



[12] 发明专利说明书

专利号 ZL 00104813.9

[45] 授权公告日 2009年1月21日

[11] 授权公告号 CN 100454805C

[22] 申请日 2000.3.27 [21] 申请号 00104813.9

[30] 优先权

[32] 1999.3.26 [33] US [31] 09/277298

[73] 专利权人 西门子信息及通讯网络公司

地址 美国佛罗里达州

[72] 发明人 G·E·卡特

[56] 参考文献

WO 9811704A2 1998.3.19

审查员 罗芳洁

[74] 专利代理机构 中国专利代理(香港)有限公司

代理人 程天正 张志醒

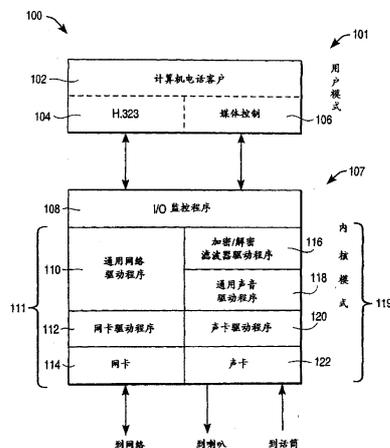
权利要求书 2 页 说明书 13 页 附图 5 页

[54] 发明名称

发送和接收电话信号的方法和使客户安全通信的配置方法

[57] 摘要

一种计算机可读出的媒体，它含有用于配置第一计算机的程序指令以使在第一计算机上的第一电话客户(10、102)可以安全地经过通信路径与第二计算机上的第二电话客户(11)通信。该计算机可读出的媒体包括用于在通信路径内插入保密算法(16、22、116)的计算机代码。保密算法(16、22、116)使第一和第二电话客户之间的安全通信变得容易，因为可以实现不止一种类型的电话客户。在特定的实施例中，保密算法是插在第一计算机的操作系统内核中的。



1. 一种用于将电话信号从第一电话系统发送到第二电话系统的方法，所述第一电话系统包括用户操作模式和操作系统内核操作模式，该方法包括：

在第一和第二电话系统之间起一次电话对话；

在所述操作系统内核操作模式，利用保密算法来加密该电话信号；

在所述用户操作模式，把该加密的电话信号格式化成为可被第二电话系统辨认的预先确定的格式，其中的加密与格式化是无关的；以及

在电话信号已被加密和格式化之后将电话信号发送到第二电话系统。

2. 如权利要求 1 所述的方法，其特征在于该格式化步骤对所述加密步骤的输出进行操作。

3. 一种用于使第一电话系统从第二电话系统接收电话信号的方法，所述第一电话系统包括用户操作模式和操作系统内核操作模式，该方法包括：

从第二电话系统接收该电话信号，所接收到的电话信号被第二电话系统格式化成为预先确定的格式；

在所述用户操作模式，解释从第二电话系统收到的电话信号的预先确定的格式；以及

在所述操作系统内核操作模式，将所解释的电话信号解密，解密是与解释该预先确定的格式相互独立地进行的。

4. 一种用于配置第一计算机以便使在第一计算机上的第一电话客户(10, 102)能经过通信路径安全地与在第二计算机上的第二电话客户(11)通信的方法，所述第一计算机包括用户操作模式和操作系统内核操作模式，该方法包括：

在该通信路径的一部分处把一个保密算法(16, 22, 116)插入到该通信路径中，其中，第一电话客户(10)在所述用户操作模式对已经在所述操作系统内核操作模式被所述保密算法加密的信号进行格式化，所说的保密算法(16, 22, 116)使在第一和第二电话客户之间的安全通信变得方便。

5. 如权利要求 4 所述的方法，其特征在于该保密算法的插入使第一电话客户与第二电话客户不相同。

6. 如权利要求 4 所述的方法，其特征在于该保密算法是插在第一计

计算机的操作系统的内核之内的。

7. 如权利要求 6 所述的方法，其特征在于第一计算机的操作系统内核是这样形式的操作系统，它具有一个 I/O 监控程序和一个声卡驱动程序，而该保密算法是插在 I/O 监控程序和声卡驱动程序之间的，该保密算法被设计成一个滤波器驱动程序。

8. 如权利要求 6 或 7 所述的方法，其特征在于该保密算法是从包括 IDEA 加密算法、DES 加密算法、GOST 算法、RC5 算法、和 SEAL 算法的一个组中选出来的。

9. 如权利要求 4 所述的方法，其特征在于该保密算法是在第一计算机的操作系统的用户模式之外实现的。

10. 如权利要求 9 所述的方法，其特征在于该保密算法独立于第一或第二电话客户或任何编解码器或与第一或第二电话客户相结合地应用的通信堆栈。

发送和接收电话信号的方法和 使客户安全通信的配置方法

本发明总体上涉及在计算机电话系统中提供加密。更具体地说，本发明涉及对在计算机电话系统之间例如通过计算机网络发送的音频数据进行加密的方法和设备。

随着传输速率和带宽的增加，计算机电话正在不断地变得更加流行。因此，若干供应商现在正在提供家庭和商业用的电话应用软件包。这些电话应用软件一般都装入到两台或更多台计算机中，使得两台计算机的两个用户可以用电话通话方式通信。

电话应用软件提供给某一特定用户的价值一般是和同样也使用电话应用软件的别的用户数量成正比。例如，如果该特定用户的朋友或同事也利用电话应用软件，那么用户会很容易发现电话应用软件是十分有价值的并且经常用它来和他的朋友或同事交谈。相反，如果该特定用户的朋友或同事中没有人利用电话软件，那么，该用户会很容易地发现他们的电话软件实在没有什么用处。

但是，计算机电话用户的增加也会伴随着缺点。例如，随着计算机电话用户数量的增加，很可能会使某个特定用户的通信机密受到黑客的侵犯。也就是说，随着用户的数量和相应的电话通信的增加，对于黑客来说，破坏或偷窃计算机电话通信将变得更有吸引力。

出于对付潜在黑客的考虑，少数电话应用软件的供应商已试图在他们的应用软件中包含保密特性。保密特性通常和格式化软件模块紧密结合，这些模块随不同类型的电话应用软件而变。这就是说，保密算法取决于格式化算法，而格式化算法是由特定的供应商为特定的电话应用软件专门设计的。因此，常规的保密特性一般包括只对在使用相同的电话应用软件的两个用户之间所发送的数据即音频才起作用的解密和加密。

按照传统，计算机电话系统中声音通信的加密是发生在“用户模式”中的：或者在应用软件本身，或者在它的编码/解码器（编解码器）部件中，或者在所用的通信堆栈中。因此，由不同的公司所生产的计算机电话客户之间的加密音频通信要用常规的保密特性是不可能的。换句话说，不同的电话供应商并不提供兼容的保密机理。

根据以上所说，需要有一种可供替代的更加灵活的计算机电话设备和技术，它们能为不同的计算机电话客户之间的通信提供加密和解密方法。

因此，本发明为不同的计算机电话客户之间的通信提供进行加密及/或解密的方法和装置。概括地说，加密和解密机理是插在客户间的通信路径之内的，以便两个客户之间可以实施任何类型的电话设备或系统。例如，两个客户都可以实施西门子的 HiNet™RC 3000 电话软件，或者两个客户都可以实施微软的 NetMeeting 软件。换一种方式，一个客户可以实施从一个电话软件供应商得来的电话软件，而另一个客户可以实施从不同的电话软件供应商得来的电话软件。两个客户所用的电话软件无论有什么差异，他们的通信都可以按照本发明来加密和解密。

在一种实施例中，本发明提供一种计算机可读的媒体，它包含程序指令，用来配置第一计算机，使得在第一计算机上的第一个电话客户可以通过通信路径安全地和第二计算机上的第二个电话客户通信。这个计算机可读的媒体包含了用于在通信路径内插入一个保密算法的计算机代码。这个保密算法使得第一和第二电话客户之间的保密通信变得容易，从而让不止一种类型的电话客户得以实现。在一个特定的实施例中，这个保密算法是插在第一台计算机的操作系统内核中的。

在另外一个实施例中，本发明提供一种配置第一计算机的方法，使得在第一计算机上的第一个电话客户可以通过通信路径安全地和第二计算机上的第二个电话客户通信。在通信路径中插入一个保密算法，而这个保密算法使得第一和第二电话客户之间的保密通信变得容易，从而让不止一种电话客户得以实现。

在另一方面，本发明提供一种由处理器所使用的操作系统以便指挥计算机的操作，在该计算机上第一电话客户可以执行经过通信路径而与在第二计算机上的第二电话客户的通信。这个操作系统包括至少一个处理器可读出的媒体，以及一种嵌入于该至少一种处理器可读出的媒体中的程序机制，以便使处理器易于在第一和第二电话客户之间安全通信，使得电话客户的任何类型的组合都可以实现。

在另一种实施例中，本发明提供一种计算机可读出的媒体，它包含用于第一电话系统的程序指令以便和第二电话系统安全地通信。该第一电话客户是可配置的，以便包括一个声卡和相关联的驱动程序、用于和

声卡中相关联的驱动程序相接口的通用声音驱动程序、一个网卡和相关联的驱动程序、用于和网卡中相关联的驱动程序相接口的通用网络驱动程序、一个电话客户程序、用于在电话客户程序和通用网络及声音驱动程序之间相接口的 I/O 监控程序。在这个实施例中，计算机可读出的媒体包括用于在 I/O 监控程序和通用声音驱动程序之间插入一个滤波器驱动程序的计算机代码。滤波器驱动程序能够在音频信号被电话客户接收并发送到网卡之前对在声卡内收到的音频信号进行加密，同时滤波器驱动程序还能够将由网卡接收到的并经过电话客户而传递到滤波器驱动程序的音频信号进行解密。解密是在音频信号发送到声卡之前进行的。

在另一个实施例中，本发明提供一种计算机可读出的媒体，它含有编程指令，用于具有相关联的格式化模块的第一电话客户以便安全地和第二电话客户通信。这个计算机可读出的媒体包括从音频输入设备接收音频信号的计算机代码、将收到的音频信号独立地进行加密而与和第一电话客户相关联的格式化模块无关的计算机代码、以及输出加密的音频信号以便将其传输到第二电话客户去的计算机代码。

在再另外一个方面，本发明提供一种计算机可读出的媒体，它含有编程指令，用于具有相关联的解释模块的第一电话客户以便能安全地和第二电话客户通信。这个计算机可读出的媒体具有从网络输入设备接收音频信号的计算机代码、将收到的音频信号独立地进行解密而与和第一电话客户相关联的解释模块无关的计算机代码、以及输出解密的音频信号以便将其传输到音频输出设备的计算机代码。

在另一方面，本发明提供一种涉及从第一电话系统发送到第二电话系统的电话信号的方法。电话会话是在第一和第二电话系统之间起动的。电话信号被格式化成一种预先规定的、可以被第二电话系统辨认的格式。格式化是在对从第一电话系统的电话输入设备收到的电话信号作出响应时进行的。电话信号用保密算法进行加密，加密与格式化无关。在电话信号被加密和格式化之后被发送到第二电话系统。

在一种可替代的实施例中，本发明提供一种用于在第一电话系统和第二电话系统之间交换电话信号的计算机系统。这个计算机系统包括一个格式化模块，它被设计成能使电话信号成为第一种预先规定的、能被第二电话系统辨识的格式。格式化是在对第一电话系统的电话输入设备接收到电话信号作出响应时实施的。计算机系统还包括一个解释模块，

它被设计成能识别从第二电话系统收到的电话信号的第二种预先规定的格式，计算机系统还包括一个保密模块，它被设计成在电话信号发送到第二电话系统之前将它加密并在第一电话系统接收电话信号时进行解密。这种加密与能被第二电话系统所辨识的第一预定格式是无关的，并且这种解密与第一电话系统所收到的电话信号的第二预定格式也是无关的。

本发明具有许多优点。例如，独立的保密机制允许对特定的电话应用软件所需要的或所利用的格式化方法作各种改变而不需要改变现有的保密机制。同样，对保密机制的改变也不需要改变某个特定电话应用软件所实施的格式化方法。此外，保密机制没有必要因为每一种独特的电话格式化技术而单独开发。其结果是，开发保密电话应用软件的成本可显著减少。

本发明的这些和另外的特性和优点将在下面的对本发明的说明和以举例方式说明本发明的原理的附图中更详细地提供。

图 1A 表示按照本发明的一个实施例的从第一计算机电话系统发送而由第二计算机电话系统接收的电话信号的总体流动路径。

图 1B 是按照本发明的一个特定实施例的在一个具有用户模式和内核模式的操作系统环境中实现的计算机电话系统的图解表示。

图 2 是按照本发明的一个特定实施例的只有当加密及/或解密被选定时装入的加密滤波器驱动程序的决策过程的图解表示。

图 3 是按照本发明的一个可替代实施例的由具有可编程的加密及/或解密标志的滤波器驱动程序所实现的决策过程的图解表示。

图 4 表明适合于实施本发明的某些特定实施例的计算机系统。

图 1A 表示按照本发明的一个实施例的从第一计算机电话系统 10 发送而由第二计算机电话系统 11 接收的电话信号的总体流动路径。虽然图 1A 显示的第一电话系统 10 只有发送部件而第二电话系统 11 只有接收部件，但这个简化的示图只是用来便于讨论，因此不致于不必要地使本发明变得模糊不清。当然，每个电话系统可以同时含有发送和接收部件。本发明的更为详细的计算机电话系统的实施例将在下面参考图 1B 而予以说明。应该注意“计算机电话”客户或系统可以指由电话起动的计算机或 H323 兼容的（或对话初始化协议兼容的）电话。

现在转向由电话系统 10 表示的发送一侧，电话信号 12 由电话输入

设备 14 接收, 例如, 用户通过电话机说话, 输入设备 14 可以采取任何合适机构的形式以接收电话信号 (例如语音或音频信号) 并把它们转换成计算机可读出的信号。例如, 输入设备 14 可以包括话筒、声卡、以及各种声卡接口软件模块或驱动程序以便把模拟的电话信号转换成 1 和 0 的二进制表示。

收到的电话信号 12 可以由输入设备 14 处理然后可以由方块 16 加密。在加密以后可以对电话信号作进一步的处理。例如, 电话信号可以为操作系统或电话客户的特定接口的需要而进行合适的格式化。

任何适合于使电话通信得到保密的加密算法都可以实施。作为特定的例子, IDEA 加密算法、DES 加密算法、GOST 算法、RC5 算法、SEAL 算法, 或者密钥文件加密法都可以用于本发明。当然, 在别的应用中 (除电话外) 所用的加密类型, 例如文件转移, 也可以用在本发明中。

如图 1A 所示, 电话信号在经过加密后, 在块 18 中被格式化成能被接收计算机电话系统 11 所辨识和实施的一种特定格式。例如, 电话信号可用一种特定的、能被计算机电话系统 11 认识的压缩算法进行压缩。作为另一个例子, 格式化可以满足各种标准的协议要求而实现, 例如 H. 323、RTP (实时协议)、TCP (传输控制协议)、和 IP (因特网协议)。

这个格式化方块 18 可以包括由特定的电话系统设计所要求的任何形式的格式化。例如, 特定的电话应用软件需要不同的压缩例程或编译器, 例如 G. 711、G. 723 和 G. 729 编译器。作为另一个例子, 不同的电话应用软件需要不同的通信堆栈实施方式。除了上面提到的 H. 323 以外, 可替代的格式, 例如 SIP (对话起动机协议) 也可以使用。

现在转向接收方一侧, 加密的并经格式化的信号这时传递到接收计算机电话系统 11, 在这里信号由电话系统 11 的方块 20 进行解释。作为例子, 信号可以在方块 20 中被解压缩。

然后电话信号可以在方块 22 中解密。然后解密和经解释的信号传送到电话输出设备 24。电话输出设备 24 的功能是把解密的电话信号转变成音频信号 26。例如, 输出设备 24 可以采取音频喇叭、声卡、以及声卡软件或驱动程序的形式。

如图 1A 所示, 对于本发明而言, 加密和解密是和格式化分开进行的, 而格式化对特定的电话应用软件或所用的系统是各不相同的。这就是说, 加密和/或解密功能和任何格式化功能是相互独立的, 而格式化

功能在不同的计算机电话应用软件和系统之间是各不相同的。例如，加密并不取决于所实现的压缩算法是哪一种类型。因此，本发明提供了若干优点。举例来说，通用的加密或解密模块可以用在任何类型的电话应用上。因此，如果电话应用软件的格式化算法发生变动，加密和解密模块并不同样需要变化。此外，对于每种新的电话应用软件和对应的新的格式化技术并没有必要去建立一种独立的保密模块。总之，把特殊的格式化机理和保密机理区分开来可以明显地增加多用性而降低提供计算机电话系统的成本。

在某些实施例中，保密算法也独立于电话应用软件代码本身。也就是说，保密模块和电话应用软件是分开的软件模块。这样，保密模块和电话应用软件可以独立地开发和改变。例如，保密模块可以用不同于电话应用软件的编程语言来编写。

图 1B 是按照本发明的一个实施例的在具有用户模式和内核模式的操作系统环境内实现的计算机电话系统 100 的图解表示。图 1B 以通用的术语表明了一种音频和网络路径结构，这两者都被计算机电话客户 102 用来和另一个计算机电话系统（未示出）通信。如图所示，电话系统 100 包括耦合到网络设备 111（它一般同时包括硬件和软件部件）的用来和第二计算机电话系统（未示出）交换信号的计算机电话客户 102，以及用来接收从例如用户来的声音和产生声音的音频设备 119（它一般同时包括硬件和软件部件）。

现在转向发送方一侧，音频设备 119 接收到一个或多个声音。如上所述，音频设备可以包括任何能把声音转化成计算机可用信号的合适的机构。在所说明的实施例中，声音被接收到（例如由用户说话）连接到声卡 122 上的话筒中。声卡 122 通常和声卡驱动程序 120 共同工作以便把模拟音频信号转换成数字音频信号并实施操作系统或电话客户或应用软件所要求的任何格式化。转换和格式化功能可以由任何硬件和/或软件模块的组合来实现。作为例子，声卡 122 可以包括专用集成电路（ASIC）以便快速执行熟知的处理功能和/或可以包括可编程逻辑器件（PLD）以实现快速变化的处理功能和/或可以包括一个或多个数字信号处理器（DSP）以便执行专门的计算。

当前可以得到的声卡及其相关的驱动程序有许多类型，每一类型都以独特方式处理音频信号。例如，某些声卡和驱动程序包括对于所用的

电话应用是特有的处理功能。某些声卡和驱动程序可以实现流行的压缩算法 G. 711 编译码器。另外，别的一些声卡和驱动程序可能不包括 G. 711 编译码器，而是把该项功能留给电话客户去完成，或者虽然包括了 G. 711 但是允许这个装在板上的编译码器可被旁路。

然后音频信号通常被传送到通用声卡驱动程序 118。虽然声卡驱动程序 120 是仅仅专门和相关联的声卡 122 相接口的，但是通用声卡驱动程序 118 却能够和各种类型的声卡驱动程序和它们相关联的声卡相接口的。在没有本发明的实施方案时，音频信号将是由输入/输出 (I/O) 监控程序 108 接收的。

I/O 监控程序 108 的功能之一就是确定如何在运行于操作系统顶部的各种软件应用客户和用于和各种连接到计算机系统的外部设备进行接口的各种软件模块之间为各种数据选择路由。在一个实施例中，如果音频信号是计算机电话信号的形式，那么 I/O 监控程序 108 就把音频信号送到计算机电话客户 102。然后电话客户 102 就向 I/O 监控程序发出请求以便将音频信号送到第二计算机电话客户 (未示出)。

第二电话客户可以位于另一个计算机上，而该计算机可能连接在一个局域网上，而局域网本身又可能连接在广域网上。典型的计算机网络包括一组通信通道，通道把一组可以相互通信的计算机设备或节点互连接在一起。这些节点可以是各种各样的分布在不同地点的计算机、终端、工作站、或通信单元。它们通过通信通道相互通信，而通信通道可以从公共的承载者 (例如电话公司) 租借或由网络的拥有人提供。这些通道可以使用各种类型的传输介质，电话光纤、同轴电缆、双绞铜线、卫星链路或数字微波无线电设备。这些节点可以分布在广阔的地区内 (距离为几百或几千英里) 或只分布在局部地区内 (距离为上百英尺到几英里)，在这种情况下它们分别称为广域网 (WAN) 或局域网 (LAN)。把局域网和广域网组合起来也是可能的，例如把各分部办公室的分隔很远的局域网通过广域网互连接。

在所说明的实施例中，音频信号是被引导经过网络途径或网络设备 111 而朝向网卡 114 的。网络设备可以包括任何合适的软件及/或硬件模块以便在特定类型的网上，例如 IP 网或 ATM (异步转移模式) 网上通信。如图所示，网络设备 111 包括网卡 114、用于特定网络的网卡驱动程序 112，以及通用网络驱动程序 110。

最初，音频信号由 I/O 监控程序 108 传送而通过通用网络驱动程序 110。通用网络驱动程序 110 能够把音频信号传送到各种类型的网卡驱动程序和它们的相关网卡上。如图所示，通用驱动程序在 I/O 监控程序 108 和网卡驱动程序 112 之间提供一个接口。

网卡驱动程序 112 一般是负责和网卡进行相互接口的。例如，网卡驱动程序 112 向网卡 114 表明，现在有音频信号或数据要发送到网络上。然后网卡 114 发出通知：它已准备就绪接收一块音频数据，然后网卡驱动程序就发送一块音频数据，并伴随发送必要的信息，例如数据长度。然后音频数据经过网络，例如局域网和/或广域网传递到第二计算机电话客户。

现在转向收信方一侧，音频信号从发送的计算机电话客户经过网络而由网卡 114 所接收。然后收到的信号由网卡 114 和网卡驱动程序 112 一起处理。网卡驱动程序 112 把收到的电信号转换成计算机可读的信号，例如二进制数据。网卡 114 和/或驱动程序 112 还可以提供存储数据和控制数据流的机制（例如提供冲突控制）。此外，网卡 114 和/或驱动程序 112 认识特定类型网络的特定数据格式。与此相对照，通用网络驱动程序 110 识别从各种类型的网卡所收到的数据并与它们相接口。

然后收到的信号被传送到 I/O 监控程序 108，在那里它又被传送到计算机电话客户 102。电话客户 102 可以包括和一个或多个网络路径及媒体路径（例如声卡和声音驱动程序）相接口的机制。如图所示，电话客户 102 包括一个 H. 323 模块以便实现在网络上所用的 A. 323 标准的格式化要求。电话客户 102 还包括一个媒体控制模块 106 以便经过 I/O 监控程序 108 和各种媒体设备相接口。

H. 323 模块 104 包括实时协议（RTP）的实施，它要求音频信号格式化成为数据报文并经过一种无连接的设置发送出去。H. 323 模块的 RTP 规定了对音频数据做什么事。作为例子，RTP 把音频数据进行分组并在把它发送到另一个电话系统之前对分组后的音频数据加上一个 RTP 标题。

在音频信号经过适当的格式化以符合任何上网标准之后，I/O 监控程序 108 就从电话客户 102 接收一个请求以便把收到的信号经过通用声卡驱动程序 118、声卡驱动程序 120 而送到声卡 122。声卡 122 把收到的信号输出到一个或多个喇叭上。

媒体控制 106 可以对收到的音频数据进行选择并实现一种适宜的解压缩算法。例如，媒体控制 106 可以选择一种特定的编译码器，将它用来压缩进入的数据。在发送方一侧，媒体控制模块 106 根据所使用的特定的电话客户软件来对音频数据选择并实施一种特定的压缩算法（例如编解码器）。换句话说，不同的电话客户软件供应商利用不同的编解码器。

本发明提供与计算机电话客户 102 所进行的处理无关的对各种声音信号加密和解密的方法。这就是说，加密和解密是以同样方式进行的而不考虑由电话客户 102 所实施的特定的格式化。例如，不论电话客户 102 实施的是哪一种特定的编解码器，加密和解密功能是相同的。

在所说明的本发明的实施例中，在 I/O 监控程序 108 和通用声卡驱动程序 118 之间插进一个加密和解密滤波器驱动程序 116。这样，音频信号可以在电话客户 102 上为各种格式化功能而来回传送，同时还可以独立地在加密/解密滤波器驱动程序 116 上来回传送。换句话说，音频信号是独立于电话客户格式化而加密和解密的。

任何合适的操作系统都可以在本发明上实现。更可取的是本发明在微软的视窗 NT 环境中实现，视窗 NT 环境目前提供了在内核模式下插进专门设计的驱动程序的机制。别的操作系统可以加以修改以便包括一个类似的插入特性来在合适的地点提供本发明的滤波器驱动程序 116。

如图所示，电话系统 100 包括了在用户模式 101 或内核模式 107 中实现的软件和/或硬件。例如，特定供应商的应用软件是在用户模式 101 中执行的。如图 1B 所示，计算机电话客户 102 和相关联的媒体控制模块 106 和 H.323 模块 104 在用户模式 104 中运行。

除了用户模式软件和/或硬件外，内核模式 107 通常执行用于各种重要的网络连接和媒体控制的操作系统服务工作。一般说来，内核负责存储管理、进程、任务和硬件管理。例如，如图所示，在内核模式内 I/O 监控程序 108 是提供来作为计算机电话客户 102 和网卡 114 同时也作为声卡 122 之间的接口的。这样，各种软件和/或硬件模块是在网卡和计算机电话客户，同时也是在声卡和计算机电话客户之间实现和分层的。

加密和解密模块可以处于通信途径中的任何合适的地点，使得加密和解密和由特定的计算机电话客户所实现的任何独特的格式化功能相互独立。在图 1B 所示的实施例中，加密/解密滤波器驱动程序 116 位于内

核模式部分之内。将驱动程序安插在视窗 NT 操作系统的内核之中的一种技术在 1997 年 2 月份的 Dr.Dobb's Journal 的《探讨视窗 NT 的文件系统》(Examining the Windows NT File System)一文中说明,将其总体在此引入以供各种参考的目的。

加密/解密滤波器驱动程序 116 可以用任何适当的方式实现。例如,为了插进滤波器驱动程序可以由计算机电话客户本身或者在一个分开的实用程序中提供用户接口。用户接口会提示用户在随后的电话通信中是否需要加密和/或解密。或者,加密和/或解密的选择可以取决于例如由系统管理员设定的一个或多个系统参数。

按照特定的实施例,加密/解密滤波器驱动程序的插入可以取决于用户是否选择加密和解密。这就是说,滤波器驱动程序只是在用户选择了加密和解密时才装入。或者,滤波器驱动程序也可以在不论用户如何选择而都装入,而用户的选择是结合在滤波器驱动程序软件本身之内的。例如,可以由用户的选择使加密和/或解密标志置位和清除以表明是否要执行加密和/或解密。

图 2 是按照本发明的一个实施例的加密/解密滤波器驱动程序的决策流程的图解表示,该驱动器是仅仅在选择了加密和/或解密时才装入的。最初,输入数据在块 202 中和输出数据被区分开。输入数据可以是例如由第一用户输入到话筒去的形式。输出数据可以是经过网络路径(例如可以是图 1B 所示的网卡 114、网卡驱动程序 112 以及通用网络驱动程序 110 所表示的)而由另一个电话客户收到的音频数据的形式。

如果输入数据出现,它就在块 204 中被加密。例如,话筒的数据被加密。在这个实施例中,当有滤波器驱动程序装入时,就假定已经选择了加密。加密过的数据接着在块 206 中经过滤波器而被传送到 I/O 监控程序。

对于输出数据,首先要在块 208 中确定输出数据是否已加密。如果是已加密的,则在块 210 中要把输出数据解密,然后解密后的数据在块 214 中被传送经过滤波器和经过声音路径(例如,通用声音驱动程序 118、声卡驱动程序 120 和声卡 122)。但是,如果输出数据是不加密的,则就不必对它解密而只是在块 212 中让它通过滤波器。

图 2 只是表示了对电话数据进行加密和解密的一种方法。如上所述,加密并没有必要在装入滤波器驱动程序时就进行。换句话说,在决策过

程中可以引入更多的灵活性。例如，用户对加密和/或解密的选择可能导致加密/解密滤波器驱动程序本身的修改。

图 3 是按照本发明的一个替代实施例中由具有可编程的加密和/或解密标志的一个加密/解密滤波器驱动程序 116 所实施的决策过程 300 的图解表示。最初，在块 302 中驱动程序被装入。然后在块 304 中用户被提示选择保密设置。这就是说，用户可以被提示去选择是否要进行加密。然后在块 306 中使一个或多个保密标志置位。例如，需要加密时加密标志的值可以设置成零，而不需加密时该值可设置为 1。与此相似，需要解密时解密标志的值可设置成零，而不需解密时该值设置为 1。

虽然方块 302 到 306 按说明是在滤波器驱动程序本身之内实施的，但它们当然也可以在别的软件模块之内实现。例如，电话应用软件可以包含一个图形用户接口 (GUI) 以便提示用户去选择或取消加密和/或解密。另外，GUI 也可由实用程序提供以便插入滤波器驱动程序。当然，也可以不要 GUI。这就是说，加密和/或解密可以根据特定的系统参数而自动选择。

然后在块 308 中要确定是否有任何进入的或出去的电话数据。当有电话数据出现时，接着在块 310 中就要确定数据是进入的还是外出的。如果数据是处于输出数据的形式，那么如果解密不是可选择的（例如解密只取决于输出数据是否已经过加密），过程 300 将和图 2 所示的输出分支相同的方式进行。但是，解密是可以选择的，例如，当希望用别的可以利用的解密方法来取代滤波器解密方法的时候。例如，有的用户希望使用在电话客户软件中可以利用的解密方法。在这种情况下，最初就要在块 318 中确定输出数据是否已加密。

如果输出数据是已加密的，则在块 320 中要确定解密标志是否表明要解密。如果标志表明要解密，则在块 322 中输出数据被解密。然后在块 324 中解密后的输出数据被传送通过滤波器。当然，如果在块 318 中确定了该数据源未经加密，那么在块 324 中输出数据就不再进行解密而被传送经过滤波器，这时过程 300 结束。另外，如果在块 318 中确定了数据源是已加密的但没有指明要解密，则在块 320 中输出数据也不经解密而被传送通过滤波器，这时过程 300 结束。

对于输入数据，最初在块 312 中确定加密标志是否指明需要加密。如果指明要加密，则在块 316 中对输入数据加密，然后在块 314 中使被

加密的输入数据传送通过滤波器。但是，如果标志并不表明要加密，则在块 314 中输入数据仅仅传送通过滤波器而不进行加密。这时过程 300 结束。

图 4 表示适合于实现本发明的各种实施例的计算机系统 900。图 4 表示计算机系统的一种可能的物理形式。当然，计算机系统可以有多种物理形式，其范围可以从一块集成电路、一块印刷电路板和一台小型手持式设备、一直到巨型超级计算机。计算机系统 900 包括一个监控器 902、显示器 904、外壳 906、盘驱动器 908、键盘 910 以及鼠标 912。盘 914 是一种计算机可读出的媒体，用于和计算机系统 900 来回传送数据。

图 4 是计算机系统 900 的方块图的一个例子。接在系统总线 920 上的是各式各样的子系统。处理器 922（也称为中央处理单元 CPU）连接到包括存储器 924 在内的存储装置。存储器 924 包括随机存取存储器（RAM）和只读存储器（ROM）。就像在本技术中众所周知的，ROM 用来单向地向 CPU 转移数据和指令，而 RAM 则一般用来双向地转移数据和指令。这两种类型的存储器都可以包含下面说明的任何合适组合的计算机可读的媒体。固定盘 926 双向连接到 CPU922；它提供了外加的数据存储容量，并且也可以包含下面说明的任何计算机可读的媒体。固定盘 926 可以用来存放程序、数据及其它内容，它一般是一个二次存储媒体（例如硬盘）而比一次存储器要慢。应该理解，保存在固定盘 926 中的信息在合适的条件下可以用标准的方式体现为存储器 924 的虚拟存储器。活动盘 914 可以采取下面说明的任何形式的计算机可读的媒体。

CPU922 还连接到各种各样的输入/输出设备，例如显示器 924、键盘 910、鼠标器 912 和喇叭 930。一般说来，输入/输出设备可以是任何一种视频显示器、跟踪球、鼠标器、键盘、话筒、触摸显示屏、传感器、读卡机、磁带或纸带读带机、图形输入板、输入笔、语音或手写体识别器、生物特征读出器、或别的计算机。CPU922 也可以用网络接口 940 接到别的计算机或通信网上。有了这样一个网络接口，就可以设想这个 CPU 将可以在执行上述电话功能时从网络上接收信息，或者向网络输出信息。更进一步，本发明的实施例方法可以单独在 CPU 922 上执行，也可以在诸如因特网这样的网络上结合能分担一部分处理工作的远程 CPU 一起执行。

此外，本发明的实施例还涉及带有计算机可读出的媒体的计算机存储器产品，在该媒体上含有计算机代码以便执行各种由计算机实现的操作。媒体和计算机代码可以是专门为本发明的目标而设计和构造的，或者它们也可以是具有计算机软件技术和技巧的人所熟知和已具备的那些类型。计算机可读出的媒体包括但不限于：诸如硬盘、软盘和磁带之类的磁性媒体，诸如 CD-ROM 和全息设备一类的光学媒体，诸如磁光盘这样的磁光媒体，以及专门设计以便储存和执行程序代码的硬件设备，例如专用集成电路（ASIC）、可编程逻辑器件（PLD）、以及 ROM 和 RAM 器件。计算机代码的例子包括诸如由编译程序产生的机器码，以及含有由计算机利用解释程序来执行的高级代码的文件。

虽然前面的发明为了理解的清晰而已经作了相当详细的说明，但很明显，在所附的权利要求的范围之内可以实现一定的改变和修正。应该指出，在实现本发明的过程和设备方面，两者都有很多可替代的方法。例如，加密和解密机制可以集成在原始的操作系统软件本身之内，因此，就不再需要插入一个滤波器驱动程序。所以，本实施例应该认为是说明性的而非限制性的，而且本发明也不应限制在这里给出的细节中，而是可以在所附的权利要求的范围和等同物范围之内进行修改的。

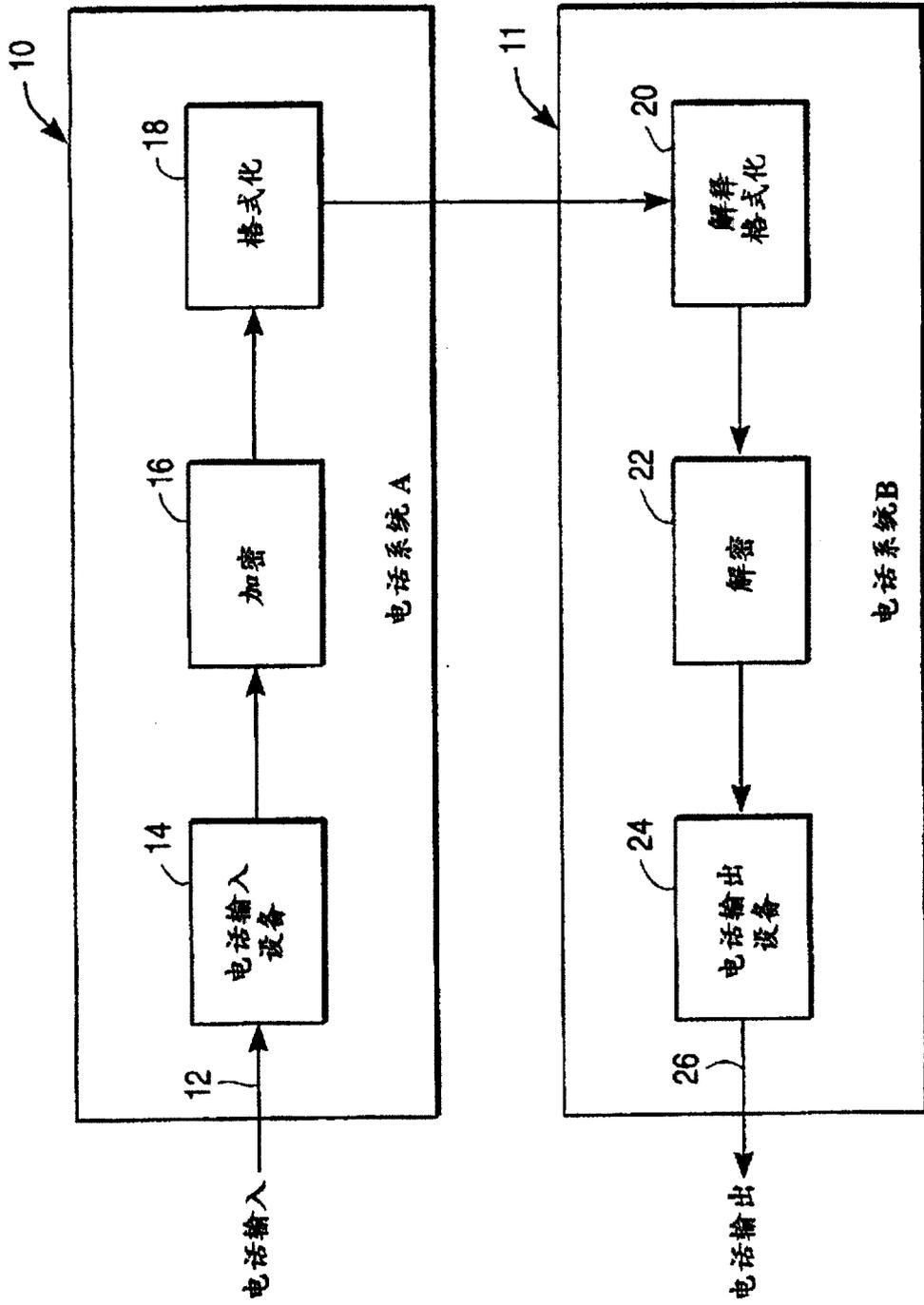


图 1A

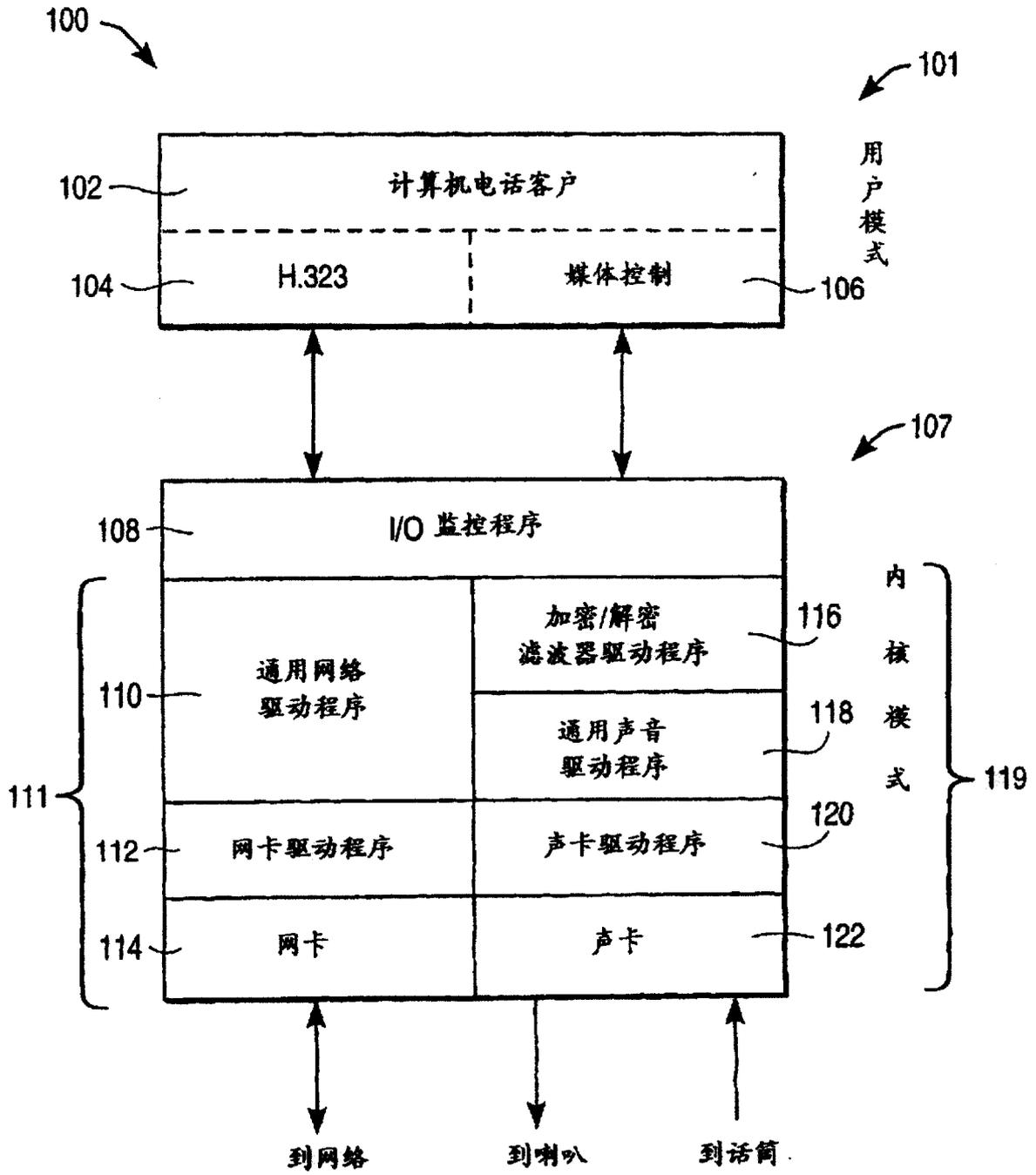


图 1B

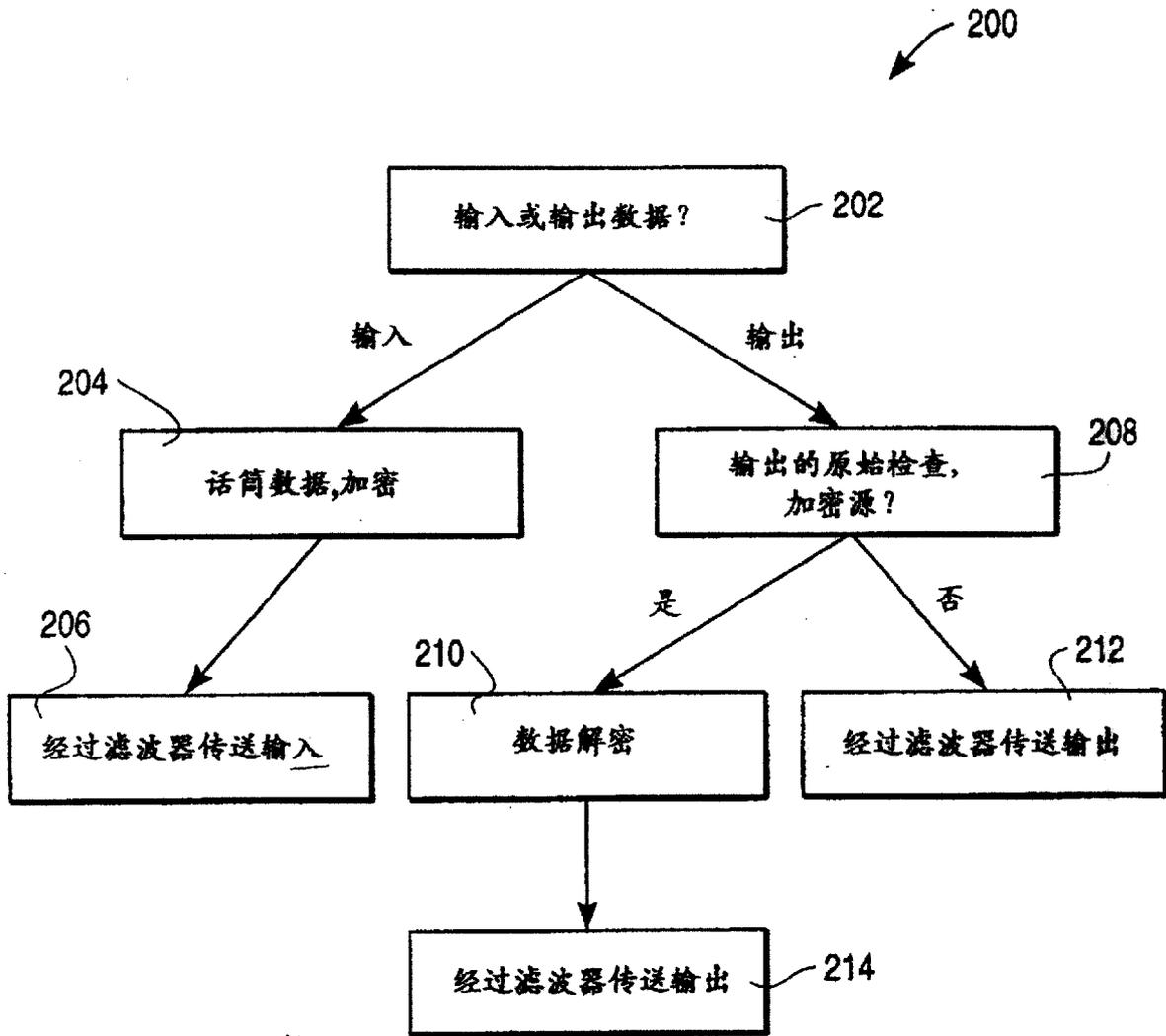


图 2

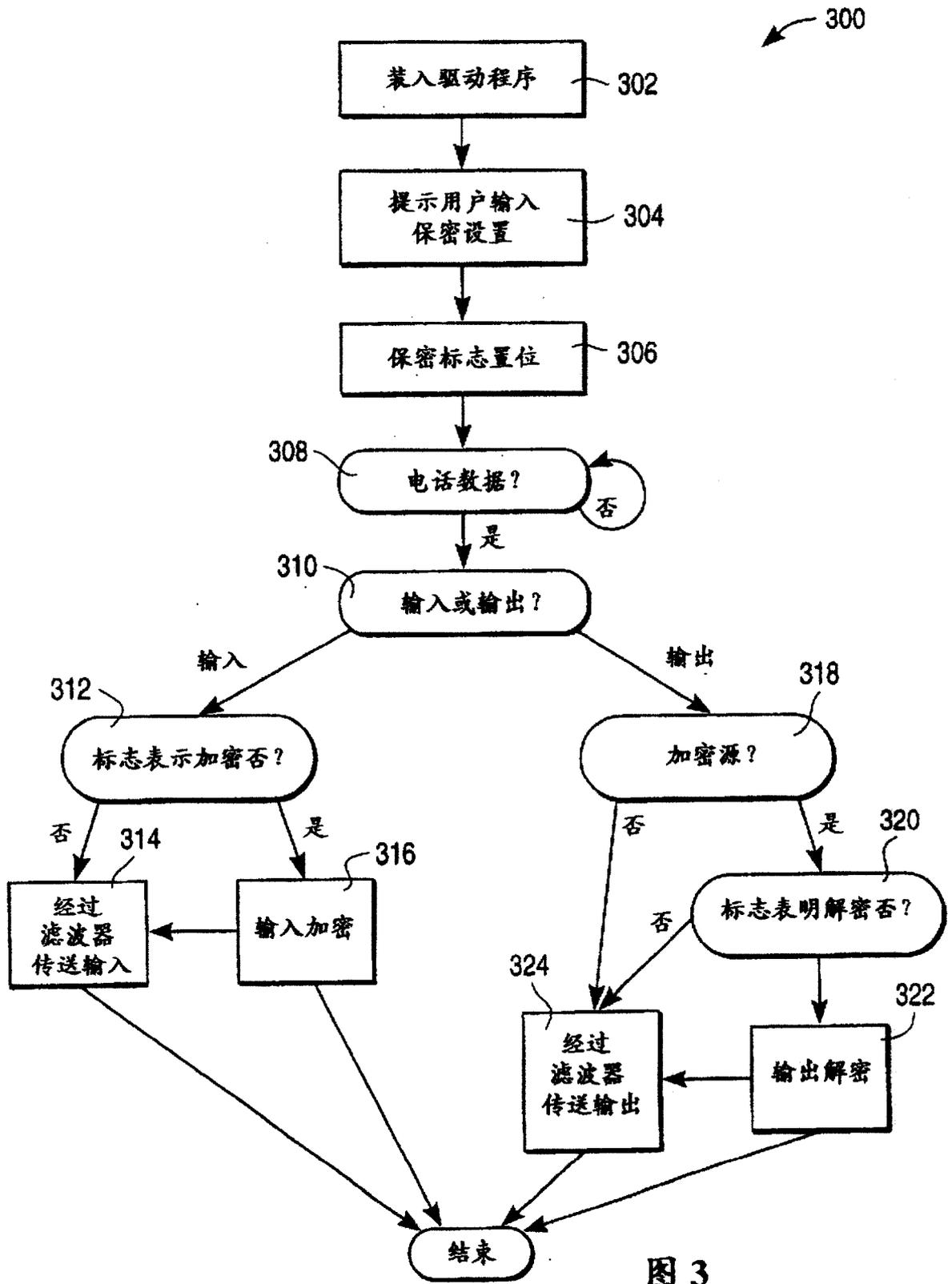


图 3

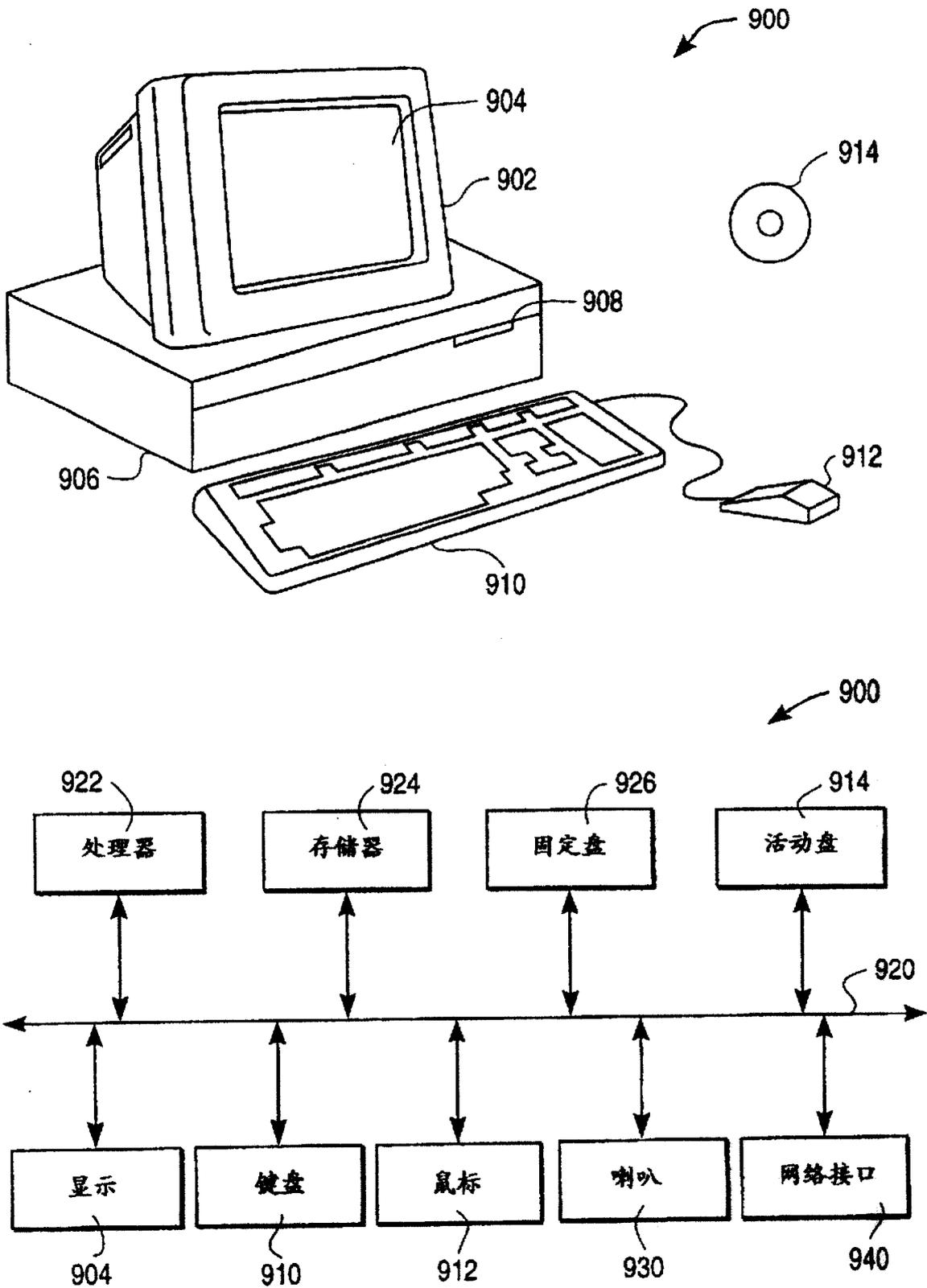


图 4