[19]中华人民共和国国家知识产权局

[51]Int. Cl[7]
H04L 29/06

[12]发明专利申请公开说明书

[21]申请号 00804313.2

[43]公开日 2002年3月20日

[11]公开号 CN 1341318A

[22]申请日 2000.1.12 [21]申请号 00804313.2
[30]优先权
[32]1999.2.26 [33]US [31]09/259,620
[86]国际申请 PCT/US00/00868 2000.1.12
[87]国际公布 WO00/51036 英 2000.8.31
[85]进入国家阶段日期 2001.8.27
[71]申请人 英特尔公司
地址 美国加利福尼亚州
[72]发明人 J·Q·米 V·帕里克
A·Y·滕

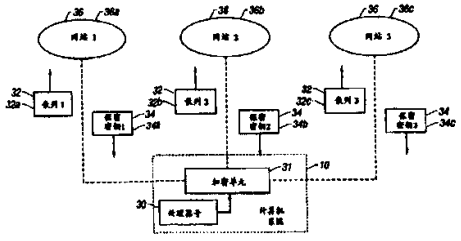
[74]专利代理机构 中国专利代理(香港)有限公司
代理人 王 勇 梁 永

权利要求书2页 说明书8页 附图页数4页

[54]发明名称 计算机系统识别

[57]摘要

计算机系统(10)包括接口(31)和处理器(200)。接口(31)用于接收来自另一个计算机系统对第一个计算机系统进行识别的请求。转接器(31)也将识别第一个计算机系统的散列值提供给其它的计算机系统。处理器(200)被连接到接口(31)上,并用于借助于与其它计算机系统相关的密钥(34)对识别第一个计算机系统的标识符进行加密,以提供散列值(32)。



ISSN1008-4274

01.08.27

权　利　要　求　书

1. 一种方法包括:

从第一个计算机系统接收对第二个计算机系统进行识别的请求; 接收识别第二个计算机系统的标识符;

用与第一个计算机系统相关的密钥对标识符进行加密，生成散列值; 和

将散列值提供给第一个计算机系统以响应请求。

2. 权利要求 1 的方法，其中，接收标识符的操作包括: 接收识别第二个计算机系统处理器的处理器号。

3. 权利要求 2 的方法还包括:

执行处理器指令; 和

接收该号码以响应指令的执行。

4. 权利要求 1 的方法还包括:

从第一个计算机系统上接收密钥。

5. 权利要求 1 的方法，其中密钥指出网站的地址。

6. 计算机系统包括:

一个接口适用于:

从另一个计算机系统上接收对第一个计算机系统进行识别的请求，和

将识别第一个计算机系统的散列值提供给所述的另一个计算机系统; 和

被连接到接口上的处理器并适用于:

借助于与所述的另一个计算机系统相关的密钥对识别第一个计算机系统的标识符进行加密，生成散列值。

7. 权利要求 6 的计算机系统，其中标识符包括识别处理器的处理器号。

8. 权利要求 6 的计算机系统统，其中处理器包括:

存储器适用于存储执行加密操作的微码; 和

被连接在存储器上的控制单元适用于执行微码以实现加密。

9. 权利要求 6 的系统，其中处理器还适用于:

与接口之间进行交互以接收来自所述另一个计算机系统的密钥。

10. 一个产品包括可由基于处理器的第一个系统读取的存储介质，存储介质中存储的指令让处理器:

从另一个基于处理器的系统中接收密钥以识别第一个系统;

确定是否密钥合法;

在识别的基础上，利用密钥有选择地认可对识别第一个系统的标识符进行加密，生成散列值.

11. 权利要求 10 的产品存储介质存储的指令要处理器:

利用所述其它系统的地址确定是否密钥合法.

12. 权利要求 11 的产品，其中密钥指出 URL 地址.

13. 权利要求 10 的产品，存储介质存储的指令要处理器:

执行指令，以便接下来处理器能够利用密钥生成散列值.

14. 权利要求 10 的产品，其中标识符包括了处理器号码.

15. 微处理器包括:

指令单元适用于指出何时指令单元接收到了指令，该指令请求识别微处理器的标识符;

被连接到指令单元上的执行单元适用于响应来自指令单元的指示，利用标识符对密钥进行加密，生成散列值; 和

被连接到执行单元上的总线接口单元适用于将对散列值的指示提供给微处理器的外部引线.

16. 权利要求 15 的微处理器，其中执行单元包括:

被连接到算法单元和寄存器上的控制单元; 和

被接到控制单元上存储微码的存储器，让控制单元使用密钥和标识符生成散列值.

17. 权利要求 15 的微处理器，其中标识符包括处理器号.

18. 权利要求 15 的微处理器，其中执行单元适用于使用单向散列函数生成散列值.

19. 权利要求 15 的微处理器，其中执行单元适用于使用不可通信联络的散列函数生成散列值.

20. 权利要求 15 的微处理器，其中执行单元用适于使用非碰撞的散列函数生成散列值.

01.08.27

说　明　书

计算机系统识别

背景

本发明与计算机系统的识别有关。

服务器（如因特网服务器）可能布置在提供特定服务的网站上。在这种方式下，网站上的用户可以通过用户计算机系统与网站间进行通信。有时，服务器可以控制对网站的访问，以便仅选取的一组用户可以访问网站提供的服务。

电子邮件的广泛应用以及团体和基于聊天的网站的迅速壮大，允许因特网用户接触和与他们以前从不相识的人相互配合。遗憾的是，并非所有加入这种论坛的人都是善意的。尽管事实是多数的聊天室使用如用户名和通行字的访问控制进行进入团体的访问控制，但是少数的用户由于不当行为被拒绝访问后仍可以绕过这些访问控制。例如，一个被封禁的用户可以采用一个新的用户名而重新获取对聊天区的访问，继续破坏行为。这种逃避现象让一个人破坏了一组人的努力，减少了他们在线经历中的快乐。

嵌入式标识符，如处理器序列号（下面称为处理器号），通过识别访问网站的计算机系统，可以提供一种阻止上述行为的有效方法。对于一个责任要求严格的特定聊天室，例如未成年人的聊天室，网站可以创建可靠的聊天环境，其中要求个人提供处理器号（另外有他们的姓名和通行字）以便获取对聊天室的访问，因而处理代码是强行的、可靠的。如果聊天区中的各个成员自愿提供他或她的处理器号，结果就会有更为安全的社区，它可以更为有效地对付潜在地威胁行为。总之，如果有问题的用户自愿加入到通过使用处理器号不仅促进而且增强责任行为的房间中，即使有问题的用户改变他们的用户名，那么仍可以阻止他们要再次获得对聊天室的曾被否认过的访问的能力。

遗憾的是，用于识别用户计算机系统的嵌入式标识符的使用会提出一些难题。例如，该号码可以被用于建立一个连接在用户和在因特网上保存着的不同数据库之间的信息路径。而这些数据库又关系到要建立一个用户私人信息的巨大数据库。尽管如此，由于事实上用户可

能具有使处理器号识别失败的能力，因而建立这样的数据库是不可能的，仍需要继续加强用户的私人保护。

概述

在本发明的一种实施例中，方法包括接收来自第一个计算机系统的对第二个计算机系统识别的请求，并检索出识别第二个计算机系统的标识符。借助于与第一个计算机系统相关的密钥，标识符被加密，生成一个散列值。散列值被提供给第一个计算机系统以响应接收的请求。

在另一种实施例中，计算机系统包括接口和处理器。接口用于接收来自另一台计算机系统的对第一个计算机系统进行识别的请求。接口能够将识别第一个计算机系统的散列值提供给其它的计算机系统。处理器被连接到接口上。处理器能够借助于与其它计算机系统相关的密钥对识别第一个计算机系统的标识符进行加密，生成散列值。

在另一种实施例中，一个产品包括可被基于处理器的第一系统读取的存储介质。存储介质存储着指令，能让处理器从另一个系统上接收密钥以识别第一个系统，并确定密钥是否合法。基于这种识别，指令引导处理器有选择性地认可标识符加密，这些标识符借助密钥来识别第一个计算机系统，生成散列值。

也是在此另一种实施例中，微处理器包括指令单元、执行单元和总线接口单元。指令单元用于指示当指令单元接收时对识别微处理器的标识符进行请求的指令。执行单元被连接到指令单元上，用于响应来自指令单元的指示，利用识别微处理器的标识符对密钥进行加密，生成散列值。总线接口单元被连接到执行单元上，用于将散列值的指示提供给微处理器的外部引线。

附图简述

图 1 是按本发明实施例的网络的示意图。

图 2 是按本发明实施例的由图 1 的计算机系统执行的软件的图解。

图 3 是按本发明实施例的图 1 计算机系统的详尽示意图。

图 4 是按本发明实施例的逻辑算法执行过程的图解，它能控制由图 3 的计算机系统的微处理器提出的识别请求。

图 5 是按本发明实施例的图 3 处理器的示意图。

详细说明

参看图 1，按本发明的计算机系统的实施例 10 包括加密单元 31，它可以从网站 36（如网站 36a，36b 和 36c）上接收对计算机系统 10 识别的识别请求。为响应这些请求，加密单元 31 要将不同的散列值 32（如散列值 32a，32b 和 32c）提供给不同的网站 36。在一些实施例中，各个散列值 32 是不同的，结果，尽管各个散列值 32 是由单一个处理器号 30 生成的，各个网站 36 要通过不同的散列值 32 去识别计算机系统 10，说明如下。因为各个网站 36 将计算机系统 10 与不同的散列值 32 联系起来，关于计算机系统 10 用户的信息在被不同网站 36 保存的数据库之间可能是不相关的。例如，特定网站 36 可以通过散列值“1bdf23”识别计算机系统 10，另一个网站 36 可通过散列值“53gh44”识别计算机系统 10。另外，正如下面要说明的，加密单元 31 生成散列值 32 的方式使得不良网站 36 难于获取其它网站 36 识别计算机系统 10 的散列值 32。因此，鉴于加密单元 31 中使用的技术之故，难于从被不同网站 36 保存的数据库中关联得到用户信息。在此文中，术语“网站（web site）”一般指一种配置方案，其中计算机系统（如服务器）执行软件以向其它的计算机系统如计算机系统 10 提供服务。

在本申请中，词组“计算机系统（computer system）”一般是指基于处理器的系统，可能包括（但不限于）如下几个例子：图形系统，台式计算机，便携式计算机（如膝上电脑），或是置顶盒。术语“处理器（processor）”指至少一个如中央处理单元（CPU）、微控制器、X86 微处理器、高级 RISC 机（ARM）微处理器或是奔腾微处理器的设备。实际上并不限于上述列举的例子，其它类型的计算机系统和处理器也可以被包括在本发明的某些实施例中。

为了获得识别计算机系统 10 的散列值，特定网站 36 可以将保密密钥 34（例如保密密钥 34a、34b、34c）传送给计算机系统 10。作为响应，加密单元 31 利用密钥 34 将被嵌入的标识符如处理器号 30 进行加密，生成散列值 32，计算机系统 10 将散列值提供给正在请求的网站 36。在这种方式下，如果各个网站 36 将不同的保密密钥 34 传递给计算机系统 10，那么各个网站 36 将接收不同的散列值 32，各个散列值都将计算机系统 10 指定到一个特定的网站 36 上。正如下面

将要进一步说明的，加密单元 31 可能包括处理器 200（如图 3），以便借助处理器号 30 辅助保密密钥 34 的加密。

保密密钥 34 可能是也可能不是保密密钥，这依赖于特定的实施例。例如，在某些实施例中，保密密钥 34 是从网站 36 的地址或通用资源定位器（URL）中导出的。因此，例如，保密密钥 34 可以指字符串，如www.example.com。如下所述，对于保密密钥 34 从 URL 中导出的这类实施例，计算机系统 10 可能要执行合法检验以确定特定网站 36 提供的保密密钥 34 是否是基于网站 36 的 URL。

在某些实施例中，加密单元 31 可能使用散列函数称之 F（PN, PRIVACYKEY）实现加密。F（PN, PRIVACYKEY）函数具有的性质可能使其更难于追踪被存储在不同网站 36 上的用户信息（有关计算机系统 10 的）。F（PN, PRIVACYKEY）散列函数中，符号“PN”代表处理器号 30，符号“PRIVACYKEY”代表保密密钥 34。

F(PN, PRIVACYKEY)散列函数的一个性质是: F(PN, PRIVACYKEY)函数是单向散列函数，意味着是给定散列值 32 和保密密钥 34 的一个符号，如果不是不可能的话，那么也难于反过来去确定处理器号 30。因此，对于特定的网站 36 难于利用从网站 36 上获得的散列值 32 导出处理器号 30。

在某些实施例中，F（PN, PRIVACYKEY）函数的另一个特性是: F（PN,PRIVACYKEY）函数是无碰撞的，这意味着 F（PN,PRIVACYKEY）是散列函数非常不可能给不同的保密密钥 34 返回相同的散列值的一个项目。因此，特定的网站 36 也非常不可能使用 F(PN,PRIVACYKEY)函数（以及相关的保密密钥 34）给两个不同的处理器号 30 获取相同的散列值 32。因此，这一特点确保了特定网站 36 很可能使用不同的、唯一的处理器号 30 去识别各个计算机系统。

F（PN,PRIVACYKEY）函数（在某些实施例中）的另一个性质是: F（PN,PRIVACYKEY）函数是不可通信联络的，如下所述 F（F（PN,PRIVACYKEY），PRIVACYKEY’））≠F（F（PN,PRIVACYKEY’），PRIVACYKEY）），其中“PRIVACYKEY’”表示的保密密钥 34 不同于由“PRIVACYKEY”表示的保密密钥 34。不可交换这一性质的结果导致在使用不同保密密钥 34 时难于将不同数据库中（不同网站 36 上）与计算机系统 10（以及用户）相关的信息互联起来。

在不同的实施例中，多种不同的散列函数可能得以应用，它们可能满足一个，多个或者以下解释过的所有的性质．例如，在某些实施例中使用了安全散列逻辑（SHA），该逻辑算法满足以上所有描述过的性质．

在某些实施例中，当特定网站 36 正在请求系统识别时，计算机系统 10 可能会通知系统 10 的用户．例如，这种通知以在计算机系统 10 的显示器 14（如图 3）上形成提示窗口的形式给出．以这种方式用户可以允许网站 36 获得标识符（由散列值 32 提供）或是拒绝该请求．在某些实施例中，用户可以选择关闭该提示．

除了向用户提示这一识别请求外，计算机系统 10 还采取措施防止恶意网站 36 由提交不正确的保密密钥 34 以达到获取与另一网站 36 相联系的散列值 32 的目的．例如，在某些实施例中，识别请求可能包括两部分识别程序．首先，网站 36 通过执行（如下所述如果能得到认可）处理器 200（如图 2）上的指令（称为 SETKEY(PRIVACYKEY)）设置保密密钥 34．参见图 2，如下所述，SETKEY（PRIVACYKEY）函数可能是与操作系统 28 的零级环（ring zero）（即最高层）相关的．结果，在计算机系统 10 通过执行软件程序一称之驱动程序 19 使提供的保密密钥 34 合法之前，计算机系统 10 不可能允许处理器指令的执行．当保密密钥经过驱动程序 19 执行而被合法化后，网站 36 可以得到认可去执行处理器指令称为 HWID（）（即 HWID（）指令可能没有输入参数），该指令与操作系统 28 的三级环（即低级优先层）相关，用于获取散列值 32．

更为特殊的是，在某些实施例中，上述说明过的识别程序可包括操作系统 28、因特网浏览器 27（如 Internet Explorer 或 Netscape Navigator）和驱动程序 19 之间的交互作用．例如，因为 SETKEY(PRIVACYKEY)指令与零级环相关，网站 36 本身不可能引导指令的执行以获得散列值 32，网站 36 仅可以访问操作系统 28 的三级环（低级优先层）和更高级的环（即更为低级的优先层）．然而，驱动程序 19 可能具有零级环优先权，因而可以构成网站 36 和操作系统 28 的零级环优先权之间的桥梁．以这种方式，当网站 36 想要执行 SETKEY(PRIVACYKEY)指令时，驱动程序 19 可以被操作系统 28 调用以便在提供散列值 32 之前让处理器 200 对保密密钥 34 进行合法化．在

驱动程序 19 的执行中，处理器 200 可以利用从浏览器 27 获得的执行结果将保密密钥 34 合法化，如下所述。

参看图 4，当驱动程序 19 被处理器 200 执行时，该程序引导处理器 200 执行下列功能。尤其是，当识别请求被接收到后，驱动程序 19 要引导处理器 200 去确定（菱形块 50）是否用户激活了用户提示选项。如果是，处理器 200 提示（方块 52）（如通过显示器 14（如图 2））用户网站 36 已经提交了识别请求并等待用户指示（如通过键盘 24 或鼠标 26（如图 2））是否用户想要拒绝请求。如果拒绝，处理器 200 通知网站 36（块 56）拒绝请求。

然而，如果用户并未拒绝请求，处理器 200 可以确定（菱形块 58）是否浏览器现在正在被执行。如果是，程序 19 引导处理器 200 将保密密钥 34 传送给（块 60）浏览器 27。因此，当处理器 200 执行浏览器 27（如在另外的线程中）时，处理器 200 要将保密密钥 34 与网站 36 上的 URL 进行比较。接下来，处理器 200 传送比较结果，以便由驱动程序 19 使用。用这种方式，当处理器 200 接下来执行了驱动程序 19 时，处理器要确定（菱形块 62）是否保密密钥 34 与网站 36 上的 URL 匹配。如果不匹配，处理器 200 拒绝请求并通知（块 56）网站 36 拒绝识别请求。否则，处理器 200 执行（块 64）SETKEY(PRIVACYKEY) 指令，设置保密密钥以用于处理器号 30 的加密。以这种方式，提交了保密密钥 34 的网站 36 引导处理器 200 执行 HWID()指令，使处理器 200 生成散列值 32 的指示。然而，如果保密密钥 34 未被设定，处理器 200 将返回错误的指示，而不是散列值 32 的指示。

回头参看图 3，在某些实施例中，计算机系统 10 可能包括桥接器或存储器插机 16。处理器 200 和存储器插机（hub）16 可被连接到主机总线 23 上。存储器插机 16 可以提供接口，将主机总线 23，存储器总线 29 和加速图形端口（AGP）总线 11 连接到一起。在 1996 年 7 月 31 日由 Santa Clara，California 的因特公司发行的加速图形端口接口说明书版本 1.0 中有 AGP 的详细说明。系统存储器 18 可被连接到存储器总线 29 上，并存储驱动程序 19、浏览器 27 和操作系统 28 的各部分（图 3 中为给出）。图形加速器 13（控制显示器 14）可被连接到 AGP 总线 11 上。插机通信链 15 可将存储器插机 16 连接到另一个桥接器电路上，或是输入/输出（I/O）插机 20 上。

在某些实施例中，I/O 集线器 20 包括到 I/O 扩展总线 25 和外围部件互联（PCI）总线 21 上的接口。PCI 详细说明可以从 PCI Special Interest Group, Portland, Oregon97214 上获得。网络接口 12（如调制解调器或局域网卡（LAN））可被连接到 PCI 总线 21 上，给计算机系统 10 提供与网站 36 进行通信的通信路径。以这种方式，处理器 200 可以与网络接口 12 进行交互作用，以便与网站 36 进行通信。I/O 插机 20 也包括到如硬盘驱动器 37 和 CD－ROM 光驱 33 上的接口。I/O 控制器 17 可被连接到 I/O 扩展总线 25 上，接收来自如键盘 24 和鼠标 26 的输入数据。I/O 控制器 17 也控制软盘驱动器 22 的操作。驱动程序 19 的复本被存储在如下列举的几种设备上：硬盘驱动器 32、磁盘或光盘。

参看图 5，作为一个例子，处理器 200 可包括总线接口单元（BIU）208，它被连接到主机总线 23 的地址、控制和数据线上，在其它的操作中收回来自系统存储器 18 的指令和数据。对于指令而言，处理器 19 可包括指令单元 203，它被连接到总线单元 208 上，对指令进行译码。这种方式下，指令单元 203 可具有缓冲区和高速缓存以存储指令。（处理器 200 的）控制单元 208 可接收指令单元 203 的对译码后的指令进行指示的信号。例如，信号可能指出该指令要执行 SETKEY(PRIVACYKEY)函数还是指令要执行 HWID()函数。

为了响应被指令单元 203 指示的指令，在某些实施例中，控制单元 208 接收来自处理器 200 的微码只读存储器（ROM）210 中的相应的初等指令—称为微码，然后执行微码。例如，会引导处理器 200 执行 SETKEY(PRIVACYKEY)和 HWID()指令的微码 211 可能被存储在微码只读存储器（ROM）210 上。在执行指令完成时，控制单元 208 可以控制数学逻辑单元（ALU）212、寄存器 214 和地址单元 206。

其它的实施例也是在下列权利要求的范围内。例如，在其它的实施例中，执行 SETKEY(PRIVACYKEY)和 HWID()指令的电路系统是硬接线的，而不是在微码中实现的。处理器号 30 可被其它识别计算机系统 10 的标识符所代替。使用的是保密密钥而非指示 URL 的字符串。应用程序而非正被网站执行的应用程序可以请求计算机系统 10 的标识符。例如，通过局域网（LAN）被连接的其它计算机系统可能请求来自计算机系统 10 上的标识符。

鉴于本发明仅表述了有限的几个实施例，受益于这些阐述的本领域中的技术人员会意识到在此基础上的更多改进和变化。因而要在附加的权利说明中囊括所有这些本发明的精神和范围内的变换。

说 明 书 附 图

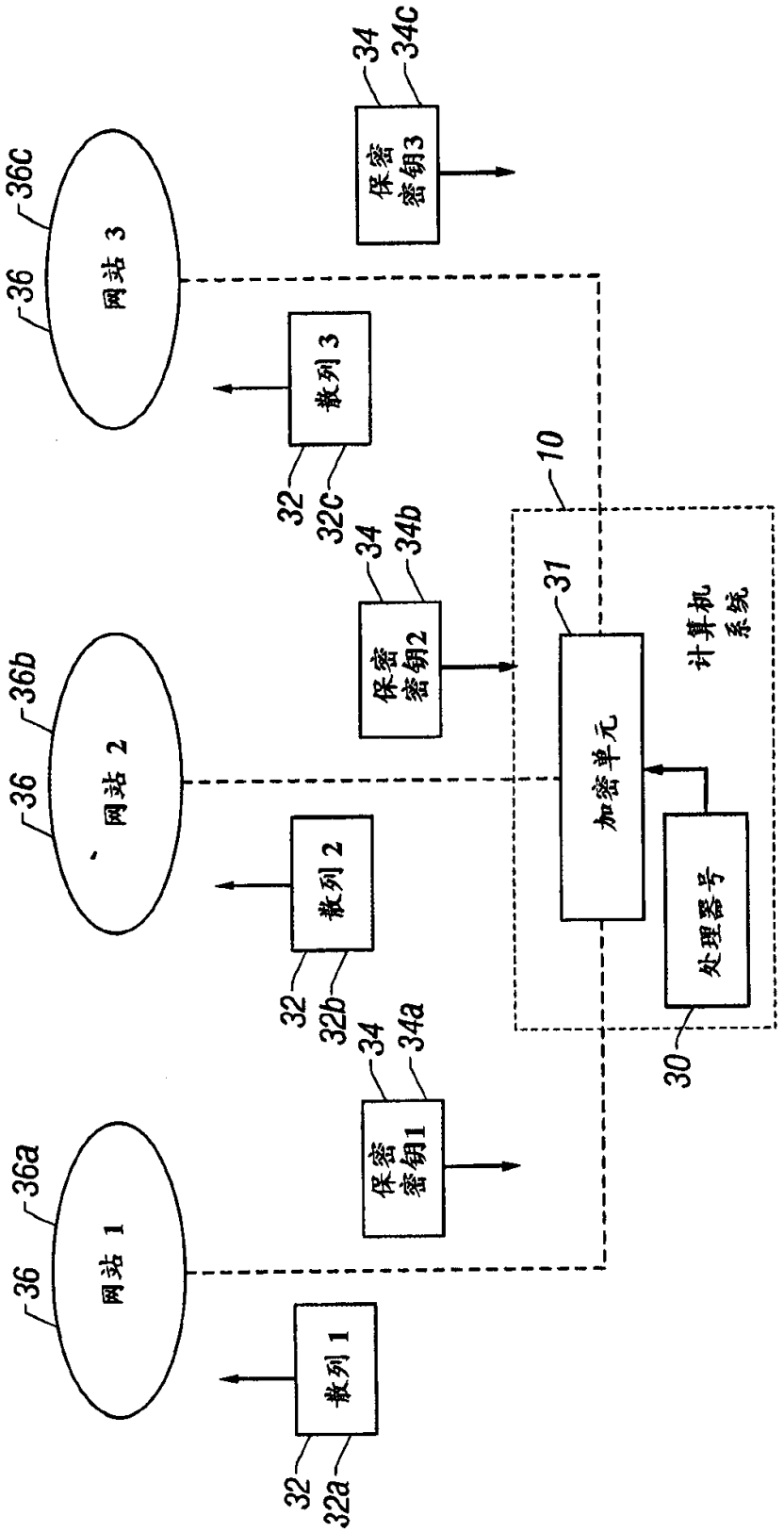

网站 1
网站 2
网站 3
36
36a
36b
36c
散列 1
散列 2
散列 3
32
32a
32b
32c
保密密钥1
保密密钥2
保密密钥3
34
34a
34b
34c
加密单元
处理器号
计算机系统
10
30
31

图 1

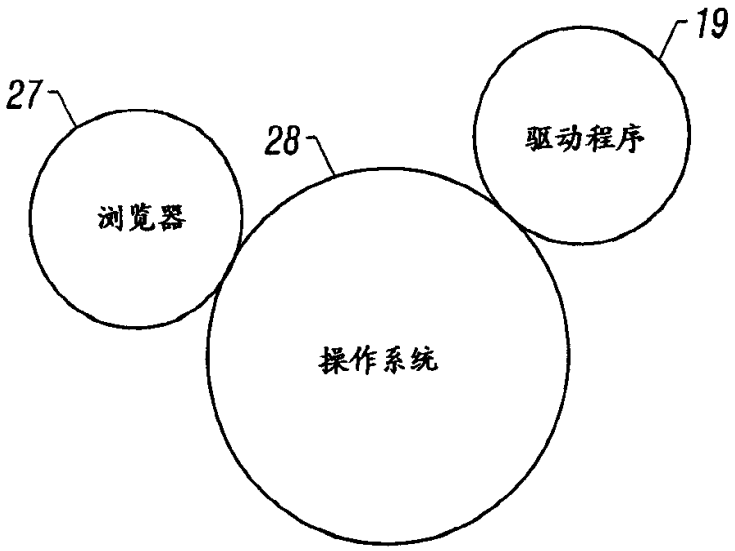

19
驱动程序
27
浏览器
28
操作系统

图 2

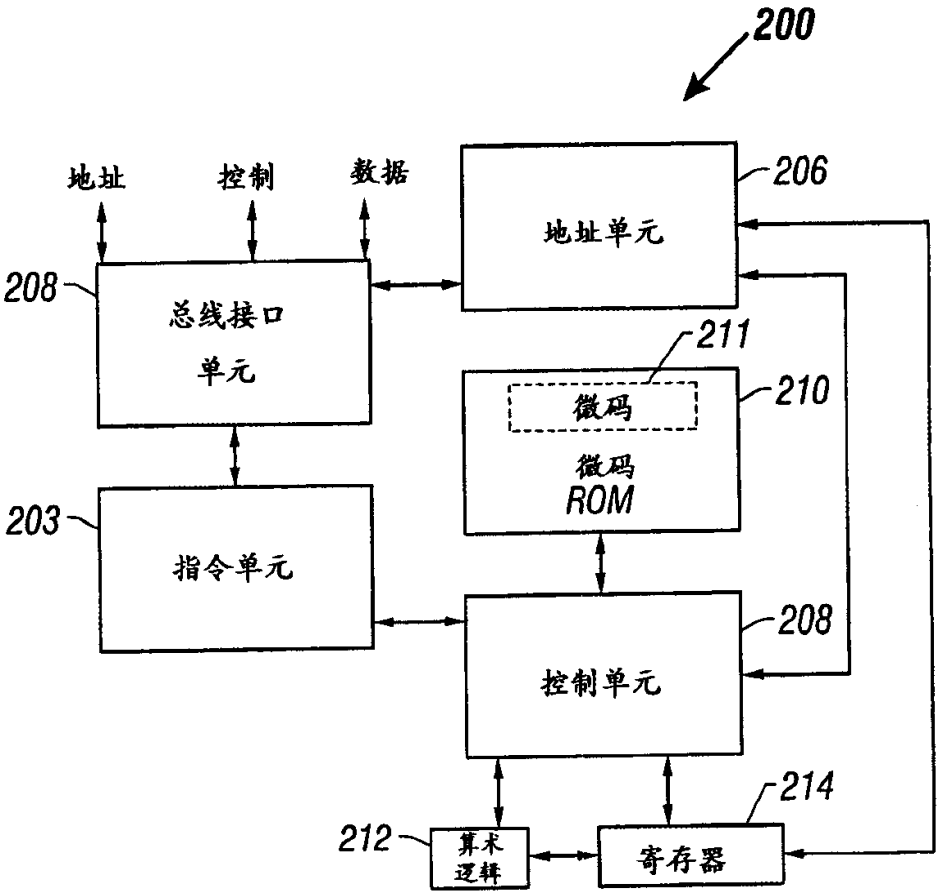

200
地址
控制
数据
206
地址单元
208
总线接口
单元
211
微码
210
微码
ROM
203
指令单元
208
控制单元
214
212
算术
逻辑
寄存器

图 5

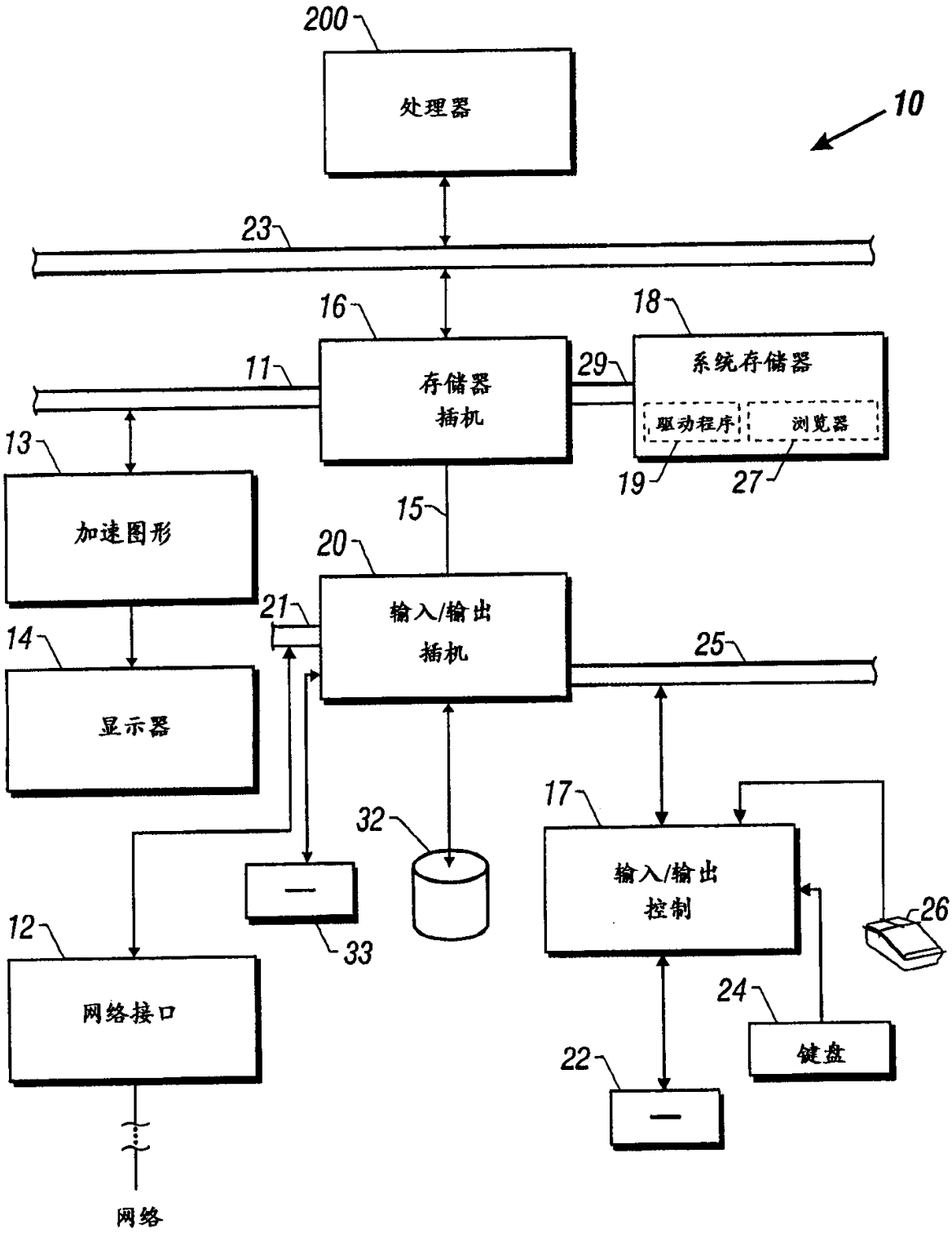

200
处理器
10
23
16
18
11
存储器
插机
29
系统存储器
驱动程序
浏览器
19
27
13
加速图形
15
20
21
输入/输出
插机
25
14
显示器
32
17
输入/输出
控制
26
12
33
网络接口
24
键盘
22
网络

图 3

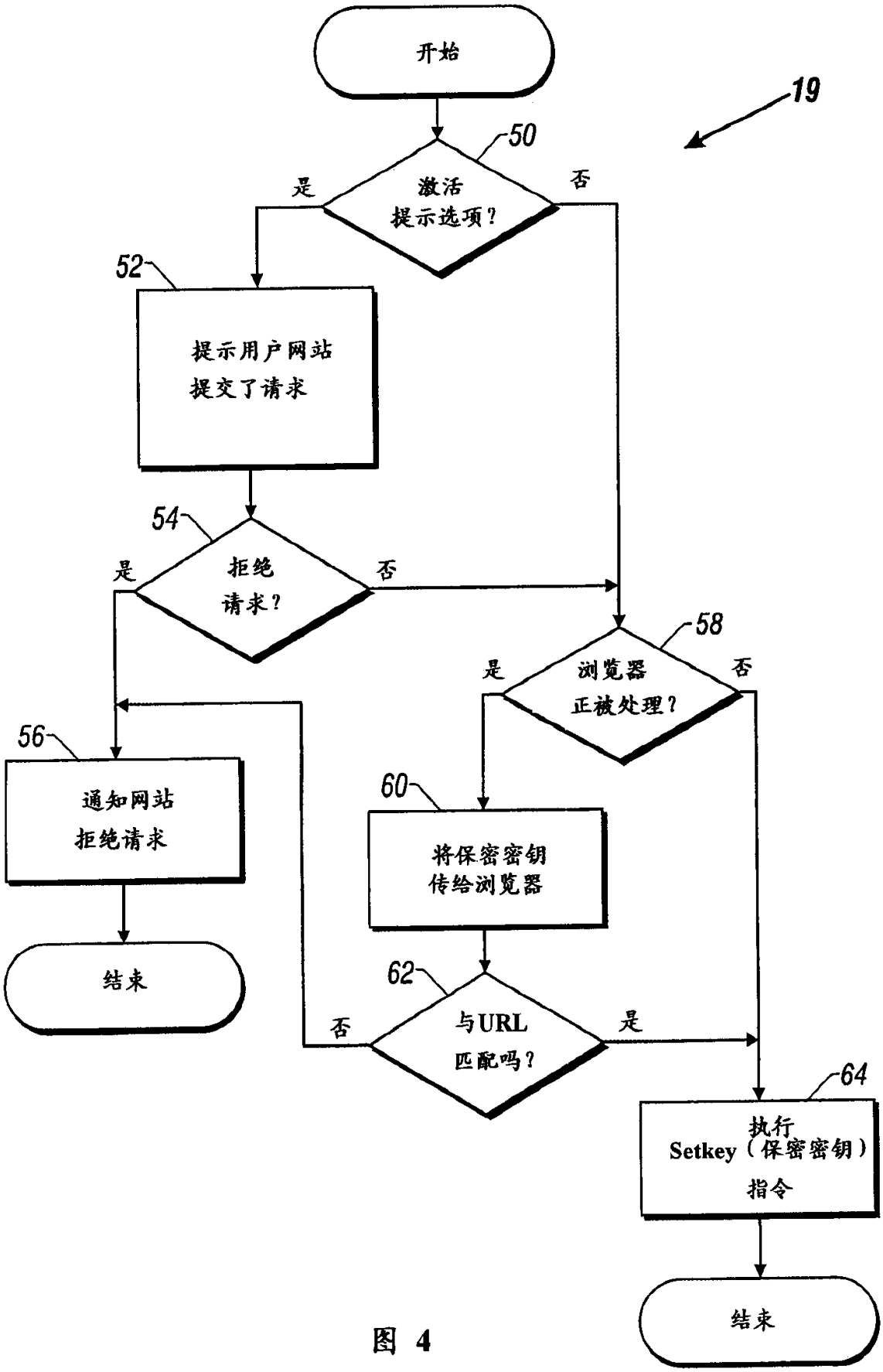

开始
19
50
激活
提示选项？
是
否
52
提示用户网站
提交了请求
54
拒绝
请求？
是
否
58
浏览器
正被处理？
是
否
56
通知网站
拒绝请求
60
将保密密钥
传给浏览器
结束
62
与URL
匹配吗？
否
是
64
执行
Setkey（保密密钥）
指令
结束

图 4