 3 输出数据。

[0052] 处理器 75 根据储存在存储器 67 中的程序例程执行处理操作。这些程序例程可以在生产过程中储存，也可以通过操作员接口 61 或网络接口 63 输入到邮件注册授权服务器 7。程序例程处理储存在存储器 67 中的数据和由邮件注册授权服务器 7 通过操作员接口 61 和网络接口 63 接收的数据。

[0053] 存储器 67 由不同类型的分别具有不同访问时间的存储器形成，并且采用传统的处理技术通过预先将可能会需要的数据缓存到快速访问时间存储器中来改进处理速度。

[0054] 存储器 67 包括储存邮件注册授权服务器 7 所使用的程序例程的区域 75、储存数据的区域 77 和提供工作存储的区域 79。

[0055] 具体来说，程序例程存储区域 75 储存：

[0056] -Master_Control（主控制）例程 81；

[0057] -Register_Client（注册客户）例程 83；

[0058] -Register_Message（注册消息）子例程 85；

[0059] -Access_Message(访问消息)子例程 87;和

[0060] -Provide_Report(提供报告)子例程 89。

[0061] 所储存数据的存储区域 77 储存:

[0062] - 客户数据库 91;和

[0063] - 消息数据库 93。

[0064] 客户数据库储存每个客户的细节,包括客户姓名、电子邮件地址、登录密码和账户细节。消息数据库储存每个已注册消息的细节,包括发送该消息的客户、该消息的唯一跟踪代码、注册服务的类型、该消息的接收方、跟踪密钥和标识每个接收方何时取回跟踪密钥的信息。

[0065] 主控制例程 81 在需要时使用子例程来控制邮件注册授权服务器的操作。

[0066] 注册客户子例程 83 由主控制例程 81 来启动,以便在客户数据库 91 中注册新客户的细节。剩余的子例程将在后面进行详细讨论。

[0067] 用户计算机

[0068] 现在将参考图 4 至 6 来描述诸如发送计算机 1a 和接收计算机 1b 的用户计算机 1 的主要部件。

[0069] 如图 4 所示,用户计算机 1 具有通过总线系统 109 互连的操作员接口 101、网络接口 103、处理器 105 和存储器 107。

[0070] 操作员接口 101 包括供操作员将数据输入用户计算机 1 的键盘(未示出)和允许操作员读取用户计算机 1 所产生的数据的显示器(未示出)。操作员接口 101 还包括 CD-ROM 读写器(未示出),通过该 CD-ROM 读写器,储存在 CD-ROM111 上的数据可以被输入到用户计算机 1,由用户计算机 1 产生的数据也可以被写入到可记录的 CD-ROM111 上。

[0071] 网络接口 103 以网络信号 113 的形式从因特网 3 接收数据且向因特网 3 输出数据。

[0072] 处理器 105 根据储存在存储器 107 中的程序例程执行处理操作。这些程序例程可以在生产过程中储存,也可以通过操作员接口 101 或网络接口 103 输入到用户计算机 1。程序例程处理储存在存储器 107 中的数据和由用户计算机 1 通过操作员接口 101 和网络接口 103 接收的数据。

[0073] 存储器 107 由不同类型的分别具有不同访问时间的存储器形成,并且采用传统的处理技术通过预先将可能会需要的数据缓存到快速访问时间存储器中来改进处理速度。

[0074] 存储器 107 包括储存用户计算机 1 所使用的程序例程的区域 115、储存数据的区域 117 和提供工作存储的区域 119。

[0075] 具体来说,除其它程序之外,程序例程存储区域 107 储存:

[0076] - 诸如 Microsoft Windows 的传统操作系统 119;

[0077] - 诸如 Microsoft Internet Explorer 的传统万维网浏览器 121;

[0078] - 包括加密插件 125 的电子邮件程序 123。

[0079] 除其它数据之外,所储存数据的存储区域储存:

[0080] - 储存与邮件注册服务器相关联的用户注册细节的用户数据 127;和

[0081] - 储存与加密插件 125 相关联的数据的加密数据 129。

[0082] 图 5 更详细地示出加密插件 125 的程序例程。正如所示,加密插件 125 包括:

[0083] -Master_Control(主控制)例程 141;

[0084] -Install_Encryption_Plug-in(安装加密插件)子例程 143;

[0085] -Encrypt_Message(加密消息)子例程 145;

[0086] -Decrypt_Message(解密消息)子例程 147;

[0087] -Encrypt_Registered_Message(加密已注册消息)子例程 149;和

[0088] -Decrypt_Registered_Message(解密已注册消息)子例程 151。

[0089] 图 6 更详细地示出加密数据 129。正如所示,加密数据 129 包括:

[0090] - 非对称密钥数据库 161;和

[0091] - 跟踪密钥数据库 163。

[0092] 非对称密钥数据库 161 储存用户公共密钥和私有密钥对,每个密钥对都与对应核心公共密钥 $\mathbf{K}_{pub}^{G}$、该密钥对和相关联的核心公共密钥有效的时限进行关联储存。

[0093] 传送密钥数据库 163 储存列出针对每个向邮件注册授权服务器 7 注册的电子邮件的对应跟踪代码和跟踪密钥的表格。

[0094] 主控制例程 141 根据需要使用子例程对加密插件 141 的操作进行控制。安装加密插件子例程在该计算机的用户最初向加密授权服务器 5 注册时被用,并将初始用户私有密钥和公共密钥对储存在密钥数据库 161 中。主控制例程 141 还控制由于加密授权服务器 5 更新核心公共密钥和私有密钥对而需要对用户公共密钥和私有密钥对进行的更新。

[0095] 加密消息子例程 145 在用户计算机 1 的用户希望发送未注册的已加密消息时被使用。加密消息子例程 145 生成该消息的随机会话密钥,然后使用所生成的会话密钥对该消息进行对称加密,以形成已加密消息的 DEM 部分。然后,加密消息子例程 145 计算与该消息的每个接收方相关联的公共密钥(使用该接收方的电子邮件地址和核心公共密钥 $\mathbf{K}_{pub}^{G}$),并针对每个接收方,使用该接收方的公共密钥对该会话密钥进行非对称加密。接着,加密消息子例程 145 将得到的已加密会话密钥集与由使用与发送方(即该计算机的用户)相关联的公共密钥被加密的会话密钥形成的已加密会话密钥进行组合,以形成已加密消息的 KEM 部分。然后,加密消息子例程 145 将 KEM 部分和 DEM 部分进行组合以形成已加密消息。

[0096] 解密消息子例程 147 用于对未注册的已加密消息进行解密。解密消息子例程 147 从已加密电子邮件的 KEM 部分提取使用该计算机的用户的公共密钥被加密的已加密会话密钥。然后,解密消息子例程 147 从密钥数据库 161 中取回在发送该消息的时刻有效的用户私有密钥,并使用所取回的用户私有密钥对所提取的已加密会话密钥进行解密,来复原会话密钥。接着,解密消息子例程 147 使用所复原的会话密钥对所接收的已加密消息的 DEM 部分进行解密,并向用户显示已解密的消息。

[0097] 加密消息子例程 145 和解密消息子例程 147 的进一步细节可以在 WO2005/050908 中找到,该专利的全部内容通过引用合并于此。

[0098] 发送 / 读取已注册的已加密电子邮件

[0099] 现在参考图 7A-7D 描述对已注册的已加密电子邮件的发送和读取。

[0100] 当发送计算机 1a 的用户期望发送已注册的已加密电子邮件时,在 S1,用户通过选择由加密插件 125 提供的已注册电子邮件菜单选项来开始。响应于已注册电子邮件菜单选项的选择,加密插件 125 的主控制例程 141 启动加密已注册消息子例程 149。

[0101] 加密已注册消息子例程 149 通过与邮件注册授权服务器 7 建立 http 链接并使用

万维网浏览器 121 下载由邮件注册授权服务器 7 提供的登录网页来开始。然后，用户在登录网页中输入用户标识和密码信息，并向邮件注册授权服务器 7 发送登录信息。

[0102] 一旦接收到该登录信息，在 S5 处，邮件注册服务器 67 的主控制例程 81 即使用客户数据库 91 中的数据对该登录信息进行验证，然后启动注册消息子例程 85。注册消息子例程 85 发送跟踪服务网页，该网页提供可用的跟踪服务连同它们所关联的费用的列表。该跟踪服务网页还给出客户账户中当前持有的量，并包括用于输入该电子邮件的期望接收方的电子邮件地址的数据入口框。

[0103] 在该实施例中，可用的跟踪服务仅有“在读取之前签名”服务，该服务需要接收方在能够查看电子邮件消息之前进行数字签名以确认接收。

[0104] 在 S9 处接收跟踪服务网页之后，在 S11 处，发送计算机 1a 的用户输入电子邮件的期望跟踪服务和期望接收方，然后将所输入的信息发送给邮件注册授权服务器 7。在 S13 处，一旦接收到跟踪服务和接收方电子邮件地址信息，电子邮件注册授权服务器 7 即在 S15 处生成该电子邮件的唯一跟踪代码和该电子邮件的跟踪密钥（在该实施例中是二进制数），并针对该电子邮件在消息数据库 93 中创建新项目，用于储存跟踪代码、跟踪密钥、接收方电子邮件地址的列表和所选择的跟踪服务。然后在 S17 处，电子邮件注册授权服务器 7 向发送计算机 1b 发送待被每个接收方访问的跟踪代码、跟踪密钥和统一资源定位器 (URL)。这就结束了注册消息子例程 85。

[0105] 在 S19 处，一旦从邮件注册授权服务器 7 接收到跟踪代码、跟踪密钥和 URL，发送计算机即在 S19 处生成已加密注册电子邮件。具体来说，发送计算机 1a 首先生成该电子邮件的会话密钥（在该实施例中是二进制数），并使用所生成的会话密钥对该消息进行加密以形成已加密消息的 DEM 部分。然后，发送计算机 1a 通过对跟踪密钥和会话密钥执行位异或功能来生成中间密钥。然后加密已注册消息子例程 149 计算与该消息的每个接收方相关联的公共密钥（使用该接收方的电子邮件地址和核心公共密钥$\mathbf{K}_{\mathbf{pub}}^{\mathbf{G}}$），并针对每个接收方，使用该接收方的公共密钥对该中间密钥进行非对称加密。接着，加密已注册消息子例程 149 将得到的具有由使用与该发送方（即该计算机的用户）相关联的公共密钥被加密的中间密钥形成的已加密中间密钥的已加密中间密钥集与包括 URL 和跟踪代码的头部信息进行组合，以形成已加密消息的 KEM 部分。然后，加密已注册消息子例程 149 通过将指示该电子邮件被加密的 KEM 部分、DEM 部分和未被加密的消息部分进行组合来形成已加密的已注册电子邮件。

[0106] 接着在 S23 处，发送计算机 1a 将该已加密的已注册电子邮件发送给接收方。然后加密已注册消息子例程 149 结束。

[0107] 在 S25 处，接收计算机 1b 接收到已加密的已注册消息，并且在 S27 处，接收计算机 1b 的用户打开已加密的已注册电子邮件之后，未加密消息部分被显示。然后，在 S29 处，接收计算机 1b 的用户选择由加密插件软件提供的解密电子邮件菜单选项。响应于解密电子邮件菜单选项的选择，接收计算机读取 KEM 部分中的头部信息，并识别必须从邮件注册服务器访问跟踪密钥。接着，接收计算机 1b 使用万维网浏览器 121 访问 KEM 部分的头部部分中的 URL，并在接收计算机 1b 处将跟踪代码和接收方的电子邮件地址传送给邮件注册服务器 7。

[0108] 当在 S31 处，邮件注册授权服务器 7 接收到传送包括跟踪代码和接收方电子邮件

地址的URL的信号时，邮件注册授权服务器7建立与接收计算机1b的http链接。然后，邮件注册授权服务器7启动访问消息子例程87，在S33处，该访问消息子例程87向接收计算机1b发送验证身份网页。该验证身份网页请求接收计算机的用户发回确认消息，该确认消息带有使用接收计算机1b的用户的私有密钥而生成的数字签名。

[0109] 在S35处，一旦接收到验证身份网页，在S37处，接收计算机1b的用户即通过发送所请求的签名确认来响应。

[0110] 一旦接收到签名确认，在S41处，邮件注册授权服务器7即以传统的方式使用该用户的公共密钥来验证接收计算机1b的用户身份，并在与跟踪代码相关联的消息数据库93中的项目中检查接收计算机1b的用户确实是该电子邮件的接收方之一。如先前所讨论的，在该实施例中，用户公共密钥可以使用接收计算机1b的用户的电子邮件地址和核心公共密钥K_{pub}^{G}来被计算。

[0111] 在验证接收计算机1b的用户是该电子邮件的接收方之一之后，邮件注册授权服务器7从与跟踪代码相关联的消息数据库93的项目中取回跟踪密钥，并在S43处，将所取回的跟踪密钥发送给接收计算机1b。邮件注册授权服务器7还更新指示消息数据中接收计算机1b的用户下载跟踪密钥的时刻的项目。然后，访问消息子例程结束。

[0112] 在S45处，一旦接收到跟踪密钥，接收计算机1b即启动解密已注册消息子例程151，在S47处，该解密已注册消息子例程151对已注册的已加密电子邮件进行解密以供查看。具体来说，接收计算机1b从已加密的已注册电子邮件的KEM部分提取使用接收计算机1b的用户的公共密钥被加密的已加密中间密钥。然后，接收计算机1b从密钥数据库161中取回该消息被发送时有效的用户私有密钥，并使用所取回的用户私有密钥对所提取的已加密中间密钥进行非对称解密，以复原中间密钥。

[0113] 接着，接收计算机1b对所复原的中间密钥和所接收的跟踪密钥执行位异或功能，从而复原会话密钥，如本领域技术人员将理解的。然后，接收计算机1b使用所复原的会话密钥对所接收的已加密消息的DEM部分进行解密，并向用户显示解密后的消息。然后在S49处，加密已注册消息子例程151结束。

[0114] 在该实施例中，在访问消息子例程87结束之后，提供报告子例程89被启动，在S51处，该提供报告子例程89向发送计算机1a的用户发送指示接收计算机1b的用户下载跟踪密钥的时刻的报告。发送计算机的用户在S53处接收到该报告之后，在S55处，该过程结束。

[0115] 改进和其它实施例

[0116] 所图示的实施例中，接收计算机1b的用户已经向加密授权服务器5注册，因此具有用户私有密钥。应该理解，由于接收方的公共密钥可以由任何人使用该接收方的电子邮件地址和核心公共密钥K_{pub}^{G}计算出，因此已加密的电子邮件也可以被发送给还没有向加密授权服务器注册的接收方。然而，如果还没有向加密授权服务器5注册的人接收到已加密电子邮件，则他们必须向加密授权服务器5注册，以便获得对已加密电子邮件进行解密所需的用户私有密钥。在优选实施例中，已加密电子邮件的未加密消息部分包括如何向加密授权服务器5注册的细节，以方便注册。这些细节可以包括指向加密授权服务器所提供的注册网页的URL。

[0117] 在图示的实施例中，仅有一个运行一个邮件注册加密授权服务器的邮件注册机构。可替换地，可以有多个邮件注册加密机构，每个邮件注册加密机构具有各自的服务器。

如果是这种情况，则可以对图示的实施例进行修改，从而在选择已注册电子邮件菜单选项时，可用邮件注册加密机构的列表被呈递。在优选实施例中，从因特网访问该列表，从而使其易于被更新。方便地，可以从加密授权服务器访问邮件注册机构的列表。

[0118] 已加密电子邮件可能向多个邮件注册机构注册。例如，中间密钥可以利用对会话密钥、来自第一邮件注册授权服务器的第一跟踪密钥和来自第二邮件注册授权服务器的第二跟踪密钥使用可交换的数学运算而形成。以此方式，会话密钥仅在第一跟踪密钥和第二跟踪密钥分别从第一和第二邮件注册机构被复原之后才能被复原。

[0119] 在图示的实施例中，提供的跟踪服务需要电子邮件的接收方在能够读取该电子邮件之前提供数字签名。使用数字签名提供了高级别的接收方身份证明，但是需要大量的处理。然而，并不是所有的应用都需要这样高级别的证明。在这类应用中，可以去除对数字签名的需求，从而使跟踪密钥仅在请求时被提供给已加密的已注册电子邮件的接收方。这仍然允许已加密的已注册电子邮件的始发者得知该电子邮件已经被访问。应该理解，可以对已加密的已注册电子邮件的不同接收方采用不同的跟踪规则。

[0120] 在图示的实施例中，每当接收方成功下载跟踪密钥时，由邮件注册授权服务器发布报告。可以理解，不需要任何自动报告。可替换地，可以在所有的接收方都成功下载跟踪密钥时或者一个或多个接收方在预定的时间内还没有下载跟踪密钥时自动发布报告，也可以在预定的时间之后发送指示截止该时刻哪个接收方已经成功下载跟踪密钥的报告。

[0121] 使本发明提供的已加密的已注册电子邮件的使用有用的一种应用是银行结单或诸如信用卡账单之类的账单的分发。注册这种分发的一个优点在于，关于银行结单或账单是否被读取的信息有助于提供该接收方是否处于财务困难状态的早期指示。具体来说，已经发现如果一个人处于财务困难状态，则这个人不会经常开出银行结单或账单。

[0122] 还可以对图示的实施例进行修改，从而使邮件注册授权服务器仅在预定的时间之后下载跟踪密钥。以此方式，已加密的已注册电子邮件可以被预先发送出去，但仅在预定时间之后才能被读取。为此，邮件注册服务器的消息数据库中的项目指明指示一时刻的日期和时间信息，即在该时刻之前跟踪密钥不能被下载，并且当邮件注册服务器接收到跟踪密钥的请求时，邮件注册服务器使用提供日期和时间信息的实际时钟来检查在其之前跟踪密钥不能被下载的时刻是否已经过去。

[0123] 跟踪密钥的这种限时发布在需要同时向多方公布大型文件时很有用。可以使用这种限时发布的一种应用是在通过电子邮件公布公司财务报告。

[0124] 应该理解，在图示的实施例中，得知接收方的私有密钥本身还不足以对已加密的已注册电子邮件进行解密。还必须对存储在邮件注册授权服务器 7 中的解密数据（在图示的实施例中即跟踪密钥）进行访问。因此，邮件注册授权服务器 7 能够通过监测对相关联的解密数据的访问来监测对已加密的已注册电子邮件的访问，这允许查帐索引（audit trail）被有效记录。在实施例中，查帐索引被保留以记住所有已经访问该已加密的已注册电子邮件的人。

[0125] 如果接收方的私有密钥被泄露，那么尽管知道接收方私有密钥的第三方能够使用该接收方私有密钥来得到数字签名，并因此而冒充该接收方，但是邮件注册授权服务器 7 所保留的查帐索引可以包括接收方私有密钥的泄露的指示符。例如，查帐索引可以指示从不同的网络地址对解密数据的访问。在优选实施例中，邮件注册授权服务器 7 监视查帐索

引中接收方私有密钥可能已经被泄露的指示符，并且一旦检测到指示符，即警告有可能已泄露的私有密钥的所有者。

[0126] 在图示的实施例中，已加密的已注册电子邮件具有未加密部分和已加密部分。应该理解，已加密部分可以是附到该电子邮件上的一个或多个文件，并且未加密部分也可以附到该电子邮件上。在一个实施例中，为附到电子邮件上的多个已加密文件提供单独的跟踪密钥和跟踪代码，从而能够监视对所附的已加密文件中各个文件的访问。

[0127] 应该理解，一旦电子邮件在用户计算机上被接收，该电子邮件的已加密部分就作为一个或更多已加密文件存储在该用户计算机上。已加密文件并不一定是通过电子邮件从发送方传达的，尽管通过电子邮件发送具有固有地将已加密文件链接到电子邮件接收方的优点。然而，使用 KEM-DEM 方法还固有地将已加密文件链接到一个以上预计接收方，因此当使用 KEM-DEM 方法时，已加密文件可以使用网络文件传输而非电子邮件的形式（例如使用 FTP 协议）被传达，甚至也可以作为储存在诸如 CD-ROM 的硬件储存设备上的已加密文件被传达。

[0128] 在图示的实施例中，对跟踪密钥和会话密钥执行位异或运算以确定在 KEM 部分中被非对称加密的中间密钥，并且对中间密钥和跟踪密钥执行位异或运算以复原会话密钥。可替换地，可以对会话密钥进行非对称加密，并且对该结果和跟踪密钥执行位异或运算以确定储存在 KEM 部分中的数据。

[0129] 应该理解，其它数学函数可以对跟踪密钥、中间密钥和会话密钥进行链接。例如，中间密钥可以通过使用跟踪密钥作为加密密钥对会话密钥进行对称加密而形成，且会话密钥通过使用跟踪密钥作为加密密钥对中间密钥进行对称解密来复原。

[0130] 在图示的实施例中，为已注册电子邮件的所有接收方发布单一跟踪密钥。应该理解，在可替换的实施例中，可以为不同的接收方发布不同的跟踪密钥，从而存在与不同的用户相关联的不同中间密钥。

[0131] 在图示的实施例中，邮件注册授权服务器 7 向接收计算机 1b 发送跟踪密钥，并且接收计算机 1b 从中间密钥和跟踪密钥得到会话密钥。在可替换的实施例中，接收计算机 1b 向邮件注册授权服务器 7 发送中间密钥，邮件注册授权服务器 7 使用中间密钥和跟踪密钥得到会话密钥，然后将得到的会话密钥发送给接收计算机。这允许邮件注册服务器对链接跟踪密钥、中间密钥和会话密钥的数学函数进行控制。

[0132] 尽管在图示的实施例中使用 KEM/DEM 类型的电子邮件，但是这不是必须的。在可替换的实施例中，发送计算机使用会话密钥对电子邮件消息进行对称加密，并将会话密钥发送给邮件注册授权服务器。为了对该消息进行解密，接收方必须从邮件注册授权服务器下载会话密钥，并且这种会话密钥的下载受到监视。

[0133] 在图示的实施例中，加密授权服务器生成根私有密钥和根公共密钥对。这种生成涉及某种形式的随机数生成，从而使所生成的密钥不是预定义的。一旦根私有密钥被生成，用户私有密钥就可以从该根私有密钥和某种形式的用户标识符被计算出。类似地，一旦根公共密钥被生成，用户公共密钥就可以从该根公共密钥和用户标识符被计算出。具体来说，计算用户私有密钥和公共密钥不需要生成任何随机数，并且是可重复的计算，无论该计算什么时候在哪里执行，每次都能够产生相同的结果。

[0134] 在图示的实施例中，用户的电子邮件地址被用作用户标识符。也可以使用其它形

式的标识符，但是电子邮件地址很方便，因为为了给接收方发送电子邮件消息，发送方总要知道接收方的电子邮件地址。

[0135] 如上所述，发送方能够使用接收方的电子邮件地址和根公共密钥来计算该接收方的公共密钥。因此，尽管根公共密钥通常形成包含以传统方式确认根公共密钥真实性的信息的公共密钥证书的一部分，也不需要验证接收方的公共密钥的真实性（例如通过公共密钥证书）。

[0136] 在图示的实施例中，使用 WO03/017559 中所讨论的非对称加密算法。应该理解，也可以使用具有相同的总体功能的可替换算法，例如 R. Sakai 和 M. Kasahara 在报告 2003/054 的密码技术电子印刷档案 (Cryptology ePrintarchive) 中的“ID based cryptosystems with pairing on elliptic curve(基于 ID 的在椭圆曲线上成对的密码系统)”中所讨论的算法以及 Chen 等人在报告 2005/224 的密码技术电子印刷档案中的“An Efficient ID-KEM Based On theSakai-Kasahara Key Construction(基于 Sakai-Kasahara 密钥结构的有效 ID-KEM)”中所讨论的算法（由此将这两个文献通过引用合并于此）。

[0137] 进一步，非对称加密算法不需要使用客户身份来确定客户的公共密钥，并且可以使用任何非对称加密算法，例如 RSA 算法。

[0138] 在图示的实施例中，使用各个接收方的相应公共密钥来对电子邮件进行加密，从而使各个接收方能够使用相应的私有密钥来对该电子邮件进行解密。以此方式，仅有期望的接收方能够对该电子邮件进行解密。应该理解，该电子邮件另外可以使用发送方的私有密钥被签名。以此方式，每个接收方能够验证该电子邮件发自该发送方且未被篡改。

[0139] 尽管在图示的实施例中使用 AES 加密算法来执行对称加密，但是应该理解，也可以使用其它对称加密算法，例如 DES 算法。

[0140] 在图示的实施例中，加密授权服务器 5 和邮件注册授权服务器 7 都包括允许以网页的形式向用户计算机 1 传达信息的万维网服务器，用户计算机 1 使用并入该用户计算机 1 的传统万维网浏览器程序来将网页呈现在相应的显示器上。应该理解，可以使用包括结构化数据传输的其它数据传送技术，例如使用 XML 文件。在一些实施例中，用户计算机可以包括使能与加密授权服务器和邮件注册授权服务器中的一个或两个进行通信的私有客户端软件。

[0141] 在图示的实施例中，用户计算机是传统的个人计算机。应该理解，这种个人计算机可以是例如膝上型或桌上型。进一步，用户计算机可以由诸如瘦客户端 (thin client) 或个人数字助理 (PDA) 之类的其它类型的计算机设备形成。

[0142] 尽管本发明的图示实施例包括计算机设备和在该计算机设备上执行的处理，但是本发明还扩展到计算机程序，尤其是适于将本发明付诸实践的载体上的计算机程序。该程序可以采用源代码、目标代码、代码中间源和诸如部分已编译形式的目标代码的形式，也可以采用适合使用根据本发明的过程的工具的任意其它形式。

[0143] 该载体可以是能够承载程序的任意实体或器件。例如，该载体可以包括诸如 ROM 之类的储存介质，例如 CD-ROM 或半导体 ROM，也可以包括诸如软盘或硬盘之类的磁记录介质。进一步，该载体可以是诸如可以通过电缆或光缆或通过无线电或其它手段传送的电子或光信号的可传输载体。

[0144] 当以可以通过线缆或其它设备或手段传送的信号的形式实施该程序时，该载体可

以由这类线缆或其它设备或手段构成。可替换地，该载体可以是其中嵌入程序的集成电路，该集成电路适于执行相关处理或在执行相关处理时使用。

[0145] 尽管在所描述的实施例中，本发明是用软件实现的，但是应该理解，可替换地，本发明可以用硬件设备或硬件设备与软件的组合来实现。

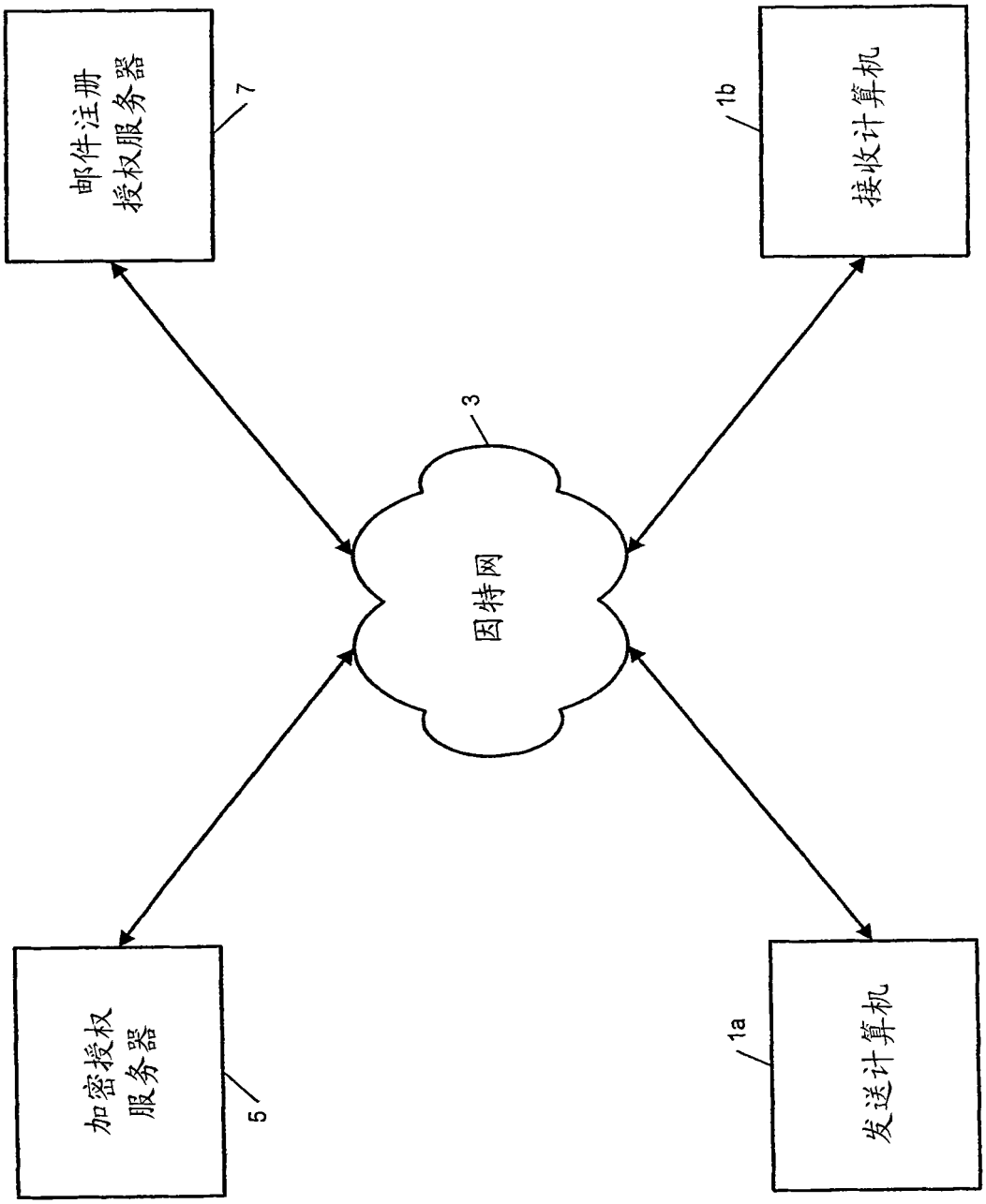


图 1

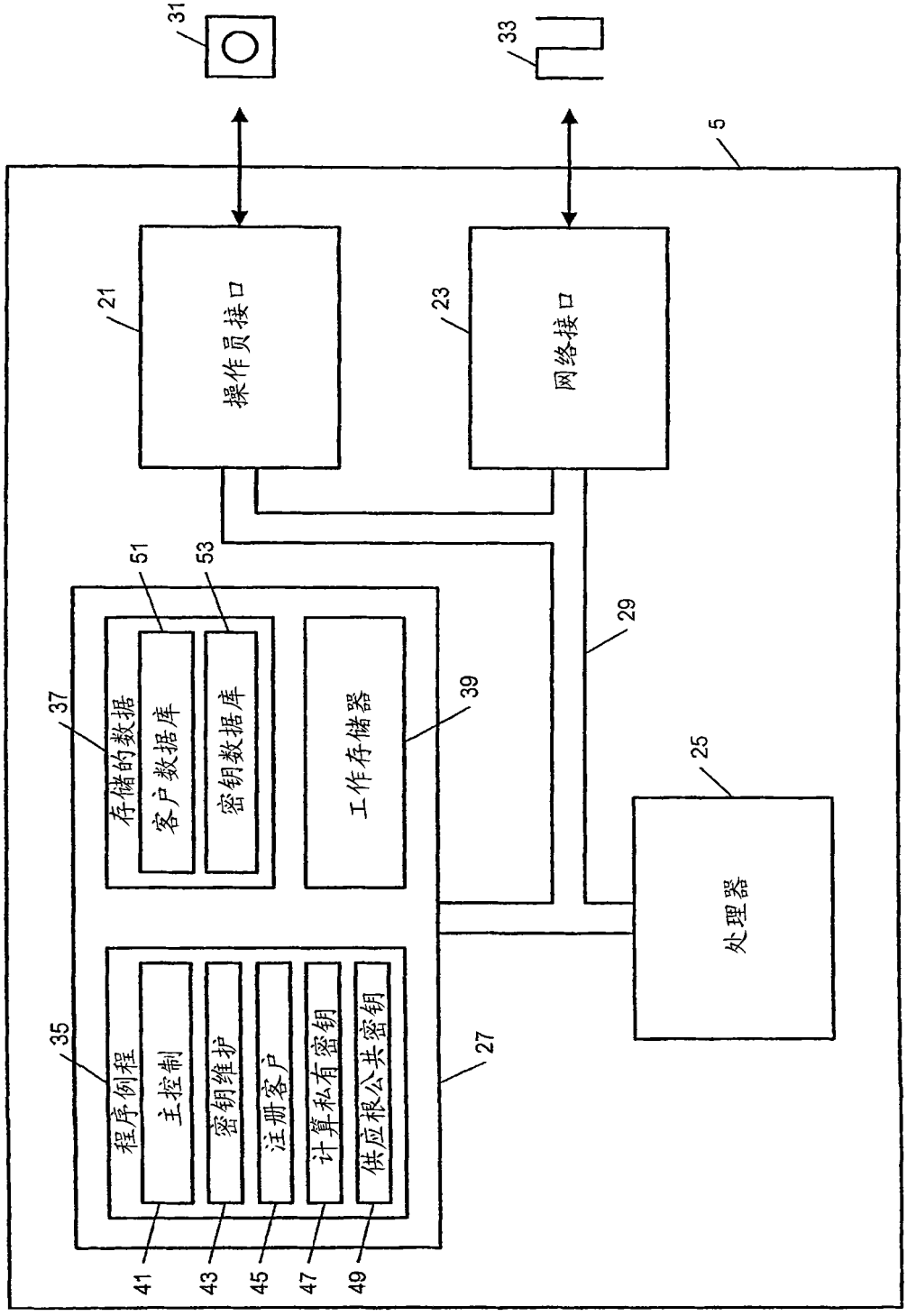

31
33
5
操作员接口
网络接口
21
23
51
53
存储的数据
客户数据库
密钥数据库
工作存储器
37
39
29
25
处理器
程序例程
主控制
密钥维护
注册客户
计算私有密钥
供应根公共密钥
35
27
41
43
45
47
49

图 2

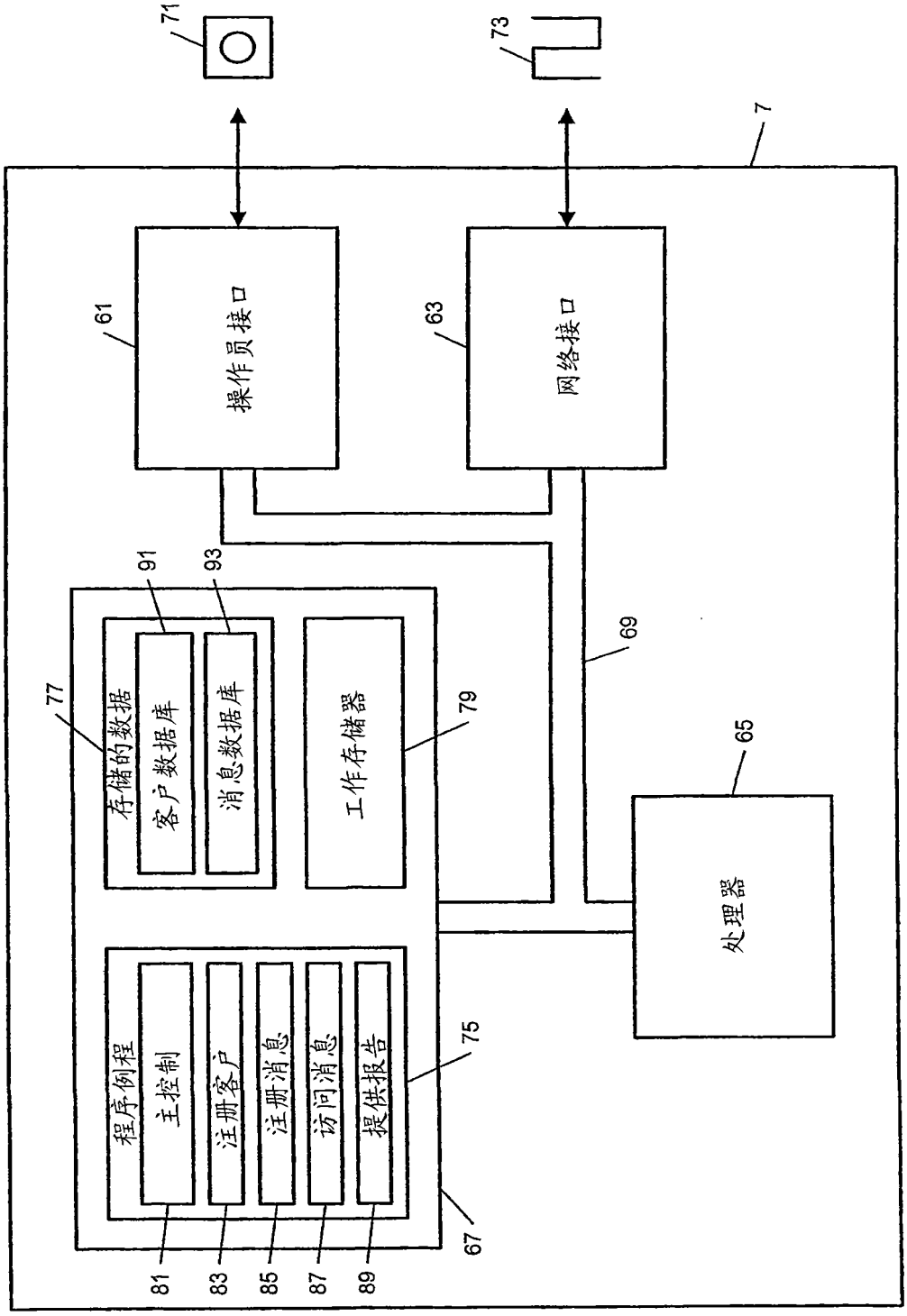

71
73
7
61
操作员接口
63
网络接口
91
93
77
存储的数据
客户数据库
消息数据库
工作存储器
79
69
65
处理器
程序例程
主控制
注册客户
注册消息
访问消息
提供报告
75
67
81
83
85
87
89

图 3

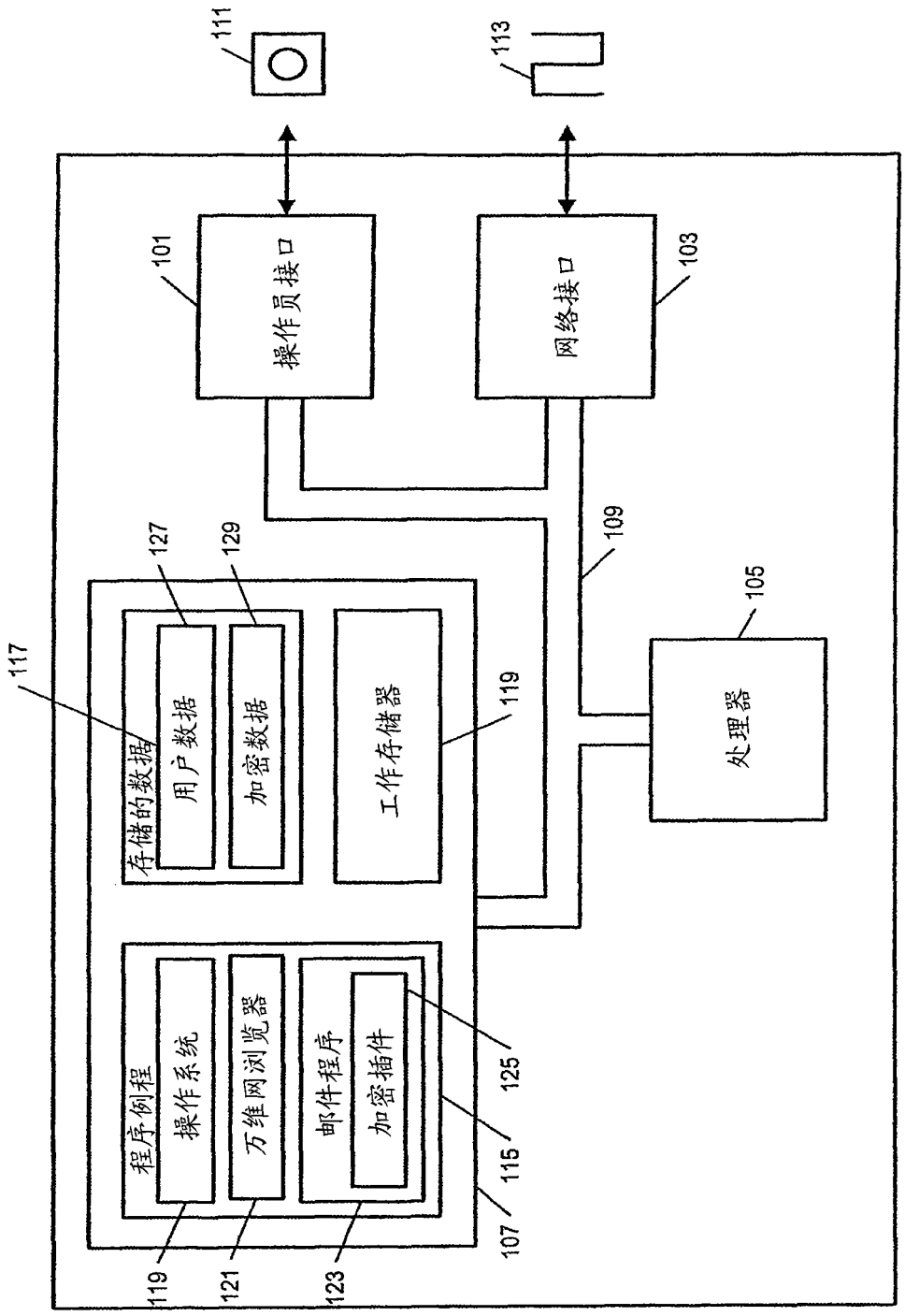

111
113
101
操作员接口
网络接口
103
109
105
处理器
127
129
117
存储的数据
用户数据
加密数据
工作存储器
119
程序例程
操作系统
万维网浏览器
邮件程序
加密插件
125
115
107
119
121
123

图 4

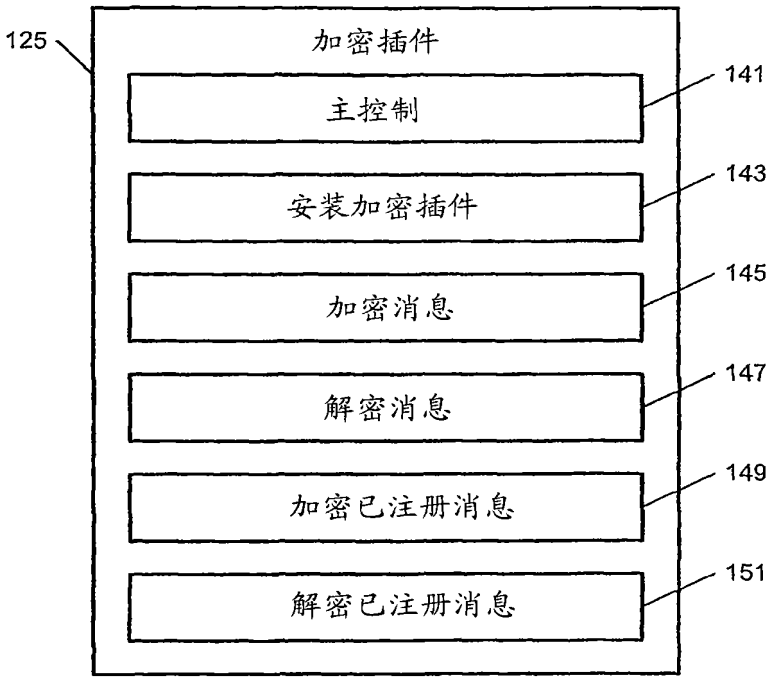

125
加密插件
141
主控制
143
安装加密插件
145
加密消息
147
解密消息
149
加密已注册消息
151
解密已注册消息

图 5

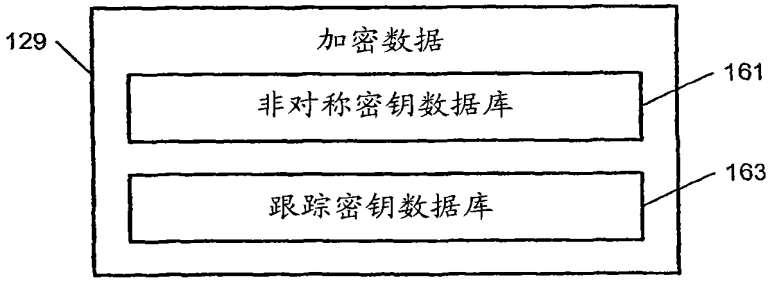

129
加密数据
161
非对称密钥数据库
163
跟踪密钥数据库

图 6

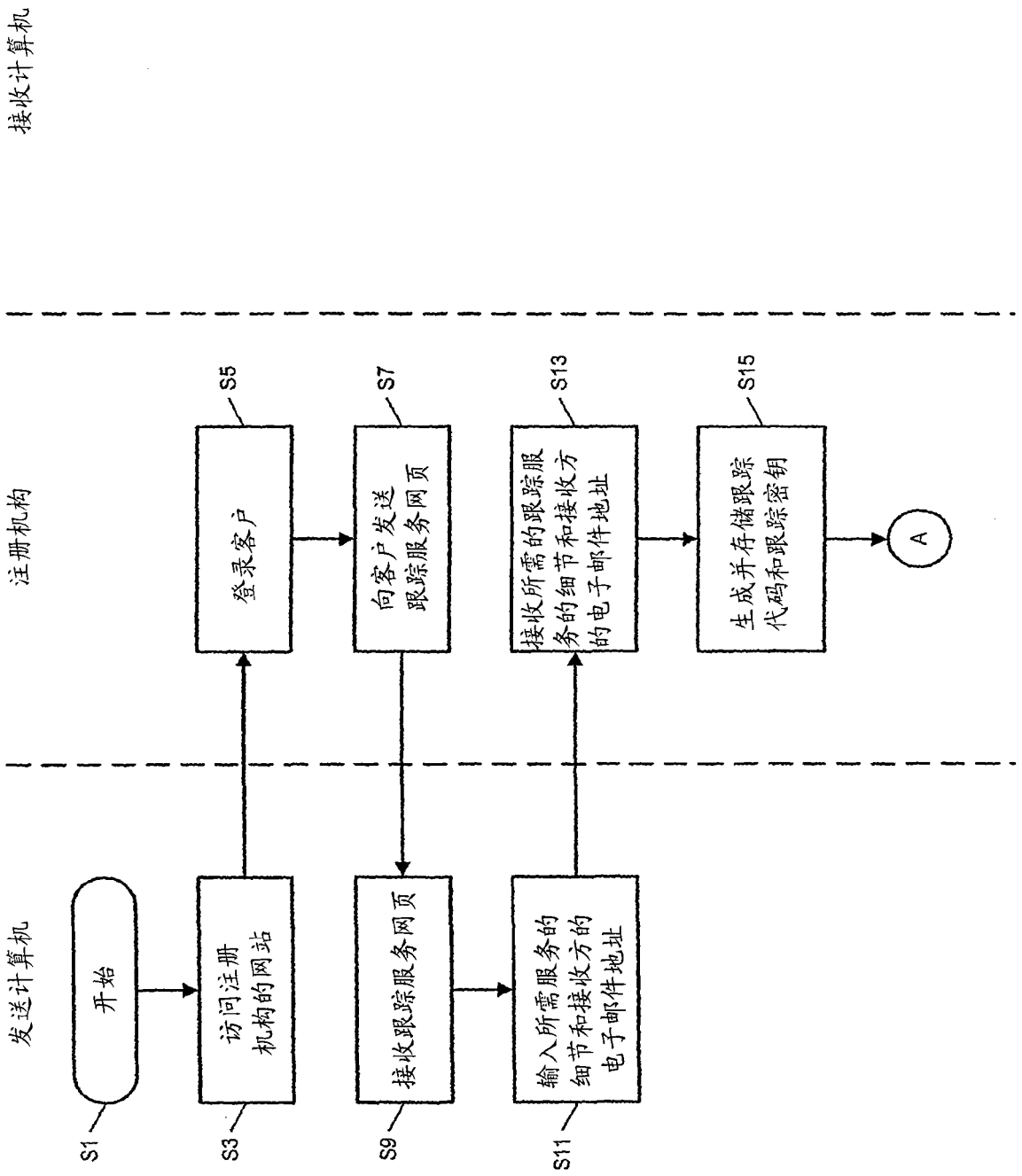

发送计算机
注册机构
接收计算机
开始
S1
访问注册机构的网站
S3
登录客户
S5
向客户发送跟踪服务网页
S7
接收跟踪服务网页
S9
输入所需服务的细节和接收方的电子邮件地址
S11
接收所需的跟踪服务的细节和接收方的电子邮件地址
S13
生成并存储跟踪代码和跟踪密钥
S15
A

图 7A

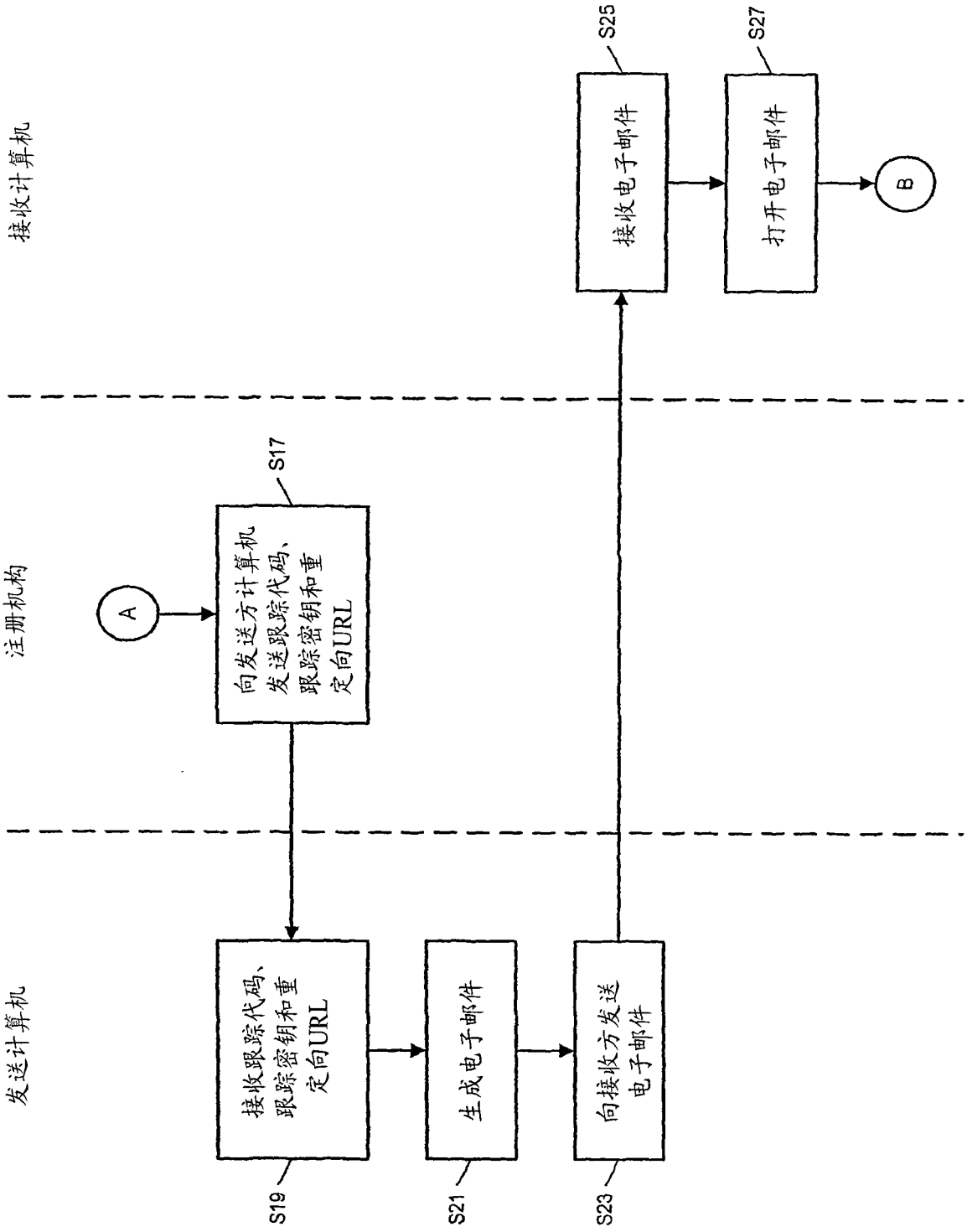

接收计算机
注册机构
发送计算机
A
B
S17
S19
S21
S23
S25
S27
向发送方计算机发送跟踪代码、跟踪密钥和重定向URL
接收跟踪代码、跟踪密钥和重定向URL
生成电子邮件
向接收方发送电子邮件
接收电子邮件
打开电子邮件

图 7B

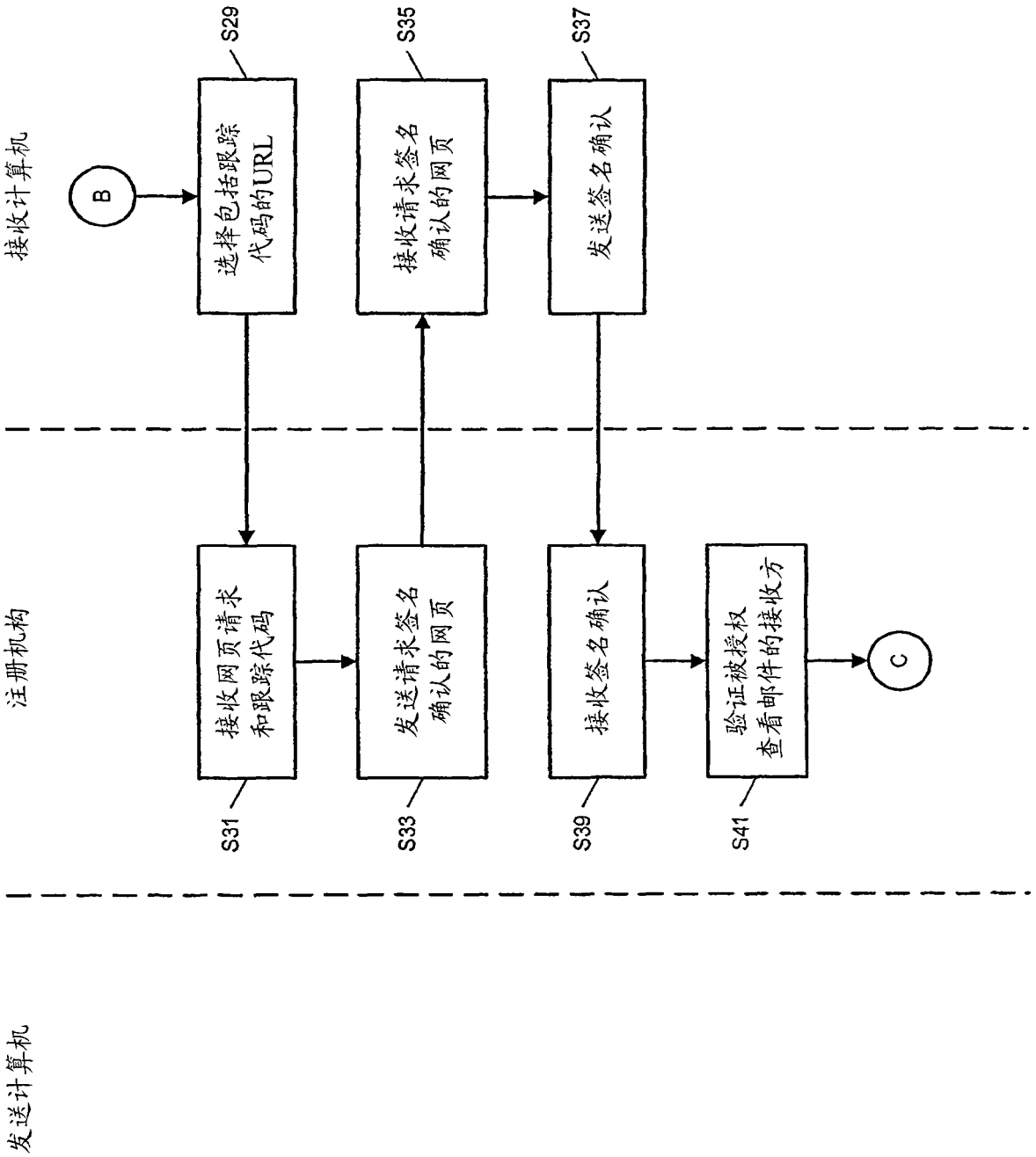

发送计算机
注册机构
接收计算机
B
选择包括跟踪代码的URL
S29
接收请求签名确认的网页
S35
发送签名确认
S37
接收网页请求和跟踪代码
S31
发送请求签名确认的网页
S33
接收签名确认
S39
验证被授权查看邮件的接收方
S41
C

图 7C

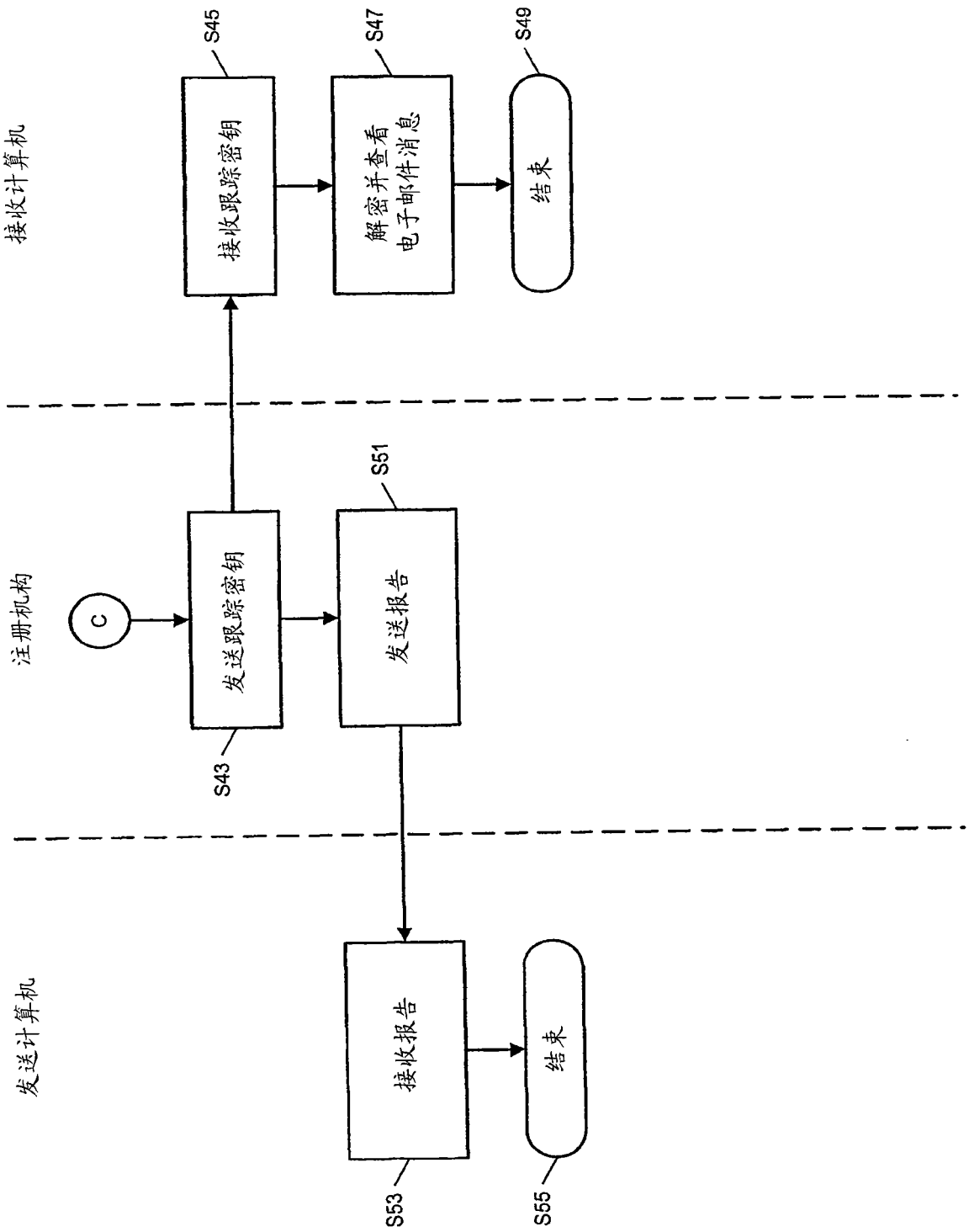

接收计算机
注册机构
发送计算机
S45
接收跟踪密钥
S47
解密并查看
电子邮件消息
S49
结束
C
发送跟踪密钥
S43
S51
发送报告
接收报告
S53
结束
S55

图 7D